# Vymezení předmětu plnění veřejné zakázky

## Předmět plnění veřejné zakázky

* + - 1. Předmětem plnění veřejné zakázky jsou **dodávky zařízení a služeb** (dále také jen „řešení“) – vybudování systému pro správu identit, systému pro správu provozní dokumentace a personálního systému.
      2. Předmětem plnění veřejné zakázky jsou dodávky a služby (komodity) uvedené v následující tabulce. Podrobná specifikace dodávek a služeb je uvedena dále v dokumentu.

|  |  |  |
| --- | --- | --- |
| **Označení** | **Zařízení** | **Počet** |
| K1 | Správa identit | 1 |
| K2 | Správa provozních dokumentů | 1 |
| K3 | Systém pro řízení virtuálních desktopů | 1 |

## Popis výchozího stavu

### Popis organizace a její členění

* + - 1. Organizace Karlovarská krajská nemocnice a.s. (dále také jen KKN) vznikla fúzí nemocnic v Karlových Varech, Sokolově a Chebu. K 1. lednu 2011 byla na základě Smlouvy o pronájmu části podniku vyčleněna Nemocnice v Sokolově, kterou nyní spravuje společnost Nemos Sokolov spol. s r.o. – tato nemocnice není součástí lokalit pro realizaci předmětu plnění.
      2. Organizace sídlí v areálu nemocnice Karlovy Vary (dále KV), kde pracuje větší část zaměstnanců a je zde umístěná významná část IT technologií.

### Popis lokalit

* + - 1. Z pohledu IT je pro Zadavatele nejvýznamnější lokalitou areál nemocnice Karlovy Vary. V této lokalitě jsou umístěny jak ICT technologie pro nemocnici KV, tak i sdílené technologie pro nemocnici CH. Provoz ICT je zajišťován vlastními zaměstnanci Zadavatele ve spolupráci s externími specializovanými firmami.
      2. Projekt bude realizován v těchto lokalitách:
         1. Areál nemocnice Karlovy Vary (dále také jen „KV“) na adrese Bezručova 1190/19, 360 01 Karlovy Vary.
         2. Areál nemocnice Cheb (dále také jen „CH“) na adrese K Nemocnici 1204/17, 350 02 Cheb.

### Popis stávajícího HW prostředí

* + - 1. Pro provozování ICT technologií má Zadavatel v každé lokalitě vybudovány serverovny, které jsou mezi sebou propojeny optickou trasou Regionální komunikační infrastruktury (dále RKI). RKI je WAN na bázi optických vláken propojující významné úřady a veřejné organizace v kraji včetně všech lokalit Zadavatele. Přenosová kapacita páteřních spojů RKI je 512 Mb/s. RKI je vlastněná Karlovarským krajem a je jím, ve spolupráci s externími partnery, provozována a rozvíjena.
      2. RKI je provozována na technologiích HP, klíčovými prvky jsou 2 centrální šasi HP 7500, jako koncové a uzlové přepínače jsou využívány prvky řady HP 5500 a HP 5800.
      3. Každá serverovna je v uzamykatelném prostoru, je vybavena třema klimatizacemi, přičemž trvale v provozu jsou dvě (třetí klimatizace slouží jako záloha). V serverovně je nainstalováno prostorové čidlo požáru, jeden centrální RACK se zhášecím systémem a ručním hasicím přístrojem. Pro případ dlouhodobého výpadku elektrické energie je k dispozici dieselagregát.
      4. Serverovna KV je navržena, tzn. má prostorovou kapacitu, pro poskytování vysoce dostupných infrastrukturních ICT služeb jak v rámci lokality KV, tak i ostatním lokalitám.
      5. Serverová infrastruktura KKN je tvořena kombinací tří fyzických serverů HPE serverů v Karlových Varech a tří fyzických serverů HPE serverů v Chebu. Všechny servery jsou virtualizovány technologií Hyper-V Jako operační systém jsou využívány Windows a Linux. Disková pole jsou značky HPE.
      6. Síťová infrastruktura KKN je tvořena přepínači HPE řad 1xxx, 25xx, 4xx a 5xxx s operačním systémem Comware. V obou lokalitách je vybudované kompletní propojení všech pavilónů pomocí optické sítě na 1GB, páteřní spoje mají kapacitu 10Gb.
      7. Zálohování a obnova dat v KKN je řešeno pomocí centrálního zálohování na NAS úložiště v KV.
      8. Přístup na internet je zajištěn 300MBit bezdrátovou linkou (v obou lokalitách). Zabezpečení přístupu k internetu využívá firewall postavený na linuxové distribuci IP COP.
      9. KKN používá pro vzdálený přístup terminálové připojení.
      10. Obě lokality jsou napojeny na RKI (regionální komunikační infrastrukturu) Karlovarského kraje, které propojuje hlavní krajské organizace (Nemocnice, Správa silnic apod.), školy a městské úřady ORP (obcí s rozšířenou působností) v kraji.
      11. Zadavatel má implementovány adresářové služby Active Directory. Pro jmenné a adresní síťové služby (DNS a DHCP) je využívána služba Windows Serveru.
      12. Koncové stanice (počítače) jsou různého stáří (více jak 50% je starších 7 let), pocházejí od různých výrobců, provozovanými operačními systémy jsou Windows 7 a 10, celkem je cca 600 PC v lokalitě KV a cca 240 PC v lokalitě CH. PC jsou průběžně nahrazovány tenkým klienty využívajícím aplikační virtializace Microsoft Remote desktop services (RDS)
      13. Tiskové prostředí je tvořeno v KV převážně síťovými tiskárnami v celkovém počtu 240 kusů, v CH přávážné lokální tiskárny (USB) a dvě multifunkční tiskárny v pronájmu. V CH je v provozu 180 tiskáren. Typové řady jsou velmi různorodé.
      14. Serverová a systémová infrastruktura je vybudována jako redundantní a v současné době jsou implementovány technologie umožňující automatické překlenutí odstávky (plánované i neplánované) klíčového prvku s žádným nebo minimálním (v řádu jednotek minut) výpadkem služeb.

### Popis stávajícího SW prostředí

* + - 1. Systémové služby Zadavatele jsou provozovány na platformě Microsoft Windows převážně ve verzi 2016 a Linux.
      2. Část uživatelů má k dispozici kancelářský balík Microsoft Office ve verzích 2016 a nižší, zbývající uživatelé mají k dispozici volně šiřitelné kancelářské aplikace (Libre Office).
      3. K ukládání sdílených souborů je využíváno prostředků Windows serveru a diskového úložiště.
      4. Data informačních systémů a ostatních aplikací jsou ukládána převážně do databází Microsoft SQL Server, provozovány jsou verze 2016 a 2012 Standard.
      5. Groupwarové služby zajišťuje systém IceWarp. Systém zajišťuje i obsluhu mobilních zařízení.
      6. Pro správu požadavků je využíván systém Service Desk (výrobce Alvao)
      7. K technické evidenci a správě majektu je využívám systém Asset Management (výrobce Alvao)
      8. Služby single-sign-on a vícefaktorového ověřování 400 klíčových uživatelů jsou zajšťovány systémem Imprivata (výrobce Imprivata)
      9. Hlavními informačními systémy Zadavatele jsou:
         1. nemocniční informační systém je Fons Enterprise (výrobce Stapro).
         2. laboratorní informační systém OpenLIMS (výrobce Stapro) a Lims (výrobce Dssoft)
         3. ekonomický informační systém Helios Green (výrobce Asseco)
         4. PACS systém MARIE-PACS (výrobce OR-CZ)
         5. Mzdový systém Avensio (výrobce Alfa Software)
         6. Docházkový systém (výrobce IVAR a.s.),
         7. dále systémy menších agend potřebných pro provoz nemocnice – systém pro objednávání stravy, nemocniční lékárna (výrobce Apatyka servis) a další
      10. Dostupnost dat ze stávajících informačních systémů je možná pomocí rozhraní API. API pro jednotlivé aplikace, které je nutné integrovat, jsou buď k dispozici, nebo v současné době neexistují a budou vytvořena stávajícími výrobci a vítěznému uchazeči bude zpřístupněn popis těchto API do 60 kalendářních dní od data účinnosti smlouvy. Uchazeč je povinen zahrnout do své nabídky náklady na vytvoření těchto API rozhraní v dále uvedené výši:

|  |  |  |
| --- | --- | --- |
| **Stávající systémy** | **API rozhraní** | **Náklady na vytvoření API** |
| Ekonomický systém Helios Green (výrobce Asseco) | K dispozici je API tvořené sadou WS | API rozhraní – cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 1.850 Kč za hodinu |
| Nemocniční informační systém FONS Enterprise (výrobce Stapro) | API není k dispozici | API rozhraní není k dispozici, je možné připravit v ceně dle skutečnosti v hodinové sazbě 1.890 Kč bez DPH.  Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 1.350 Kč bez DPH za hodinu. |
| Laboratorní systém OpenLims (výrobce Stapro) | API není k dispozici | API rozhraní není k dispozici, je možné připravit v ceně dle skutečnosti v hodinové sazbě 1.890 Kč bez DPH.  Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 1.350 Kč bez DPH za hodinu. |
| PACS - MARIE PACS (výrobce OR-CZ) | API je k dispozici | Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 1.200 Kč bez DPH |
| Groupware IceWarp Mail Server (výrobce IceWarp) | API je k dispozici | Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 2.500 Kč bez DPH za hodinu práce technika – juniora, 3.500 Kč bez DPH za hodinu práce technika – seniora. |
| Docházkový systém (výrobce IVAR) | API není k dispozici | API rozhraní není k dispozici, je možné připravit v ceně 160.000 Kč bez DPH, v případě uzavřené smlouvy o podpoře bude cena za přípravu 120.000 Kč bez DPH.  Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 1.100 Kč za hodinu, prvních 24 hodin implementačních prací je zahrnuto v ceně za tvorbu API rozhraní. |
| Personální systém Avensio (výrobce Alfa Software) | API není k dispozici | API rozhraní není k dispozici, je možné připravit v ceně 56.000 Kč bez DPH.  Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v hodinové sazbě 1.400 Kč bez DPH za hodinu. |
| Asset Management a Service Desk (Alvao) | K dispozici je API tvořené sadou WS (SOAP) | API rozhraní – cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v sazbě 12.000 Kč/člověkoden konzultantské práce a 16.000 Kč/člověkoden programátorské práce |

* + - 1. Zadavatel v souladu s § 96 odst. 2 ZZVZ poskytne dodavatelům popis API rozhraní informačních systémů podle předchozího odstavce na písemnou žádost a proti podpisu písemného čestného prohlášení dodavatele, že tento popis využije výhradně pro účely přípravy své nabídky na plnění předmětu této veřejné zakázky a s podmínkou, že případné zneužití popisu rozhraní nad rámec uvedeného účelu bude vůči dodavateli sankcionováno částkou 400 000,- Kč.

### Popis dokumentace

* + - 1. K provozování a řízení rozvoje ICT je využívána a udržována Provozní dokumentace ICT.
      2. Provozní dokumentace ICT popisuje základní nastavení technologií, hardwarových a softwarových systémů.
      3. Citlivé údaje (přístupové účty apod.) jsou uloženy odděleně od Provozních dokumentace ICT.
      4. Relevantní části dokumentace budou Uchazeči zpřístupněny až po podpisu Smlouvy o dílo k této zakázce.
      5. Uchazeč je povinen v rámci zakázky zajistit nezbytné doplnění Provozní dokumentace ICT reflektující provedené změny.

### Popis způsobu řešení incidentů

* + - 1. Zadavatel pro řešení incidentů a podporu uživatelů částečně využívá vlastní jednoduchý evidenční systém.
      2. Zadavatel zajišťuje podporu 1. úrovně a většinu běžných problémů jsou schopni vyřešit interní pracovníci Zadavatele.
      3. Incidenty a požadavky, které nevyřeší interní specialisté, jsou zadávány do helpdeskových systémů dodavatele systému, který vykazuje incident nebo na který směřuje požadavek uživatele. Hlášení incidentů a požadavků je prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.

### Popis servisních oken

Zadavatel nemá pevně definovaná pravidelná servisní okna. Aplikace aktualizací a oprav virtuálních serverů provádějí specialisté Zadavatele dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů.

## Povinné parametry technického řešení

### Obecné požadavky

* + - 1. Uchazeč v rámci zakázky navrhne:
         1. způsob nasazení a zavedení personálního a mzdového systému včetně převodu relevantních údajů ze stávajícího systému a napojení na související systémy.
         2. způsob nasazení a zavedení systému pro správu identit včetně propojení (integrace) s hlavními informačními systémy
         3. způsob nasazení a zavedení systému pro správu provozní (nezdravotní) dokumentace
      2. Uchazeč v rámci zakázky provede po schválení návrhů z předchozího bodu jejich realizaci.
      3. Zadavatel při výstavbě, správě a provozu ICT technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.
      4. Uchazeč ve své nabídce detailně popíše vazby na stávající systémy Zadavatele, které jsou nezbytné pro správné fungování řešení nabízeného Uchazečem.
      5. Pokud Uchazečem navržené řešení vyžaduje využití konkrétních softwarových produktů, neobsažených v popisu předmětu plnění, a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
      6. Pokud Uchazečem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, síťové prvky atp.) neobsaženou v popisu předmětu plnění, zahrne Uchazeč do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.
      7. Pro každý softwarový produkt, který Uchazeč nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.
      8. Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že Uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky-není přípustné implementovat např. další serverovou virtualizační platformu, adresářovou službu apod.
      9. Uchazeč bude při implementaci respektovat provozní řád Zadavatele, vítězný Uchazeč bude s provozním řádem seznámen před podpisem Smlouvy o dílo.
      10. Veškeré produkty, které Uchazeč dodává v rámci plnění Zadavateli, musí splňovat následující podmínky:
          1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
          2. mají plnou záruku od výrobce,
          3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
          4. obsahují všechny nezbytné licence na používání příslušného softwaru,
          5. jsou určeny pro provoz v České republice,
          6. z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti Uchazeč doloží čestným prohlášením výrobce/distributora, popř. Uchazečem samotným, nelze-li prohlášení distributora získat.

Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

* + - 1. Veškerá dokumentace vytvořená v rámci veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF) používaných Zadavatelem na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ICT ve formě vhodné pro použití administrátory v serverovně). Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena Zadavatelem.

### Specifické požadavky K1 – Správa identit

* + - 1. Systém pro správu identit (Identity management – IDM) bude koncipován jako ústřední systém správy ICT. Bude kopírovat organizační strukturu Zadavatele a umožní automatizaci úkonů spojených se správou identit v informačních systémech Zadavatele a zvýší úroveň kybernetické bezpečnosti.
      2. Automatizací správy identit dojde k odstranění nebo alespoň významnému omezení rutinních činností správců systémů spojených se správou identit a dále ke zrychlení reakcí na změny v organizace (např. změny oprávnění v systémech při změně pozice zaměstnance), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržením procesů (např. včasným nenahlášením odchodu zaměstnance všem správcům systémů nedojde včas nebo vůbec ke zrušení přístupových účtů zaměstnance) a získání okamžitého detailního přehledu o stavu identit a jejich oprávnění v systémech Zadavatele.
      3. Na IDM budou navázány hlavní informační systémy Zadavatele – personalistika, docházka, groupware, informační systémy NIS a PACS, systém pro správu požadavků, systém pro správu a evidenci majetku i nově pořizovaný systémy správy dokumentů. IDM tak vytvoří jeden autorizovaný zdroj informací ohledně uživatelů a jejich práv přístupů k jednotlivým systémům, tím bude současně provedena konsolidace identit, která je nezbytná pro realizaci budoucí uvažovaných projektů spojených s identitami – realizaci nařízení Evropské unie č. 910/2014 eIDAS o elektronické identifikaci a důvěryhodných službách pro elektronické transakce.
      4. IDM poskytne uživatelům základní službu „Přístup k systémům synchronizovaným s IDM“. Tato služba je realizována v procesech přístup do systému, přístup k aplikacím synchronizovaným s IDM apod. V případě, že jsou poskytovány aplikace externím subjektům, zajistí IDM přihlášení k aplikacím pro externí subjekty. V IDM budou vytvářeny role a těm se přidělovány oprávnění pro jednotlivé aplikace. Role budou naplňovány konkrétními uživateli. Tímto způsobem mohou být definovány role pro všechny zaměstnance a nový zaměstnanec automaticky při nástupu získá všechna potřebná oprávnění, a naopak při ukončení pracovního poměru bude zřejmé, že mu všechna přístupová práva byla odebrána.
      5. Součástí IDM bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).
      6. Implementace systému bude provedena v souladu s § 19 Nástroj pro řízení přístupových oprávnění Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

### Specifické požadavky K2 – Správa provozních dokumentů

* + - 1. Systém správy dokumentů (Document management system - DMS) bude navržen jako webový prostor (intranet) pro interní využití s důrazem na jednoduchost a rychlost použití, s možností dále toto řešení rozvíjet a dotvářet vlastními silami zadavatele.
      2. Systém vytvoří podmínky pro zavedení automatizovaného zpracování dokumentů a souvisejích procesů včetně jejich schvalování. Nativní vlastností řešení bude možnost parametrizace systému včetně tvorby wokflow – pro pozdější rozšiřování a úpravy systému.
      3. Systém umožní rychlé vyhledávání. Zadáním a potvrzením hledaného slova či fráze se prohledá uložená dat a zobrazí se relevantní výsledky.
      4. Systém bude využívat a poskytovat data ekonomickému systému HELIOS Green v rozsahu funkčnosti požadované povinnými parametry – viz. **3.5**
      5. Systém bude integrován se systémem K1 pro správu identit pro zajištění automatizace správy identit (uživatelských účtů) a stávajícm groupwarovým systémem tak, aby uživatelé byli informováni o svých úkolech (např. požadavek na schválení).

### Specifické požadavky K3 – Řízení virtuálních desktopů

* + - 1. Systém řízení virtuálních desktopů bude určen pro automatizaci a zrychlení přístupu vybraných uživatelů k jejich aplikacím.
      2. Systém umožní rychlé přihlašování uživatelů k virtuálním desktopům pomocí dvoufaktorového (volitelně vícefaktorového) ověření s využitím běžné bezkontaktní karty (faktory – „něco vlastním“ (např. kartu), „něco vím“ (např. pin). Systém musí umožnit ověřování uživatelů i pomocí běžné zabezpečené karty (Smartkarty) připojením odpovídající čtečky karet. Čtečky ani karty nejsou součástí dodávky.
      3. Systém umožní odhlášení uživatele nebo uzamčení či odpojení jeho relace opětovnou aktivací bezkontaktní karty, popř. deaktivací (vyjmutím) kontaktní karty.
      4. Systém umožní automatizovat spuštění uživatelských aplikací po přihlášení uživatele. Podle přihlášeného uživatele budou automaticky spuštěny předvolené aplikace a uživatel do nich bude automaticky přihlášen bez potřeby interakce uživatele. Uživatel tak pouhým přihlášením k virtuálnímu desktopu získá plně připravené a funkční pracovní prostředí rychle a bez prodlev způsobených ručním přihlašováním do aplikací.
      5. Systém umožní rychlou migraci uživatelů mezi pracovišti (tenkými klienty) – po ukončení práce na jednom pracovišti (tenkém klientu) potvrzeném aktivací karty dostane uživatel k dispozici pracovní prostředí na jiném pracovišti ve stejném stavu, jako jej opustil na předchozím pracovišti okamžitě po přihlášení kartou (bez opětovného spouštění aplikací) a to v řádu jednotek sekund.
      6. Systém bude možné implementovat i na fyzické počítače – desktopy.
      7. Systém lze realizovat jako samostatný s integrací (sdílení identit a profilů/politik) se stávajícím systémem pro single-sign-on a vícefaktorové ověřování nebo rozšířením stávajího systému pro single-sign-on a vícefaktorové ověřování.

### Popis povinných parametrů dodávaného řešení

* + - 1. V dále uvedené tabulce tabulkách jsou uvedeny minimální povinné parametry dodávaného řešení.

**Uchazeč musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena**

| **Komodita K1 - Správa identit** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Systém pro správu identity (Identity management - IDM)** | Základní funkce | Systém pro správu identit - Identity management (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi. |  |  |
| Licence | Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Minimální počet spravovaných uživatelů je 2100. |  |  |
| Škálovatelnost | Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. |  |  |
| Evidence aplikací a rolí | Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby. |  |  |
| Uživatelské role | Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS. |  |  |
| Historizace | Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti. |  |  |
| Automatizace | Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). |  |  |
| Logování SIEM | Systém bude poskytovat auditní logy ve formátu vhodném pro systém typu SIEM (Security Information and Event Management) |  |  |
| Logování systému | Systém obsahuje logování min. následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) |  |  |
| Správa identit | Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury. |  |  |
| Systematizovaná místa | Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. |  |  |
| Podpora eIDAS | Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. |  |  |
| Vysoká dostupnost | Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti. |  |  |
| Požadavky na portál - obecné | IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. |  |  |
| Podpora mobilních zařízení | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno) |  |  |
| Správa referenčních objektů | Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát. |  |  |
| Referenční objekty | Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity |  |  |
| Zabezpečení referenčních objektů | Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů |  |  |
| Rozšiřující atributy | Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM. |  |  |
| Přehledné zobrazení | Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit). |  |  |
| Vyhledávání - diakritika | Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.) |  |  |
| Správa certifikátů | Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti. |  |  |
| Obrázky | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie. |  |  |
| Přesun identit | Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními. |  |  |
| Kopírování rolí | Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy. |  |  |
| Ochrana proti chybám | Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). |  |  |
| Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem |  |  |
| Slučování identit | Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. |  |  |
| Export údajů | Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu |  |  |
| Filtrování | Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití. |  |  |
| Správa oprávnění | Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) |  |  |
| Granularita oprávnění | Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět. |  |  |
| Oprávnění k atributům | Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů. |  |  |
| Kontextový výběr | Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky. |  |  |
| Správa licencí | IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. |  |  |
| Časová omezení | IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere. |  |  |
| Vícenásobné vazby | Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. |  |  |
| Přehled rolí | Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role. |  |  |
| Přehled dědičností | IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu. |  |  |
| Skupiny | IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. |  |  |
| Zastupitelnost | IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta,…) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. |  |  |
| Delegování oprávnění | Možnost delegování administrátorských práv. |  |  |
| Správa osobních údajů | IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací. |  |  |
| Osobní údaje | IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům. |  |  |
| Osobní údaje - automatizace | IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů. |  |  |
| Obnovení hesla | IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu). |  |  |
| Žádosti | IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení. |  |  |
| Externí subjekty | IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin. |  |  |
| Kontextový výběr | Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. |  |  |
| Individualizace | IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně. |  |  |
| Workflow | Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele  - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění  - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů |  |  |
| Workflow - sledování | Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazní workflow např. aktivity diagram, BPMN nebo Archimate |  |  |
| Upozornění | IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. |  |  |
| Včasná upozornění | Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně. |  |  |
| Šablony upozornění | Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. |  |  |
| Kontext upozornění | Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd. |  |  |
| Logování | Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu. |  |  |
| Důvěryhodnost logování | Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. |  |  |
| Provozní stav | Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách - min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu workflow. |  |  |
| Auditní report | IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. |  |  |
| Auditní report - výběr | Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů. |  |  |
| Reporty uživatelů | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. |  |  |
| Reporty - zasílání | Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel. |  |  |
| Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. |  |  |
| Reporty - porovnání | Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. |  |  |
| Webové služby (WS) | IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. |  |  |
| Standardy WS | Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. |  |  |
| Bezpečnost WS | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. |  |  |
| Logování WS | Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu |  |  |
| Služby rozhraní WS | Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu funkcí / rolí  - Získání seznamu uživatelů dané aplikace - Získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci - Zápis seznamu funkcí do IDM - Zápis certifikátů do IDM - Zápis a změna identit |  |  |
| Synchronizace | Ruční i automatické spuštění synchronizací s propojenými systémy. |  |  |
| Synchronizace - simulace | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. |  |  |
| Simulace - průběh | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. |  |  |
| Synchronizace - režimy | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému):  - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému  - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.  - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.  - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.  - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka.  - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. |  |  |
| Synchronizace - správa | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu. |  |  |
| Obecné konektory | Vestavěné obecné konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP a REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3 |  |  |
| Speciální konektory | IDM bude obsahovat konektor umožňující správu virtuálních aplikací. Požadavky na správu identit ve virtuálních aplikacích bude IDM předávat e-mailem správcům odpovídajících reálných aplikací. Správci potvrdí splnění požadavku zpět do IDM. Uvedeným systémem budou řízeny identity v aplikacích, které nelze nebo není ekonomicky efektivní integrovat s IDM pomocí obecných nebo aplikačních konektorů. |  |  |
| Aplikační konektory | IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně souvisejících operací potřebných pro plnou automatizaci správy identit v daném systému (např. řízení členství ve skupinách, přiřazení rolí, správa metadat): - Microsoft Active Directory - ekonomický systém Helios Green (Asseco) - NIS tj. nemocniční informační systém) Fons Enterprise (Stapro) - Laboratorní systém OpenLims (Stapro) - PACS - MARIE PACS (OR-CZ) - groupware IceWarp Mail Server, včetně vytváření schránek (IceWarp)  - docházkový systém (IVAR) - Service desk (Alvao) - Asset management (Alvao) - DMS - Komodita K2 |  |  |
| Zdrojový systém | IDM bude napojeno na personální systém Avensio (Alfa software). Z personálního systému budou načítány údaje o organizační struktuře, pracovních místech a funkcích, osobách a tyto údaje budou pro IDM sloužit jako zdrojové |  |  |
| Záruka | Min. 12 měsíců včetně nároku na opravné verze |  |  |

| **Komodita K2 - Správa provozních dokumentů** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Systém pro správu dokumentů** | Základní funkce | DMS systém (Document management systém - dále jen DMS nebo systém) - systém koncipovaný jako portál dostupný prostřednictvím webového prohlížeče, obsahující dále uvedené aplikace či moduly a funkce. |  |  |
| **Aplikace - moduly** | | | |
| Smlouvy | Obsahuje podklady o smluvních vztazích s partnery tj. smlouvy a související dokumenty např. přílohy. Aplikace bude primárně určená pro evidenci a schvalování smluv s externími partnery. |  |  |
| Likvidace majetku | Podpora procesu vyřazení a likvidace majetku od vytvoření požadavku přes odeslání oprávněným schvalovatelům, schválení požadavku a potvrzení likvidace. |  |  |
| Schvalování objednávek | Podpora procesu schvalování objednávek nákupu zboží či služeb včetně schvalování. |  |  |
| **Funkční požadavky a požadované vlastnosti modulu Smlouvy** | | | |
| Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, předmět smlouvy, protistranu, způsob financování, lokalitu, finanční objem, způsob schvalování, dotčená oddělení, předkladatele a přílohy. |  |  |
| Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle vyplnění finančního objemu. Min. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. |  |  |
| Výstup | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku (v rozsahu viz. Vytvoření požadavku) a jeho schválení (schvalovatelé, data schválení, komentáře). |  |  |
| **Funkční požadavky a požadované vlastnosti modulu Likvidace majetku** | | | |
| Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, předmět(y) likvidace (včetně inventárního čísla, popisu, počtu, data pořízení, umístění apod.), lokalitu, dotčená oddělení a střediska, typ likvidace, způsob schvalování, předkladatele a přílohy. |  |  |
| Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu dle způsobu likvidace. Min. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. |  |  |
| Výstup | Po schválení bude automaticky vygenerován PDF soubor a uložen do deníku požadavky, obsahující informace o požadavku (v rozsahu viz. Vytvoření požadavku), stanoviscích schvalovatelů (komise), rozhodnutí a potvrzení o provedení likvidace. |  |  |
| **Funkční požadavky a požadované vlastnosti modulu Schvalování objednávek** | | | |
| Vytvoření požadavku | Prostřednictvím upravitelného formuláře obsahujícího minimálně datum požadavku, dodavatele, předmět(y) objednávky (včetně popisu, počtu, ceny, dodací lhůty), lokalitu, dotčená oddělení a střediska, žadatele a přílohy. |  |  |
| Schvalování | Automatické spuštění po zadání požadavku. Automatický výběr schvalovacího procesu ceny. Min. 5 schvalovacích schémat. Každé schéma obsahuje jeden schvalovací krok, který obsahuje skupinu uživatelů z AD, kteří mohou schválení provést. |  |  |
| Výstup | Po schválení bude dostupný příkaz pro vygenerování PDF souboru obsahující informace o požadavku (v rozsahu viz. Vytvoření požadavku) a jeho schválení (schvalovatelé, data schválení, komentáře). |  |  |
| **Společné požadavky** | | | |
| Lokalizace | Lokalizované uživatelské rozhraní |  |  |
| Zabezpečený přístup | Zabezpečený přístup do aplikace včetně integrovaného přihlašování do uživatelského prostředí i konzol prostřednictvím účtu Active Directory, řízení oprávnění přístupu k informacím. |  |  |
| Active Directory | Automatické načítání vztahu zaměstnance a jeho nadřízeného. |  |  |
| Uživatelská přívětivost | Intuitivní grafické rozhraní - prostředí bude odpovídat moderním trendům a zvyklostem - přehlednost, rychlá orientace bez nutnosti čtení textů, využití piktogramů či ikon, kontextové nápovědy. Vhodné pro použití na mobilních (dotykových) zařízeních. |  |  |
| Integrace | Integrace s HELIOS Green pro získávání potřebných údajů (např. o majetku dle inventárního čísla) v rozsahu funkcí API HELIOS Green. Automatizace a usnadnění práce uživatelů při vyplňování požadavků, prevence chybných zadání. |  |  |
| API | Systém musí umožnit rozšíření funkcí a ovládání pomocí otevřeného rozhraní API |  |  |
| Licence | Min. pro 1200 uživatelů pracujících na 750 koncových zařízení. |  |  |
| Vyhledávání | Fulltextové vyhledávání napříč požadavky |  |  |
| Záruka | Min.12 měsíců včetně nároku na opravné verze |  |  |

| **Komodita K3 - Systém pro řízení virtuálních desktopů** | | | | |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Ověřovací platforma** | Obecné požadavky | Platforma pro zajištění centrálních (serverových) služeb vícefaktorového a jednotného (SSO - single sing-on) ověřování |  |  |
| Klientské systémy | Podpora desktopových a serverových Windows OS (verze 7/2008 a vyšší) a Linuxu |  |  |
| Vysoká dostupnost | Vysoce dostupná architektura z minimálně 2 automaticky zastupitelných prvků (cluster apod.) s jednotnou správou celého řešení |  |  |
| Virtualizace | Podpora provozu ve virtuálním prostředí nabízené serverové virtualizace |  |  |
| Bezpečnost | Ověřování administrátorských účtů vůči Active Directory |  |  |
| Adresářové služby | Podpora běžných adresářových služeb - Active Directory, NetWare NDS/eDirectory |  |  |
| Bezpečná komunikace | Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba apod.) je šifrována (SSL či kompatibilní) |  |  |
| Licence | Min. pro 1200 uživatelů |  |  |
| Záruka | Záruka včetně nároku na opravné verze min. 12 měsíců. |  |  |
| **Vícefaktorové ověřování** | Obecné požadavky | Zajištění ověření uživatele pro přihlášení k pracovní stanici (PC nebo tenký klient) s využitím více faktorů |  |  |
| Ověřovací metody | Podpora autentizačních předmětů (kontaktní čipové karty, bezkontaktní karty, USB a bezkontaktní tokeny), biometrických prvků (otisk prstu), kombinace jméno/heslo (s vazbou i bez vazby na Active Directory), PINu a jejich vzájemných kombinací. |  |  |
| Dynamické ověřování | Podpora konfigurace podmínek pro využití vícefaktorového ověřování - např. dvoufaktorové ověřování povinné jen při prvním přihlášení v daném dni (pro další přihlášení postačí jeden faktor) apod. |  |  |
| Virtualizované aplikace a desktopy | "Bezešvá" integrace přihlašovacího procesu bez nutnosti opakovaně zadávat přihlašovací údaje a potvrzovat připojovací dialogy s nejběžnějšími produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix XenApp/XenDesktop) |  |  |
| Tencí klienti | Podpora náhrady běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování |  |  |
| Scénáře | Podporované scénáře použití "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi". Koncovou stanicí může být tenký klient i běžný počítač s OS Windows/Linux. |  |  |
| Licence | Min. pro 1200 uživatelů |  |  |
| Záruka | Záruka včetně nároku na opravné verze min. 12 měsíců. |  |  |
| **Jednotné přihlašování** | Obecné požadavky | Podpora jednotného (SSO) automatického přihlášení uživatele do libovolných desktopových aplikací včetně jejich automatického spuštění pro přihlášení do operačního systému. |  |  |
| Podporované aplikace | Podpora SSO do různých typů aplikací - Win aplikace, webové aplikace včetně Java aplikací, terminálové aplikace používající znakové rozhraní apod. Funkčnost nesmí vyžadovat úpravu aplikací. |  |  |
| Bezpečnost | Přihlašovací údaje do aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje musí být ukládány v ověřovací platformě a být centrálně dostupné na libovolném koncovém zařízení (počítač, tenký klient) v síti. |  |  |
| Profily | Intuitivní podpora vytváření a správu předpisů (profilů) pro jednotlivé aplikace (bez psaní kódu, používání řádkových příkazů apod.). Vytvořené předpisy (profily) aplikací musí být možné přidělovat uživatelům na základě členství v Active Directory skupinách. |  |  |
| Licence | Min. pro 1200 uživatelů |  |  |
| Záruka | Záruka včetně nároku na opravné verze min. 12 měsíců. |  |  |

### Požadavky na architekturu technického řešení

* + - 1. Architektura komodit musí být navržena tak, aby vhodně využívala a doplňovala stávající prostředky.
      2. Architektura komodit K1 a K2 bude implementována jako třívrstvá (prezenční, aplikační a datové vrstva) s tenkým klientem – internetovým prohlížečem.
      3. Aplikační a datovou vrstvu architektury komodity K1 bude možné implementovat jako vysoce dostupnou (redundantní) včetně možnosti rozkládání zátěže na jednotlivé prvky vrstvy. Případné rozšiřující licence nejsou součástí zakázky.
      4. Architektura komodit bude využívat jednotnou společnou datovou základnu (databázový stroj)

### Požadavky na integraci

* + - 1. Systémy komodit K1 a K2 budou integrovány se stávajícím systémem Active Directory a podporovat jednotné přihlašování SSO (Single sign on) pro rychlé přihlášení a přístup uživatelů.

### Požadavky na rozhraní

* + - 1. Řešení komodity K1 a K2 musí disponovat dokumentovaným, programovým aplikačním rozhraním – API, které bude součástí dodávky včetně dokumentace.
      2. Veškerá uživatelské rozhraní a rozhraní pro běžnou správu a konfiguraci systémů komodit K1 a K2 budou v českém jazyce.

### Požadavky na kompatibilitu s ostatními systémy

* + - 1. Veškeré serverové softwarové komponenty nabízených řešení budou provozovány ve virtuálním prostředí serverové virtualizace Hyper-V a musí být pro běh v těchto prostředí výrobcem podporovány.
      2. Veškeré serverové softwarové komponenty komodit K1 a K2 budou z důvodu jednotné správy a zálohování provozovány v prostředí Microsoft Windows Server a musí být pro běh v těchto prostředí výrobcem podporovány. Potřebné licence Windows Server zajistí Zadavatele a nejsou předmětem této zakázky.

### Požadavky na typy klientů

* + - 1. Klienti systémů dodaných v rámci předmětu plnění musí být podporováni v prostředí aplikační virtualizace MS RDS (Remote desktop services) a v prostředí operačních systémů Windows 7 a vyšší.
      2. Webová rozhraní nabízených komodity musí být funkční v obvyklých internetových prohlížečích – min. Internet Explorer, Edge, Chrome, Firefox, Safari v aktuálních verzích.

### Požadavky na bezpečnost informací

* + - 1. Bezpečnost interní i externí komunikace webových rozhraní řešení všech komodit musí být možno zajistit použitím šifrování (např. SSL) odpovídajícího protokolu (např. HTTPS)

### Požadavky na dokumentaci

* + - 1. Součástí komodity K1 bude podrobná příručka v českém jazyce pro uživatele i správce (administrátory) detailně a názorně popisující užívání systému a jeho správu včetně změn konfigurace (vytváření/změna workflow, reporty apod.).

## Hodnocené parametry technického řešení

### Požadavky na vlastnosti technického řešení

* + - 1. Zadavatel požaduje kromě splnění minimálních povinných parametrů také další funkční vlastnosti nabízeného řešení. Na rozdíl od povinných parametrů není uchazeč při nesplnění některého z požadovaného hodnoceného parametru vyloučen. Způsob hodnocení je uveden v ZD.

|  |  |  |  |
| --- | --- | --- | --- |
| **Hodnocené parametry** | | | |
| **Parametr** | **Popis** | **Uchazeč popíše způsob naplnění tohoto hodnoceného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Snížení nároků na správu systému** | | | |
| 1 | Z důvodu zachování jednotné datové základny, její správy a zálohování budou systémy komodit K1 a K2 využívat pro ukládání dat databázový server MS SQL server |  |  |
| **Uživatelské přívětivost a snížení nároků na správu** | | | |
| 2 | Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K1 bude v českém jazyce |  |  |
| **Integrace s MS Outlook - Komodita K2** | | | |
| 3 | Systém bude integrován s MS Outlook (2010 a vyšší). Integrací se rozumí rozšíření prvků MS Outlook (ribbon – pás karet, formuláře a jejich ovládací prvky) o možnost správy požadavků přímo v prostředí MS Outlook. |  |  |

## Implementační služby

### Obecné požadavky

* + - 1. Zadavatel požaduje provést minimálně následující implementační práce. Uchazeč je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.
      2. V rámci implementace předmětu plnění Uchazeč realizuje následující služby:
         1. Zajištění projektového vedení realizace předmětu plnění.
         2. Provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Výstupem bude prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Prováděcí dokumentace musí být připravena před zahájením realizace dodávek, tzn. po provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu a musí být výslovně schválena Zadavatelem.
         3. Dodávka a implementace nabízených předmětu plnění splňující povinné parametry technického řešení a zajištění technické podpory.
         4. Zpracování provozní dokumentace implementovaného systému v rozsahu popisu implementovaných funkcionalit a popisu činností běžné údržby a administrace systémů. Dokumentace může být poskytnuta i formou lokalizované (české) vestavěné nebo online nápověda či příručky.
         5. Provedení školení,
         6. Zajištění zkušebního provozu,
         7. Provedení akceptačních testů,
         8. Předání do ostrého provozu,
      3. Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují (nevyčísluje se zvlášť).
      4. Uchazeč dle svého uvážení může doplnit v nabídce další služby, které jsou dle jeho názoru potřebné pro úspěšnou realizaci zakázky.
      5. Činnost omezující práci uživatelů musí být prováděny mimo běžnou pracovní KKN, tj. mimo pracovní dny 7:00–15:30 hod.
      6. Uchazeč je dále povinen zahrnout do nabídky další specifické služby a požadavky (k výše uvedeným v čl. 4 a 5) specifikované v následujících tabulkách:

|  |
| --- |
| K1: Správa identit |
| * 1. Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu:      1. analýzu procesů a aplikací KKN se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,      2. analýzu požadavků KKN zasílaných informačním systémům s požadavkem na autorizaci a autentizaci,      3. technologický popis stávajících technologií s vazbou na systém správy identit      4. analýzu možností správy výstupních struktur,      5. analýzu evidenčních údajů a logů,      6. návrh životního cyklu identity uživatelů,      7. model organizační struktury,      8. seznam systemizovaných pracovních pozic,      9. přiřazení pracovníků k pracovním pozicím,      10. atributy poskytované personálním systémem v souladu s potřebami obsluhovaných systémů a návrh jejich využití,      11. manažerský souhrn vhodný pro prezentaci výstupů analýzy vedení KKN.   2. Návrh a realizace konfiguračních změn infrastruktury   3. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a prokázat plnou funkčnost integrací v obvyklých scénářích použití. |

| K2: Správa provozních dokumentů |
| --- |
| * 1. Analýza dokumentů a procesů relevantních pro implementaci požadovaných aplikací - modulů   2. Návrh vhodných datových struktur, kategorií a metadat, přístupových oprávnění a rolí včetně skupin,   3. Návrh a realizace vstupních, stavových a výstupnách formulářů a dokumentů požadavků   4. Analýza funkcionalit API HELIOS Green a realizace potřebných datových importů a/nebo dotazů.   5. Návrh vhodných pracovních postupů (workflow).   6. Implementace systému dle provedených návrhů a doporučení výrobce   7. Návrh a realizace konfiguračních změn infrastruktury   8. Návrh a provedení akceptačních testů |

| K3: Systém pro řízení virtuálních desktopů |
| --- |
| * 1. Návrh systému pro vícefaktorové ověřování uživatelů včetně vhodných politik   2. Návrh začlenění vícefaktorového ověřování uživatelů do prostředí aplikační virtualizace – k dispozici bude vícefaktorové i běžné (jméno, heslo) ověřování   3. Návrh vhodných aplikačních sad pro vybrané uživatelské role a způsob jejich spuštění a automatického přihlašování   4. Návrh způsobu realizace požadovaných scénářů "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi"   5. Implementace systému dle provedených návrhů a doporučení výrobce   6. Návrh a provedení akceptačních testů |

### Požadavky na zpracování prováděcí dokumentace

* + - 1. Uchazeč před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.
      2. Jako podklad pro zpracování prováděcí dokumentace provede uchazeč předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, minimálně pro následující oblasti:
         1. Stávající stav (vstupy) relevantní pro návrh implementace komodity.
         2. Způsob začlenění nabízených komodit do stávajícího prostředí.
         3. Konfigurační změny nabízeného systému potřebné pro naplnění povinných požadavků.
         4. Virtualizační infrastruktura (serverová, síťová, disková i aplikační) ve vztahu k plánovanému využití.
         5. Integrace nabízených softwarových systémů.
         6. Požadované součinnosti Zadavatele a jejich rozsah.
         7. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.
      3. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a musí obsahovat minimálně tyto části:
         1. Popis cílového stavu / konfigurace nabízeného systému,
         2. Detailní harmonogram realizace včetně uvedení kritických milníků,
         3. Vazby na integrované systémy systémy,
         4. Návrh akceptačních kritérií a akceptačních testů.
      4. Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně schválena zadavatelem.

### Harmonogram realizace

* + - 1. Uchazeč zajistí projektové vedení po celou dobu realizace zakázky projektovým manažerem. Součástí nabídky bude popis metodiky, která bude pro projektové řízení použita.
      2. Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo. Čísla značí počet kalendářních dnů.

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Etapa projektu – činnost** | **Zahájení etapy** | **Ukončení etapy** |
| 1 | Předimplementační analýza a zhotovení Prováděcí dokumentace včetně vypořádání připomínek a akceptace Zadavatelem | D | D+40 |
| 2 | Dodávky a implementace | D+40 | D+100 |
| 3 | Školení administrátorů | D+80 | D+110 |
| 4 | Zkušební provoz | D+90 | D+100 |
| 5 | Akceptační testy | D+100 | D+110 |
| 6 | Zahájení plného provozu | D+110 | - |

* + - 1. Uchazeč může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
      2. Maximální lhůty trvání nesmí Uchazeč při tvorbě detailního harmonogramu prodloužit.
      3. Uchazeč uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy o dílo.
      4. Uchazeč uvede potřebnou součinnost Zadavatele pro splnění harmonogramu plnění ve své nabídce.

### Požadavky na školení

* + - 1. Uchazeč zajistí školení pracovníků Zadavatele – administrátorů– na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace ICT a uživatelských příruček k jednotlivým komoditám.
      2. Školení zajistí seznámení administrátorů Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin. Minimální rozsah školení pro administrátory je:
         1. 8 hodin pro komoditu K1
         2. 4 hodiny pro komoditu K2
         3. 4 hodiny pro komoditu K3
      3. Školení bude probíhat v sídle Zadavatele.
      4. Předpokládá se účast max. 5 administrátorů.
      5. Náklady na školení administrátorů musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

### Požadavky na testovací prostředí

* + - 1. Zadavatel nedisponuje testovacím prostředím.
      2. Vyžaduje-li Uchazeč pro realizaci zakázky testovací prostředí, zahrne do nabídky náklady na jeho vybudování a požadovanou součinnost Zadavatele.

### Požadavky na provedení akceptačních testů, zkušební provoz a přechod do ostrého provozu

* + - 1. Uchazeč navrhne způsob a provedení akceptačních testů.
      2. Součástí akceptačních testů musí být pro každou komoditu minimálně:
         1. Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.
         2. Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
         3. Prokázání přiměřených odezev systému při náročnějších operacích
         4. Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
      3. Pro každou komoditu navrhne Uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení.
      4. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
      5. Uchazeč zajistí zkušební provozu v délce minimálně 10 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
      6. Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.

## Záruky a servisní podmínky

* + - 1. Zadavatel požaduje záruku na veškeré dodané služby v délce trvání minimálně 3 měsíců a zařízení minimálně 24 měsíců (není-li u konkrétní komodity uvedeno jinak) od okamžiku ukončení implementace a předání do produkčního provozu.
      2. Není-li u konkrétní komodity uvedeno jinak, požaduje Zadavatel provedení záruční opravy do 5-ti pracovních dnů nebo poskytnutí náhradního prvku shodných nebo lepších parametrů po dobu opravy.
      3. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.
      4. Uchazeč ve své nabídce výslovně uvede všechny podmínky záruk.
      5. Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
      6. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro Zadavatele.
      7. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
      8. Pro hlášení servisní požadavků zajistí Uchazeč Zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 7-17 hod. v pracovních dnech.

## Požadavky na zabezpečení provozu

* + - 1. Zadavatel požaduje detailní návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění včetně vazeb na stávající technologie od doby předání do plného provozu. Uchazeč podle svého uvážení může provést úpravu parametrů, pokud takové úpravy nepovedou ke zhoršení podmínek zajištění podpory provozu.

### Definice

* + - 1. **24x7** – služba nebo zařízení je v provozu/dostupné 24 hodin a 7 dní v týdnu s garancí minimálně 95% dostupnosti
      2. **9x5** - služba nebo zařízení je v provozu/dostupné 9 hodin denně v běžnou pracovní dobu po všechny pracovní dni v týdnu s garancí minimálně 95% dostupnosti
      3. **BD** – Business Day – standartní pracovní den
      4. **BE (Best Effort)** - Uchazeč vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů Prvku IT v nejkratší možné době.
      5. **Bezpečnostní incident -** stav nebo událost, která je v rozporu interní směrnicí Zadavatele související s provozem ICT nebo událost, která způsobila nehodu nebo potenciálně mohla způsobit omezení případně nefunkčnost ICT. Zahrnuje též kybernetické bezpečnostní incidenty - kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
      6. **Běžná pracovní doba** – čas mezi 8:00 a 17:00 v Pracovní dny.
      7. **Člověkohodina** - práce pracovníka Uchazeče v rozsahu jedné (1) hodiny v rámci Pracovního dne.
      8. **Člověkoden** - práce pracovníka Uchazeče v rozsahu jednoho (1) Pracovního dne.
      9. **Doba odezvy (Response time – R)** – metrika definující čas, který uplyne od nahlášení Požadavku na Servisní službu do začátku provádění Servisní služby. Do Doby odezvy se započítává pouze čas, určený Servisním kalendářem k řešení daného Požadavku. Za odezvu se považuje jakákoliv prokazatelná reakce servisního pracovníka Uchazeč směřující k odstranění Incidentu, zodpovězení Dotazu nebo přípravy Nového požadavku.
      10. **Dotaz** – funkce v systému existuje, Prvek IT pracuje v souladu s Prováděcí dokumentací, ale pověřená osoba zákazníka s ní není dostatečně seznámena a podá Požadavek - Dotaz na Hot-line nebo HelpDesk
      11. **HelpDesk** – nepřetržitě dostupný automatizovaný systém pro vzdálené zadávání a správu požadavků,
      12. **Hot-line** –pracoviště Uchazeče přijímající Požadavky od Zadavatele na definovaných telefonních číslech nebo elektronických komunikačních kanálech.
      13. **Odborná podpora** – konzultace, technická pomoc
      14. **Incident**- událost způsobující odchylku od očekávané funkce Prvku IT, která způsobuje nebo může způsobit přerušení anebo snížení kvality této funkce.
      15. **Priorita Incidentu** - závažnost Incidentu dle klasifikace Kontaktní osoby Zadavatele.
      16. **Koncová zařízení** - počítače uživatelů, jejich základní programové vybavení a periferní zařízení k počítačům připojená (např. tiskárny, skenery).
      17. **Monitorování –** jedná se o službu nepřetržitého online monitorování systémů s upozorněním na kritické nebo neobvyklé události a provozní hodnoty Prvků IT, upozornění budou automaticky zasílána oprávněným pracovníkům Zadavatele. Součástí služby je vzdálený přístup k aktuálním i historickým údajům o stavu systému.
      18. **Proaktivní monitorování** - monitorování prováděné dle charakteru provozu a činnosti Prvků IT v režimu 9x5. Při zjištění Incidentu je monitorovacím systém a/nebo manuálně pracovníkem Uchazeče založen Požadavek a zahájeno jeho řešení podle kategorie Incidentu
      19. **Náhradní zařízení** – zařízení podobných vlastností (parametrů).
      20. **Požadavek** - žádost o provedení Servisní služby na jednom nebo více Prvcích IT.

Požadavek může zahrnovat:

* + - * 1. žádost o odstranění závady (nefunkční Prvek IT nebo nesprávná činnost Prvku IT) - Incidentu
        2. žádost o poskytnutí konzultace
        3. žádost o provedení Změny

Požadavek může:

* + - * 1. být zadán Zadavatelem jako jednorázový
        2. být zadán Zadavatelem jako opakující se činnost
        3. vzniknout jako výstup Monitorování
        4. vzniknout na základě Správy a údržby Prvku IT
      1. **NBD**-**Next Business Day** – následující pracovní den
      2. **Neprodleně** – bez zbytečného odkladu, s vyvinutím maximálního úsilí na zjednání nápravy nebo zajištění činnosti, nejpozději však následující Pracovní den.
      3. **Pracovní dny** - všechny dny, kromě sobot a nedělí nebo zákonem stanovených svátků a dnů pracovního klidu, během nichž dohodnuté pracovní činnosti budou prováděny v čase od 8:00 do 17:00 hodin.
      4. **Prvek IT** - zařízení (Koncové zařízení, server či jiný hardware), program (software) nebo komunikační linka.
      5. **Rozsah poskytovaných služeb** – specifikace Služby a kvantifikace rozsahu Služby
      6. **Řešitel** - pracovník Uchazeče, podílející se na řešení Požadavku.
      7. **Report** – přehledový dokument, ve kterém je popsán průběh realizace Plnění za uplynulé období a hodnoty sledovaných parametrů.
      8. **SLA (Service Level Agreement)** - definice kvalitativních parametrů/metrik Služby
      9. **Správa a údržba** - provádění činností, které jsou nutné ke správné a bezchybné funkci Prvku IT. Zpravidla se jedná o pravidelnou kontrolu stavu Prvků IT a provádění takových Změn, které se pravidelně opakují, nebo jsou provedeny na základě kontroly stavu Prvku IT.
      10. **Služby** – činnosti potřebné pro řádné zabezpečení podpory provozu předmětu plnění.
      11. **Úplné odstranění závady** - se rozumí dosažení stavu, který byl akceptován v rámci smlouvy o dílo nebo je popsán v prováděcí dokumentaci popř. v dokumentaci Prvku IT.
      12. **Vzdálená správa** – provádění činností na Prvcích IT, přičemž činnosti nejsou prováděny v místě provozovny Zadavatele, ale prostřednictvím Vzdáleného přístupu z místa provozovny Uchazeče.
      13. **Vzdálený přístup** – připojení z provozovny Uchazeče k zařízení Zadavatele pomocí komunikační linky, na které je vytvořeno dočasné nebo trvalé spojení.
      14. **Zprovoznění náhradním způsobem** - se rozumí zajištění základních funkcí systému, tedy dosažení stavu, kdy není vážně omezena funkčnost informačního systému nebo jeho částí.
      15. **Změna** - změna parametrů Prvku IT nebo instalace, přemístění či odinstalace Prvku IT.
      16. **Legislativní servis -** legislativním servisem se rozumí úprava stávající funkčnosti stávajícího systému (software), kterou je nutné provést, protože stávající funkcionalita by nutila zákazníka konat v rozporu s novou legislativní úpravou. Legislativní úpravou v žádném případě není doplnění funkcionality (řešené oblasti), kterou stávající systém (software) nepokrýval.
      17. **Reklamace -** reklamací je požadavek vznesený na přezkoumání a odstranění vlastnosti Prvku IT v čase záruční doby, která je v rozporu:
          1. se standardní funkčností Prvku IT a tento rozpor je vůči uživatelské dokumentaci produktu,
          2. s funkcionalitou definovanou ve smlouvě (jejích přílohách), případně akceptačním protokolu funkcionality Prvku IT,
          3. s platnou legislativou ČR k datu podání požadavku.
      18. **Konfigurační management** - jde o službu poskytovanou za účelem udržení aktuální technické dokumentace. V případě jakékoliv provedené změny, bude aktualizována provozní dokumentace ICT o konfiguraci systému včetně zaznamenaných změn. Dokumentace bude uložena u Uchazeče i Zadavatele. Poskytuje informace o Prvcích IT a službách včetně informací o aktuálních verzích. Zahrnuje rovněž správu veškeré dokumentace ke všem prvkům infrastruktury a služeb. Obvykle je využíván automatizovaný nástroj pro sběr a aktualizaci většiny údajů v konfigurační databázi.
      19. **Patch Management -** jedná se o preventivní činnost týkající se především operačních systémů a instalace opravných balíčků, kde hlavním cílem je udržet systém v aktuálním stavu a s nainstalovanými aktuálními softwarovými komponentami.
      20. **Hotline podpora** - jde oslužbu zajišťující poradenství po telefonu nebo elektronické komunikaci
      21. **Maintenance –** jedná se o zajištěnínových a opravných verzí software (včetně hlavních verzí), nových verzí firmware, přístupu k technické podpoře výrobcea přístupu k databázi řešených problémů.
      22. **Profylaxe -** profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.

### Obecná pravidla provozu

* + - 1. Provozem se rozumí chod a udržování jednotlivých částí řešení, tj. hardware, systémový software, vybrané aplikace, technické infrastruktury, aktuální dokumentace.
      2. Informační systémy Zadavatele jsou provozovány v nepřetržitém provozu s výjimkou neočekávaných událostí a plánovaných odstávek.
      3. Veškeré technologie jsou umístěny v technologických místnostech KKN. Fyzický přístup do technologických místností je řízen interní směrnicí. Vstup je zajištěn uzamčením místnosti standardním zámkem či elektronickým zámkem. Pravidla přístupu budou vítěznému Uchazeči předána při podpisu smlouvy.
      4. Pravidelné profylaktické prohlídky probíhají v souladu s harmonogramem plánovaných profylaxí a odstávek, který je sestavován v rámci poskytování konkrétních služeb a je pravidelně předkládán ke schválení oprávněné osobě Zadavatele.
      5. Zásahy, které musí být provedeny mimo dobu profylaxe, jsou přednostně prováděny mimo provozní dobu příslušné služby. O nutnosti zásahů v provozní době služby rozhoduje projektový manažer Uchazeče a 48 hodin předem o nich informuje uživatele. Pokud je nevyhnutelně nutné provést zásah okamžitě, operátor Helpdesku a vedoucí OIT KKN jsou o této skutečnosti neprodleně informováni.
      6. Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.
      7. Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti.

### Harmonogram poskytování služeb

* + - 1. V průběhu poskytování služeb je Uchazeč povinen sestavovat harmonogram plánu poskytovaných služeb a činností. Harmonogram bude připravován vždy na dobu nejméně 3 měsíců dopředu.
      2. Harmonogram bude obsahovat časový rozvrh služeb a činností, případně jejich částí, které mají pravidelný charakter (profylaxe, údržba apod.), případně které jsou předvídatelné (instalace patchů, upgradů atd.).
      3. Všechny provozní činnosti musí být přednostně prováděny v době minimální zátěže dotčených systémů.

### Specifikace rozsahu požadované podpory provozu

* + - 1. Základní rozsah systémové podpory v rámci měsíčního paušálu:
         1. Pravidelné servisní prohlídky a revize předepsané výrobci
         2. Průběžné monitorování Prvků IT pokrývaných touto smlouvou, popř. dalších Prvků IT, které mohou ovlivnit jejich chod a které byly identifikovány v rámci předimplementační analýzy. Počet sledovaných parametrů nesmí být prakticky omezen, administrátoři KKN musí mít přístup ke sledovaným parametrům alespoň v režimu čtení.
         3. Řešení Incidentů dle podmínek SLA
         4. Profylaxe a patch management
         5. Hotline podpora v režimu 9x5
         6. Odborná podpora v režimu 9x5
         7. Celkový rozsah služeb Hotline podpora a Odborná podpora v rámci měsíčního paušálu je 6 hodin ve složení - 2 hodiny pro každou Komoditu (celkem 6 hodin).
         8. Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
         9. Servisní dispečink pro telefonické zadávání požadavků dostupný v pracovní dny 8 -17 hod.
      2. Pro případ, že bude Zadavatel požadovat služby Hotline podpory nebo Odborné podpory podle odstavců (1)(e) a (1)(f) (např. konzultace, servisní zásahy, instalace, konfigurace, řešení problémů atp.) nad rámec uvedeného rozsahu služeb zahrnutých v měsíčním paušálu - viz. (1)(g), budou tyto služby hrazeny na základě počtu hodin realizovaných služeb dle hodinové sazby, Uchazeč nacení tyto služby v položkovém rozpočtu ve formě hodinové sazby za služby (označení služby „EXP-WRK“).
      3. Seznam prvků pokrývaných službou zabezpečení provoze je uveden v kapitole 7.11.
      4. Detailní specifikace požadavků a jejich rozsah pro jednotlivé kategorie prvků IT jsou v katalogových listech, v Části 3b Zadávací dokumentace.

### Předávání informací o poskytované službě (reporting)

* + - 1. Uchazeč zpracuje a poskytne Zadavateli každý měsíc souhrn informací o poskytovaných službách (report), ve kterém je popsán průběh realizace plnění za uplynulé období, včetně přehledu dodržování SLA parametrů, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti a dostupnosti systémů a prevenci incidentů.
      2. Souhrn informací o poskytovaných službách (report) bude obsahovat informace o jednotlivých službách a jejich provádění (dle povahy jednotlivých služeb a definice dle katalogových listů služeb).
      3. Měsíční report bude vyhotovován výhradně v elektronické formě a bude obsahovat souhrn činností provedených za vykazované období.
      4. Report bude za příslušné období vždy obsahovat minimálně:
  1. Informace o provedených změnách na Prvcích IT spojených s poskytováním služby.
  2. Informace o bezpečnostních incidentech zjištěných v souvislosti s poskytováním služby.
  3. Požadavek na součinnosti Zadavatele, požadované Uchazečem, k tomu, aby mohl dostát svým závazkům v poskytování předmětné služby.

### Způsob poskytování plnění

* + - 1. Plnění je poskytováno zejména následujícím způsobem:
         1. Prostřednictvím pracovníka Uchazeče přímo na pracovišti Zadavatele
         2. Prostřednictvím pracovníka Uchazeče Vzdálenou správou
         3. Prostřednictvím pracovníka Uchazeče formou vzdálené konzultace
         4. Po dohodě smluvních stran automatizovanými nástroji při Monitorování, umožňují-li to technické prostředky na straně Zadavatele
      2. Uchazeč provede písemný záznam o provedení Služby na pracovišti Zadavatele, který předá Zadavateli a nechá si ho od něj potvrdit. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.
      3. Zadavatel je povinen zabezpečit Uchazeči podmínky pro řádné plnění, zejména
         1. v případě Monitorování a Vzdálené správy zajistit a udržovat podmínky pro Vzdálený přístup Uchazeče k Prvkům IT,
         2. zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,
         3. zajistit přístup k Provoznímu prostředí, který je nezbytný pro poskytování Služeb, včetně přístupu do prostor v objektu, kde je předmětný Prvek IT umístěn, případně přístup do prostor, v nichž jsou umístěna zařízení související s podporovaným systémem,
         4. zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku Uchazeče veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,
         5. umožnit Uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,
         6. zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné.
      4. V případě, že nebudou uvedené podmínky Zadavatelem prokazatelně zabezpečeny, lhůta pro vyřešení případného Incidentu se zastaví a počítat se bude až po obnovení zabezpečení uvedených podmínek.
      5. Uchazeč je v případě potřeby též z vlastní iniciativy oprávněn požádat Zadavatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Zadavatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu. Tím se zastavuje započítávání času, což je rozhodující pro určení čistého času řešení Incidentu při hodnocení úrovně poskytovaných služeb (SLA).
      6. Zadavatel je povinen
         1. písemně či elektronicky potvrdit Uchazeči provedení služby,
         2. zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,
         3. poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí, nejpozději do tří (3) Pracovních dnů po jejich písemném či ústním vyžádání, pokud se o obě strany nedohodnou jinak.

### Požadavky na přítomnost pracovníků

* + - 1. Zadavatel požaduje, aby v průběhu běžné pracovní doby organizace byl v lokalitě Zadavatele (on-site) přítomen technik Uchazeče, který bude schopen řešit incidenty při provádění upgradů kritických prvků (datová základna - databázový stroj)). Přítomnost technika vždy bude stanovena po vzájemné dohodě v předstihu nejméně 10 pracovních dnů předem.

### Postup při řešení požadavků

* + - 1. Zadavatel bude Požadavek oznamovat Uchazeči bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených ve Smlouvě o zabezpečení provozu, kam budou mít zajištěny přístup pověřené osoby Zadavatele. Momentem nahlášení požadavku Zadavatelem na hot-line nebo zadáním požadavku do HelpDesk začíná běžet lhůta pro Dobu odezvy.
      2. Součástí nahlášení požadavku Zadavatelem musí být:
         1. navrhovaná kategorizace a závažnost,
         2. popis Incidentu nebo Požadavku,
         3. jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh,
         4. kontaktní osoba.
      3. Uchazečem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.
      4. Incidenty musí být před jejich nahlášením začleněny do skupin, viz dále a dle těchto skupin bude Uchazeč přistupovat k jejich řešení:

|  |
| --- |
| Incident/vada kategorie A |
| Prvek IT/služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody. |
| Incident/vada kategorie B |
| Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz. |
| Incident/vada kategorie C |
| Ostatní - drobné incidenty/vady, které nespadají do kategorií A a/nebo B a které nejsou způsobeny software třetích stran. |
| Incident/vada kategorie D |
| Incidenty/vady, které jsou způsobeny software třetích stran. |

* + - 1. Uchazeč potvrdí obdržení požadavku dle podmínek SLA a bez ohledu na způsob nahlášení provede evidenci Požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.
      2. Uchazeč v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že Uchazeč v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení - zároveň přeřadí Incident do kategorie D a pokračuje v řešení v režimu BE (Best Effort).
      3. Zjistí-li Uchazeč v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele. Výskyt neodstranitelného Incidentu může být ze strany Zadavatele považován za podstatné porušení této smlouvy v případech, že Incident byl způsoben předchozím přímým jednáním Uchazeče, pokud o nich mohl mít s vynaložením veškeré odborné péče povědomost.
      4. Zjistí–li Uchazeč v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je Uchazeč povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy Uchazečem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.
      5. Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok Uchazeče na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.
      6. V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:
         1. čase vyřešení požadavku,
         2. v případě Incidentu specifikuje příčinu (pokud je známa),
         3. vyzve iniciátora k ověření funkčnosti služby.
      7. Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.
      8. Po vyřešení požadavku Uchazeč požadavek uzavře v systému HelpDesk a informuje Zadavatele. V případě Incidentu kategorie A zasílá návrh opatření pro snížení nebo eliminaci možnosti opakování stejného Incidentu.
      9. Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu Prvku IT; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu Prvku IT, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

### Podmínky SLA

* + - 1. Uchazeč se zavazuje dodržovat při řešení požadavků následující parametry (SLA).

|  |  |  |  |
| --- | --- | --- | --- |
| Kategorie incidentu | Garantovaná doba přijetí a akceptace hlášeného incidentu | Garantovaná doba zahájení prací na řešení incidentu po řádném nahlášení | Garantovaná doba ukončení incidentu po řádném nahlášení |
| A | 15 min | 6 hod | Nejpozději do 24 hod |
| B | 15 min | 8 hod | NBD |
| C | 15 min | NBD | 5BD |
| D | 15 min | NBD | BE |

* + - 1. Pro předání požadavků na plnění závazků vyplývajících z SLA je požadováno použití technologie umožňující nepřetržitý dálkový přístup v českém jazyce.
      2. Servisní kalendář (časový interval poskytování služeb) je stanoven min. v rozsahu 9x5 (8–17) v pracovních dnech, není-li u konkrétní služby uvedeno jinak.
      3. V rámci vymezení předmětu SLA Uchazeč nejlépe v technické příloze dostatečně přesně popíše, jaké služby a činnosti Zadavatele jsou pro plnění SLA zcela zásadní a kritické, respektive na jakých aplikacích a službách je provoz systémů závislý. Dále Uchazeč popíše, jakým způsobem zajistí dosažení podmínek SLA, možnosti měření SLA a možnosti ověření dosahování SLA, které bude mít Zadavatel k dispozici.
      4. Provozní činnosti budou kontrolovány Zadavatelem (nebo jím stanoveným subjektem) v rámci systému monitoringu.

### Seznam prvků IT

Následující tabulka obsahuje seznam Prvků IT, u nichž je požadováno Zabezpečení provozu

|  |  |  |
| --- | --- | --- |
| **Prvky IT** | | |
| **Prvek** | **Popis** | **Počet** |
| **Hardware** | | |
| - | není součástí dodávky | 0 |
| **Software** | | |
| 1 | Systémový software – virtuální servery, operační systémy | 4 |
| 2 | Systémový software - databázový server | 1 |
| 3 | Aplikační software - Systém pro správu identit | 1 |
| 4 | Aplikační software - Systém pro správu provozních dokumentů | 1 |
| 5 | Aplikační software – Systém pro řízení virtuálních desktopů | 1 |

### Záruky a servisní podmínky

* + - 1. Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci zajištění provozu podpor v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.