# Vymezení předmětu plnění veřejné zakázky

## Předmět plnění veřejné zakázky

* + - 1. Předmětem plnění veřejné zakázky jsou **dodávky zařízení a služeb** (dále také jen „řešení“) – rekonstrukce terminálové farmy, související upgrade Technologického centra včetně rozložení do dvou lokalit a upgrade dokumentových a archivačních technologií.
      2. Předmětem plnění veřejné zakázky jsou dodávky a služby (komodity) uvedené v následující tabulce. Podrobná specifikace dodávek a služeb je uvedena v kapitole 3 tohoto dokumentu.

|  |  |  |
| --- | --- | --- |
| **Označení** | **Zařízení** | **Počet** |
| K1 | Rekonstrukce terminálové farmy | 1 |
| K2 | Modernizace datového úložiště | 1 |
| K3 | Modernizace lokality U spořitelny (záložní centrum) | 1 |
| K4 | Upgrade archivačních technologií | 1 |
| K5 | Systém pro správu ICT zařízení | 1 |

## Popis výchozího stavu

### Popis organizace a její členění

* + - 1. Organizace **Magistrát města Karlovy Vary (dále MMKV)** sídlí ve 2 administrativních budovách, kde pracuje většina zaměstnanců a je zde umístěná převážná část IT technologií. Organizace je zřizovatelem organizací v oblasti dopravy, kultury, správy majetku, školství, sociální a zdravotní.

### Popis lokalit

* + - 1. Z pohledu IT jsou pro MMKV nejvýznamnějšími lokalitami budova Moskevská 2035/21, 361 20 Karlovy Vary a budova U Spořitelny 538/2, 361 20 Karlovy Vary. V těchto lokalitách jsou umístěny ICT technologie. Projekt bude realizován v obou lokalitách.

### Popis stávajícího HW prostředí

* + - 1. Technologické centrum ORP (dále TC ORP nebo TC) je infrastrukturním základem pro poskytování IT služeb. Cílem je zajištění co nejlepších podmínek provozu informačních systémů v režimu 5×12. V současné době je Technologické centrum situováno v lokalitě Moskevská.
      2. Technologické centrum bylo vybudováno z původní serverovny úřadu v roce 2012 v rámci Výzvy 06 IROP, dále rozšířeno v rámci Výzvy 09, kdy byly vybudován i softwarové platformy pro správu dokumentů, identit a archivaci. V roce 2014 prošlo TC zatím poslední modernizací – doplněním síťových firewallů, konsolidací zálohování, modernizací groupware a systému řízení tisku a zavedením provozního monitoringu.
      3. Hlavní serverová infrastruktura je tvořena 2 ks HP Blade šasi. Šasi jsou osazena devíti kusy dvouprocesorových Blade serverů BL460 G7 a G8. Pro řízení zálohování a další pomocné úlohy slouží samostatný fyzický server HP DL380 G8.
      4. SAN infrastruktura je tvořena optickými SAN přepínači – 2 kusy v každém HP Blade šasi a 2 kusy HP 8/24 Base SAN Switch. Do SAN infrastruktury jsou zapojena 4 externí disková pole MSA2000G3 s expanzními policemi, dále dvě páskové knihovny MSL 2024 a 4048, obě Blade šasi, zálohovací server a 2 appliance diskové virtualizace FalconStor NSS GA700 s externími rychlými vyrovnávacími pamětmi (cache) tvořenými servery HP DL380p G8 s rychlými flash úložišti. Účelem diskové virtualizace je zajištění pokročilých služeb – zejména zrcadlení úložišť, zajištění vysoké dostupnosti úložišť a abstrakce úložišť vůči fyzickým i virtuálním serverům.
      5. V TC ORP je využívána serverová virtualizační technologie VMware vSphere, aktuálně ve verzi 5.1 v edici Enterprise Plus (16 CPU). Pro správu prostředí slouží vSphere vCenter Standard. Jsou využívány rozšířené funkce virtualizační platformy High-availability, Vmotion, DRS.
      6. Pro napájení nových technologií je v primární lokalitě k dispozici zálohované napájení o výkonu 40 kVA zajišťované UPS Eaton 93PM. UPS je vybavena externím bypassem a systémem nouzového odstavení. Pro správu UPS a automatické řízení virtualizační platformy při výpadku a obnově napájení je používán systém Eaton Intelligent power manager. UPS splňuje požadavky na spolehlivé zajištění nepřetržitého napájení TC a má výkonovou rezervu pro zálohování poptávaných technologií.
      7. TC ORP je navrženo a budováno pro poskytování vysoce dostupných služeb. Klíčové prvky TC ORP jsou redundantní a jsou implementovány technologie umožňující automatické překlenutí odstávky (plánované i neplánované) klíčového prvku s žádným nebo minimálním (v řádu jednotek minut) výpadkem služeb.
      8. TC ORP je primárně zálohováno systémem Veeam Backup & Replication s ukládáním záloha na diskové pole a páskovou knihovnu MSL 2024. Některé zálohy a archivy, popř. méně důležitá data (např. instalační zdroje) jsou ukládány na úložišti typu NAS Windows Storage Server.
      9. Hlavním databázovým úložištěm MMKV je Microsoft SQL Server, aktuálně ve verzi 2008.
      10. Síťová infrastruktura LAN je osazena převážně aktivními prvky HP (HPE) řad 51xx a 55xx s operačním systémem Comware.
      11. Zabezpečení přístupu k Internetu využívá dvou firewallů Fortinet FortiGate FG-240D v režimu vysoké dostupnosti (clusteru) včetně rozšiřujících bezpečnostních UTM funkcí.
      12. Groupwarové služby zajišťuje systém Exchange 2013 s doplňkovými nástroji pro bezpečnostní kontrolu příchozích a odchozích zpráv (antivir, antispam). Systém zajišťuje i obsluhu mobilních zařízení.
      13. Většina uživatelů využívá pro přístup k aplikacím tenké klienty HP. Aplikace jsou doručovány technologií Citrix Presentation Server 4 provozovanou na virtuálních serverech Windows 2003 R2. Pro vzdálený přístup k aplikacím je využívána technologie Citrix Secure Gateway.
      14. V prostředí TC ORP je implementován systém SafeQ pro řízení tiskového prostředí. Tiskové prostředí je tvořeno zejména tiskárnami a multifunkčními stroji HP LJ 3035, HPLJ4350dtn, HPLJP2055dn, Develop INEO 353 a osobními tiskárnami uživatelů, převáženě značky HP. Celkový počet tiskových zařízení je cca. 100.
      15. Provoz TC ORP je monitorován dohledovým systémem, který vychází ze systému Nagios. Systém monitoruje dostupnost a parametry služeb, aplikací, operačních systémů a zařízení včetně speciálních – docházkové terminály, kamerové systémy a další. Systém provádí i environmentální monitoring.
      16. MMKV disponuje optickou komunikační infrastrukturou (dále KI) typu MAN (metropolitan area network) propojující většinu městských organizací a také obě lokality MMKV (délka spoje mezi lokalitami je < 1 km, k dispozici je min. 8 single modových vláken). KI prochází kontinuálním rozvojem ve dvou klíčových oblastech – připojování dalších městských organizací a zavádění služeb pro tyto organizace. Komunikace mezi KI a TC ORP i komunikace s externími sítěmi (Internet, RKI Karlovarského kraje apod.) je řízena clusterem firewallů Fortinet FortiGate FG-240D. MAN je provozována na aktivních prvcích HP (HPE) řad 55xx a 75xx a je monitorována HP Intelligent Management Center (je částečně využíván i pro monitoring LAN).
      17. V prostorách MMKV je vybudován přípojný uzel krajské Regionální komunikační infrastruktury (dále RKI) vlastněné a provozované Karlovarským krajem. RKI propojuje všechny ORP Karlovarského kraje a významné organizace Karlovarského kraje (nemocnice, střední školy, SÚS (Správa a údržba silnic) a další. RKI je připojena k národním a resortním sítím – např. KIVS. RKI prochází kontinuálním rozvojem stejně jako KI.
      18. Pro účely správy dokumentů a provoz specifických aplikací (např. Registr dlužníků) využívá MMKV platformy Microsoft Sharepoint Foundation 2010 s rozšířením Nintex Workflow a Nintex Forms v edici Workgroup.
      19. Pro účely archivace dokumentů (např. stavebního archivu) využívá MMKV platformu IBM FileNet (Business proces manager a Content Collector for E-mail).
      20. Standardním kancelářským balíkem využívaným pro potřeby MMKV je Microsoft Office, s ohledem na sjednocení uživatelského rozhraní a kompatibilitu dokumentů ve verzi 2007 a vyšší. Standardně jsou využívány aplikace Word, Excel, Outlook a OneNote. Nabízená řešení a produkty musí být s používaným kancelářským balíkem plně kompatibilní.

### Popis dokumentace

* + - 1. K provozování a řízení rozvoje TC je využívána a udržována Provozní dokumentace.
      2. Provozní dokumentace popisuje základní nastavení technologií, hardwarových a softwarových systémů a je tvořena souborem dokumentací zpracovaných v průběhu realizovaných implementačních ICT projektů.
      3. Citlivé údaje (přístupové účty apod.) jsou uloženy odděleně od Provozních dokumentací.
      4. Uchazeč je povinen v rámci zakázky zajistit nezbytné doplnění Provozní dokumentace reflektující provedené změny.

### Popis způsobu řešení incidentů

* + - 1. Zadavatel pro řešení incidentů a podporu uživatelů využívá vlastní systém Helpdesk.
      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

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

## Povinné parametry technického řešení

### Obecné požadavky

* + - 1. Uchazeč v rámci zakázky navrhne:
         1. způsob rekonstrukce a optimalizace stávající terminálové farmy s optimálním využitím aktuálně dostupných licencí a možností software – MMKV udržuje platnou maintenance na produkty Citrix XenApp Advanced a má dispozici potřebné licence serverové a klientské licence Microsoft min. ve verzích 2012R2.
         2. způsob modernizace a konsolidace SAN a datových úložišť pro zvýšení kapacity a výkonu.
         3. způsob provedení modernizace datového centra v lokalitě U spořitelny, vhodné rozmístění technologií TC do obou lokalit MMKV s ohledem na výkon a dostupnost navrhne a způsob provedení navrženého rozmístění.
         4. způsob upgrade a modernizace stávajících platforem pro správu a archivaci dokumentů.
         5. vhodnou strukturu pro evidenci a správu ICT zařízení a způsob nasazení systému pse zapracováním navržené struktury
      2. Uchazeč v rámci zakázky provede po schválení návrhů z předchozího bodu jejich realizaci.
      3. Serverová infrastruktura je virtualizována a provozována v TC s využitím všech jeho výhod (vysoká dostupnost, bezpečnost, zálohování, trvalý monitoring a správa).
      4. 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.
      5. V technickém popisu mohou být uvedeny značky, či přímo názvy řešení, a to v případě, že Město považuje za odůvodněné, že řešení rozšiřuje stávající funkcionalitu, doplňuje funkčně stávající řešení, či požaduje řešení minimálně s vlastnostmi řešení uvedeného a konkrétní popis by byl nad rámec tohoto dokumentu.
      6. Dodavatel ve své nabídce detailně popíše vazby na stávající systémy Zadavatele, které jsou nezbytné pro správné fungování řešení nabízeného Dodavatelem.
      7. Pokud uchazečem navržené řešení vyžaduje využití konkrétních softwarových produktů, neobsažených v popisu předmětu plnění, a jím zvolený přístup k řeše zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
      8. 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.
      9. 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.
      10. 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 apod.
      11. Uchazeč bude při implementaci respektovat provozní řád TC, vítězný uchazeč bude s provozním řádem TC seznámen před podpisem Smlouvy o dílo.
      12. 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 v databázi výrobce uvedeny jako prodaná kupujícímu,
          6. jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel 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.

Výjimkou mohou být pouze jednotlivé komponenty určené pro rozšíření stávajících technologií, které již výrobce nedodává (např. z důvodu náhrady novým modelem). V takovém případě lze nabídnout originální komponenty dodávané v rámci servisního programu a splňující požadované parametry včetně záruk.

* + - 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 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 – Rekonstrukce terminálové farmy

* + - 1. Stávající terminálová farma bude rekonstruována s využitím aktuálních licencí vlastněných MMKV a licencí dodaných v rámci této zakázky.
      2. Rekonstrukce nesmí negativně ovlivnit chod stávajících aplikací MMKV. Všechny aplikace musí být v rekonstruované farmě otestovány a případně optimalizovány (případné náklady na nezbytné aktualizace nejsou součástí této zakázky). Seznam aplikací provozovaných v současné farmě je uveden v následující tabulce:

| **Aplikace** | **Výrobce / Dodavatel** |
| --- | --- |
| AccountiX | ATECO spol. s r.o. |
| Ginis | GORDIC spol. s r.o. |
| Fenix (Helios) | Asseco Solutions |
| Gemini | BSC PRAHA, spol. s.r.o., v |
| WinPED | GORDIC spol. s r.o. |
| Crypta | Česká pošta - PostSignum |
| Dopravní agendy | YAMACO Software |
| Elektronické pořizování výkazů | ONYX Software s.r.o. |
| Elektronické testy pro MS | YAMACO Software |
| ESPI | INISOFT s.r.o. |
| EVI | INISOFT s.r.o. |
| Evidence myslivosti | YAMACO Software |
| Evidence obyvatel | Triada, spol. s r. o. |
| eVPE4 - editor vodoprávní evidence | MGE DATA, spol s r.o. |
| Informační servis 2000 | vlastní vývoj |
| PDS lesní hospodářství | PDS s.r.o. |
| Podatelna | PilsCom s.r.o. |
| URS - manažerské přehledy staveb | KROS a.s. |
| ASPI | Wolters Kluwer ČR, a. s. |
| Docházka | FLUX, spol. s r.o. |
| FluxPAM | FLUX, spol. s r.o. |
| Stavební úřad | VITA software s.r.o. |
| INSYMPO | Fofrs software s.r.o. |
| Misys | GEPRO spol. s r. o. |
| PC Translator | LangSoft s.r.o. |
| Munis | Triada, spol. s r. o. |
| Zoner Photo Studio | ZONER software, a.s. |
| Microsoft Office | Microsoft |
| Dobrné agendy Visual Foxpro a Microsoft Access |  |

* + - 1. Součástí rekonstrukce bude vybudování aplikačního firewallu pro publikaci virtualizovaných aplikací a webových aplikací MMKV. Vzdálený přístup k aplikacím bude zabezpečen 2 faktorovou autentizací pomocí SMS a umožní autentizaci min 100 uživatelům. Pro zasílání SMS se předpokládá využití externí (webové) služby, náklady na zasílané SMS nejsou součástí této zakázky.
      2. Součástí implementace bude i zabezpečení stávající aplikace Outlook Web Access 2013 aplikačním firewallem.
      3. Pro začlenění serveru budou využity stávající licence VMware vSphere a Veeam Backup & recovery.
      4. Rekonstrukce nesmí negativně ovlivnit dostupnost aplikací uživatelů. Součástí návrhu a realizace musí být vhodný scénář a podpora přechodu uživatelů na novou farmu zpracovaný v Prováděcí dokumentaci
      5. Klientská zařízení budou nadále využívána stávající, jde o tenké klienty HP TC, kompatibilní se současnými verzemi Citrix XenApp.
      6. Rekonstruovaná farma umožní snadné (ideálně automatické) nasazování dalších serverů doručujících aplikace pro zlepšení odezvy a/nebo dostupnosti publikovaných aplikací.

### Specifické požadavky K2 – Modernizace datového úložiště

* + - 1. Cílem modernizace je s využitím stávajícího hardware a jeho rozšířením navýšit kapacitu a výkon diskového úložiště a SAN, doplnění moderních funkcí (např. automatický tiering) a zlepšení škálovatelnosti celého systému.
      2. Modernizované řešení musí zachovat klíčové funkcionality současného stavu (synchronní replikace, resp. zrcadlení diskových úložišť a bezobslužný transparentní failover v případě výpadku úložiště a/nebo virtualizační appliance pro připojené servery).
      3. Řešení musí být možno provozovat na hardware různých výrobců (tzv. vendor independent) a musí být schopno virtualizovat disková pole i DAS (direct attached storage) různých výrobců.
      4. Jednotlivé uzly řešení budou rozmístěny ve dvou lokalitách (Moskevská a U spořitelny), navržené řešení musí tento scénář podporovat.
      5. Součástí modernizace musí být veškeré případné migrace dat uložených na diskových polích a NAS, celkový objem dat nepřevyšuje 50 TB.
      6. Modernizací dojde ke zvýšení výkonu virtualizovaných úložišť min. o 10%. Zvýšení Uchazeč prokáže měřením výkonu (IOPS - input / output operations per second) z prostředí virtuálního serveru na srovnatelných virtualizovaných discích (LUN) před a po modernizaci.
      7. Řešení bude plně využívat funkcionalit moderních úložišť (typu SSD, NVMe nebo obdobné technologie) pro maximalizaci výkonu úložiště a bude umožnovat i provoz plně flashových virtualizovaných disků pro kritické aplikace (typicky databázový server).

### Specifické požadavky K3 – Modernizace lokality U spořitelny

* + - 1. V rámci komodity bude provedeno rozložení TC do obou lokalit MMKV. Jedná se o další zvýšení dostupnosti dat a služeb TC i v případě úplného či rozsáhlého výpadku serverových technologií v jedné z lokalit.
      2. TC bude rozloženo počtem zařízení přibližně symetricky (zejména blade šasi a disková virtualizace s úložišti) s výkonovou preferencí lokality Moskevská – zde budou umístěny komponenty novější/výkonnější a technologie společné pro obě lokality.
      3. Lokalita U spořitelny bude doplněna o datový rozvaděč se zálohovaným napájením a síťovými přepínači pro napojení na lokální datové rozvody a KI.
      4. Součásti projektu je přesunutí, zprovoznění a otestování stávajích zařízení (viz. 2 Popis výchozího stavu) v rozsahu a dle postupu navrženého Uchazečem a schváleného Zadavatelem.

### Specifické požadavky K4 – Upgrade archivačních technologií

* + - 1. V rámci komodity bude realizován upgrade a optimalizace platforem pro správu dokumentů (Sharepoint + Nintex) a archivaci dokumentů (IBM FileNet).
      2. Upgrade bude proveden na poslední dostupné verze všech produktů. MMKV má dispozici platné potřebné produktové maintenance.
      3. Součástí upgrade budou aktualizace a optimalizace aplikací a řešení provozovaných na obou platformách:
         1. Sharepoint-Registr dlužníků včetně integrace na insolvenční rejstřík, Agenda žádanek (dovolená, pracovní pomůcky, právní služby), Agenda rezervací (rezervace zdrojů, např. vozidel), Dokumenty (správa dokumentů podle kategorií) a Nástěnka (aktuální informace pro zaměstnance),
         2. IBM FileNet – archiv stavebního úřadu, archiv e-mailové komunikace (Exchange).
      4. Součástí upgrade bude revize a případná optimalizace designu platforem a jejich napojení na systémovou infrastrukturu (SQL databáze, zálohování apod.)
      5. V rámci upgrade bude platforma Sharepoint rozšířena o možnost šifrování ukládaných dokumentů a 2 faktorovou autentizaci uživatelů přistupující k těmto dokumentům.

### Specifické požadavky K5 - Systém pro správu ICT zařízení

* + - 1. Systém pro podporu elektronizace a řízení vnitřních procesů a služeb úřadu včetně správy ICT zařízení í (Asset Management).
      2. Pro standardizaci IT služeb bude využit doporučující rámec ITIL a systém bude vykazovat shodu s tímto rámcem.
      3. Správa ICT zařízení umožní efektivně a přehledně evidovat a spravovat veškerá ICT zařízení zadavatele. Uživatelé budou v systému propojeni s přiděleným zařízením a bude existovat kompletní záznam událostí spojených se zařízením.
      4. Systém pro správu ICT zařízení bude podporovat správu libovolného ICT zařízení, k tomu umožní jednoduché doplňování libovolných popisných položek a jejich plné využití např. při filtrování, vyhledávání atp. Zařízení bude možno propojit s odpovědnou osobou (uživatelem) a uživateli bude kdykoliv (on-line) dostupný přehledný seznam a stav ICT zařízení, za který odpovídá. Nadřízení budou mít dostupný přehled ICT zařízení svých podřízených.
      5. Správa ICT zařízení bude umožňovat veškeré obvyklé operace s majetkem (pořízení, zavedení, převod, opravy, údržba, vyřazení apod.) včetně tisku příslušných předávacích protokolů a automatického upozorňování na opakované události (revize, údržba, kalibrace apod.). Pro správu IT ICT zařízení bude systém disponovat neinvazivní (bezagentovou) automatickou detekcí a inventarizací hardware a software počítačů a serverů a bude umožňovat obvyklé funkce softwarového auditu (přehled, přidělování, odebírání licencí a upozorňování na neoprávněně instalovaný software) v rozsahu akceptovaném hlavními výrobci software - např. Microsoft, Adobe, Autodesk.
      6. V rámci předmětu plnění bude systém implementován pro správu majetku IT (počítače, software, mobilní telefony, tiskárny, servery, síťové prvky atd.) zaměstnanců MMKV.
      7. Celý systém musí být jednoduše rozšiřitelný (aktivací nebo pořízením modulů, nikoli programovými úpravami).
      8. Celý systém musí být technicky i licenčně dostupný všem zaměstnancům úřadu, aby nebylo omezeno zavádění služeb do systému.

### 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 - Rekonstrukce terminálové farmy** | | | | |
| --- | --- | --- | --- | --- |
| **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** |
|
| **Virtualizační server 1 ks** | Provedení | Blade server |  |  |
| Procesor | 2x procesor osmi-jádrový (dohromady 16 jader), nominální frekvence min. 3.2 GHz, automatické zvýšení frekvence jádra až o 0,5 GHz při nevyužití ostatních jader) |  |  |
| Pevné disky | 2x SSD, min. 140 GB pro hypervizor |  |  |
| Řadič disků | min. RAID 0,1, zálohovaná cache pro zápis min. 1 GB |  |  |
| Paměť | minimálně 320 GB RAM, min. 2600 MT/s |  |  |
| Rozšiřitelnost | rozšiřitelnost RAM min. na 700 GB bez výměny RAM modulů |  |  |
| RAID | řadič RAID 0,1, 10, SAS 12 Gb, zálohovaná vyrovnávací paměť pro zápis min. 1 GB |  |  |
| LAN porty | LAN 2x10Gb s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. Podpora partitioningu - rozdělení fyzického LAN adaptéru na více virtuálních adaptérů - min. 4 virtuální adaptéry na každý port |  |  |
| FC porty | 2x FC (fibre channel) port min. 16 Gb |  |  |
| Vzdálená správa | Podpora vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. |  |  |
| Kompatibilita | Podpora nejrozšířenějších operačních systémů (Windows, Linux) a hypervizorů (Hyper-V, VMware) |  |  |
| Kompatibilita | Plně kompatibilní se stávajícím Blade šasi HP C7000 na fyzické i elektrické úrovni |  |  |
| Vysoká dostupnost | Podpora a licence pro clusterový provoz |  |  |
| Management | Plná integrace s management modulem HP Blade šasi HP 7000 |  |  |
| Záruka | Záruka 60 měsíců, oprava následující pracovní den v místě instalace |  |  |
| **SW licence operačních systémů** | Operační systémy | Licence 64 - bitového serverového operačního systému v aktuální verzi pro nabízený server. Licence musí umožnit provoz neomezeného počtu virtuálních serverů stejné verze v prostředí stávající serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů a komponent terminálové farmy |  |  |
| **Aplikační firewall 1 ks** | Publikace aplikací | Bezpečné zpřístupnění virtualizovaných aplikací terminálové farmy prostřednictvím webového rozhraní včetně SSO (single sign on) |  |  |
| Zabezpečení aplikací | Zabezpečení publikovaných webových aplikací a rozhraní |  |  |
| Řízení aplikací | směrování klientů dle stavu a vytížení serveru na úrovni aplikace (L7 dle OSI modelu) |  |  |
| Šifrování | SSL offload a akcelerace |  |  |
| Routování | Podpora dynamických routovacích protokolů |  |  |
| Loadbalancing | umožňuje rozkládání zátěže serverů aplikační virtualizace i obecných serverů - min. protokoly TCP, UDP, FTP, HTTP, HTTPS, DNS, SIP |  |  |
| Zabezpečení aplikací | URL/HTTP rewriting |  |  |
| Optimalizace | optimalizace TCP provozu pro pomalé linky (redukce otevřených spojení, zkrácení odezev apod.) |  |  |
| Autentizace | Podpora vícefaktorové autentizace (ověřování), min. pomocí SMS |  |  |
| Ochrana | ochrana proti DoS útoku |  |  |
| Monitoring | Monitoring provozu publikovaných aplikací včetně historie |  |  |
| RDP | Integrovaná proxy pro zabezpečení RDP (Remote desktop protocol) - pro vzdálenou správu technologií |  |  |
| VPN | integrovaná SSL VPN |  |  |
| Výkon | Propustnost portálu min. 200 Mbit/s při SSL šifrování |  |  |
| Záruka | Nárok na technickou podporu výrobce a nové verze min. 12 měsíců |  |  |

| **Komodita K2 - Modernizace datového úložiště** | | | | |
| --- | --- | --- | --- | --- |
| **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** |
|
| **Disková virtualizace** | Funkcionalita | SDS - software definded storage |  |  |
| Provedení | Software, instalovaný přímo na serverový hardware (včetně případného operačního systému) bez použití hypervizoru |  |  |
| Protokoly | FC (Fibre Channel) a iSCSI pro připojení diskových polí i export virtuálních disků (LUNů) připojených serverům |  |  |
| Diskové úložiště | Podpora virtualizace externích diskových polí i přímo připojených úložišť DAS (direct attached storage)) - HDD, SSD, NVMe |  |  |
| Licence | Pro 2 uzly (appliance) v režimu active-active (cluster) a min. 62 TB obsluhované diskové kapacity každým uzlem |  |  |
| Efektivní využití úložišť | Deduplikace uložených dat |  |  |
| Thin provisioning | Vytváření virtuálních disků s větší prezentovanou kapacitou, než je dostupná fyzicky na připojených úložištích. Dynamická alokace fyzického prostoru na úložištích podle skutečně uloženého objemu dat, včetně jeho uvolnění při vymazání dat (tzv. space reclamation) |  |  |
| Multipathing | Podpora vícecestného a redundantního připojení serverů, diskových polí a uzlů vzájemně |  |  |
| Zrcadlení | Synchronní replikace dat mezi 2 fyzicky oddělenými uzly diskové virtualizace a jimi obsluhovanými úložišti |  |  |
| Vysoká dostupnost | automatický a pro připojené servery transparentní failover při výpadku libovolného diskového úložiště a/nebo virtualizačního uzlu |  |  |
| Provozní režim | Podpora active-active režimu s možností nastavení preferovaných cest připojeným serverům |  |  |
| Vyrovnávací paměť | Podpora min. 128 GB vyrovnávací pamětí (cache) v každém uzlu pro zápis i čtení. |  |  |
| Priority | Kategorizace virtuálních disků (např. kritický, standard) a prioritizace operací diskových podle kategorií. |  |  |
| Ochrana datové konzistence | Podpora automatického vypnutí zápisové vyrovnávací paměti při nestandardním provozním stavu (např. přepnutí připojené UPS na provoz z baterií) |  |  |
| Snapshoty | Podpora vytváření snapshotů (snímků virtuálních disků) exportovatelných připojeným serverům |  |  |
| Řízení přenosů | QoS (Quality of services) - omezení max. přenosové rychlosti a počtu vstupně/výstupních operací za sekundu směrem k připojeným serverům i na úrovní virtuálního disku. |  |  |
| Tiering | Automatický tiering (přesouvání dat podle četnost používání (čtení i zápis)) s podporu min 4 úrovní (tierů): NVMe, SSD, SAS, SATA/MDL SAS |  |  |
| Cluster | Podpora tzv. stretch clusteru - rozmístění uzlů do dvou vzdálených lokalit se sdílenou SAN. |  |  |
| Zachování dat, migrace | Popora připojení a exportu stávajích LUNů z připojených úložišť se zachováním obsahu, podpora přenosu obsahu zrcadlením na virtuální disky. |  |  |
| Propustnost | podpora vyhrazených (oddělených) portů (FC, iSCSI) podle rolí pro zvýšení propustnosti:  - obsluha připojených servery - obsluha diskový polí  - replikace (zrcadlení) dat pro vysokou dostupnost |  |  |
| Disaster recovery | Asynchronní replikace přes TCP/IP do vzdálené DR (disaster recovery) lokality na záložní uzly (licence záložních uzlů není součástí dodávky) |  |  |
| Kompatibilta | Kompatibilita se stávající serverovou virtualizací, integrace s management nástrojem (vCenter), podpora rozhraní vSphere VAAI |  |  |
| Záruka | Záruka min. 12 měsíců včetně nároku na podporu výrobce a nové verze software |  |  |
| **Rozšíření stávajících technologií Technologického centra** | SAN přepínače | 2x SAN přepínač pro osazení do HP Blade šasi C7000. FC porty min. 8 Gb. 24 FC portů (16 interních, 8 externích), všechny porty aktivní. |  |  |
| LAN přepínače | 2x LAN přepínač pro osazení do HP Blade šasi C7000. Min. 24 portů 10 Gb - 16 interních, 8 externích. Externí porty SFP+. Podpora technologie Virtual Connect Flex pro vyžítí adaptérů v Blade serverech disponujících touto technologií. |  |  |
| Procesory | 2x procesor min. šestijádrový, nominální frekvence min. 2.8 GHz určený pro server HP DL380p G8 (653200-B21) včetně příslušenství (chladiče, ventilátory apod.) |  |  |
| PCI-E risery | 2x PCI-E riser, každý min. 3 PCI-E sloty, určené pro server HP DL380p G8 (653200-B21) |  |  |
| Paměťové moduly | 16x paměťový modul RAM určené pro server HP DL380p G8 (653200-B21). Každý min. 8GB, DDR3-1600 |  |  |
| FC adaptéry | 6x FC HBA určené pro server HP DL380p G8 (653200-B21). Každý min. porty 8 Gb, obslužný čip QLOGIC |  |  |
| Optické moduly | 12x FC 8 Gbit pro nabízené FC přepínače, shortwave 4x FC 8 Gbit pro nabízené přepínače, longwave (10 km) 4x SFP+ 10Gb SM včetně DMI pro nabízené přepínače |  |  |
| Optické kabely | optický kabel 5 m ke každému optickému modulu, protilehlé konektory LC |  |  |
| Záruka | Záruka min. 12 měsíců, oprava následující pracovní den v místě instalace. Komponenty musí podporovány výrobcem pro použití v rozšiřovaném zařízení (Blade šasi, server apod.) a nesmí omezit podporu těchto zařízení poskytovanou výrobcem |  |  |
| **Rozšíření flash úložišť 2 ks** | Provedení | PCI-E Gen 3 NVME karta pro rozšíření serveru HP DL380p G8 (653200-B21) |  |  |
| Kapacita | min. 4 TB |  |  |
| Výkon a latence | min. 700 000/200 000 IOPS pro náhodné čtení/zápis a velikost bloku min. 4 kB Latence max 80/40 mikrosekund pro čtení/zápis |  |  |
| Trvanlivost | min. 2.5 DWPD (drive writes per day - přepis plné kapacity disku denně) po dobu záruky dle metodik JEDEC (https://www.jedec.org/) |  |  |
| Kompatibilita | s nabízenou diskovou virtualizací |  |  |
| Záruka | Záruka min. 5 let |  |  |
| **Rozšíření diskových úložišť** | HDD 2,5" | 26 ks HDD 600 GB / 10000 ot. min, SAS min. 6 Gb |  |  |
| Kompatibilita | Plná kompatibilita s diskovými poli HP MSA 2000G3 a expanzními policemi HP D2700 |  |  |
| Záruka | Záruka min. 3 roky s výměnou v místě instalace |  |  |
| **Síťové úložiště NAS 1 ks** | Provedení | do racku, rozměr max. 6RU, včetně montážního materiálu do racku |  |  |
| HDD | Min. 36 pozic pro HDD 3,5" SATA III |  |  |
| CPU | Min. 8000 bodů dle https://www.cpubenchmark.net |  |  |
| Rozšiřitelnost | Podpora připojení externích disků přes USB 3.0 (min. 2 porty) |  |  |
| Podpora SSD | Integrovaná podpora SSD HDD pro ukládání dat i jako vyrovnávací paměť (cache) rotačních disků |  |  |
| Hot-swap | Disky vyměnitelné za chodu. |  |  |
| Kapacita | Osazeno min. 24x 4TB HDD SATAIII/128 MB cache, 7200 ot/min. Disky musí být výrobcem určeny pro nepřetržitý provoz v NAS nebo disková pole  , nejsou přípustné disky určené pro jiné využití - např. desktopy, kamerové systémy apod. |  |  |
| Konektivita | Min. 1x 10 Gb SFP+ a 4 x 1GBit Ethernet porty s podporou agregace linek a redundance. |  |  |
| Výkon | Rychlost zápisu min. 1500 MB/sec při RAID5 a CIFS (SMB) pro velikost bloku min 64 kB |  |  |
| Kompatibilita | Podpora Windows ADS a ACL, podpora VMware VAAI |  |  |
| Komunikace LAN | Síťové protokoly CIFS (SMB), WebDAV, iSCSI, SSH, SNMP, http/s |  |  |
| UPS | Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení |  |  |
| Paměť | RAM 4 GB využitelná i jako cache, rozšiřitelnost min na 16 GB |  |  |
| Ochrana dat | Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10 |  |  |
| Záruka | Záruka výrobce min. 5 let s opravou v místě instalace včetně disků a nároku na nové verze firmware |  |  |

| **Komodita K3 - Modernizace lokality U spořitelny (záložní centrum)** | | | | |
| --- | --- | --- | --- | --- |
| **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** |
|
| **UPS - rack 1 ks** | Provedení | Provedení do racku, max. 6U (včetně bateriových modulů), včetně montážního materiálu |  |  |
| Elektrické provedení | Jmenovité napětí 230 V, jednofázová na vstupu i výstupu |  |  |
| Výkon (VA/W) | 5000 VA / 4500 W |  |  |
| Technologie | dvojitá konverze, on-line |  |  |
| Účinnost | Min. 98%, účiník min 0,9 |  |  |
| Stabilizace | Stabilizace výstupního napětí |  |  |
| Kapacita | Doba běhu na baterie min. 10 min při 70% zátěži (samotná UPS) |  |  |
| Vstup | Pevný (svorkovnice) |  |  |
| Výstupy | Min. 8 zásuvek IEC C13 a 2 zásuvky IEC C19 |  |  |
| Napájecí segmenty | Min. 2 nezávisle ovládané (i dálkově) a měřené napájecí segmenty pro postupný náběh napájených technologií (přepínače, servery, úložiště) |  |  |
| Diagnostika | Vestavěný úplný́ systémový́ autotest, možnost automatického plánovaného provádění |  |  |
| Servis | Baterie musí být vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení. |  |  |
| Rozšíření | Součástí dodávky je požadováno rozšíření kapacity kapacity baterií pro zajištění doby běhu na bateria min. 40 min. při 70% zátěži. Možnost dalšího rozšíření až do min. 150 min |  |  |
| Komunikační porty | RS-232, USB, LAN RJ-45 pro management a automatické řízení zálohovaných zařízení |  |  |
| Komunikace LAN | Podpora http/s, SNMP s podporou standardní UPS MIB, SMTP |  |  |
| Stavové informace | Grafický stavový displej pro konfiguraci a provozní informace o stavu UPS |  |  |
| Řízení | Schopnost dálkového ovládání a restartování chráněných zařízení přes síť, korektní shutdown operačních systémů |  |  |
| SW kompatibilita | UPS musí být plně podporovaná výrobcem pro použití v obvyklých virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky |  |  |
| Optimalizace | Integrované technologie pro maximalizaci životnosti baterií |  |  |
| Alerty | Real-time e-mailová upozornění na události |  |  |
| Záruka | Záruka min. 60 měsíců včetně baterií s opravou v místě instalace |  |  |
| **UPS – volně stojící 1 ks** | Provedení | Volně stojící včetně podstavce |  |  |
| Elektrické provedení | Jmenovité napětí 230 V, jednofázová na vstupu i výstupu |  |  |
| Výkon (VA/W) | min. 2100 VA /1950 W |  |  |
| Technologie | Interaktivní s možností zvyšování i snižování napětí |  |  |
| Účinnost | Min. 98%, účiník min 0,9 |  |  |
| Stabilizace | Stabilizace výstupního napětí |  |  |
| Kapacita | Doba běhu na baterie min. 5 min při 70% zátěži (samotná UPS) |  |  |
| Vstup | Zásuvka IEC C20 |  |  |
| Výstupy | Min. 8 zásuvek IEC C13 a 1 zásuvka IEC C19 |  |  |
| Napájecí segmenty | Min. 2 nezávisle (i dálkově) ovládané a měřené napájecí segmenty pro postupný náběh napájených technologií (přepínače, servery) |  |  |
| Diagnostika | Vestavěný úplný́ systémový́ autotest, možnost automatického plánovaného provádění |  |  |
| Servis | Baterie musí být vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení. |  |  |
| Rozšíření | Součástí dodávky je požadováno rozšíření kapacity baterií pro zajištění doby běhu na bateria min. 35 min. při 70% zátěži. Možnost dalšího rozšiřování do min. 120 min |  |  |
| Komunikační porty | RS-232, USB, LAN RJ-45 pro management a automatické řízení zálohovaných zařízení |  |  |
| Komunikace LAN | Podpora http/s, SNMP s podporou standardní UPS MIB, SMTP |  |  |
| Stavové informace | Grafický stavový displej pro konfiguraci a provozní informace o stavu UPS |  |  |
| Řízení | Schopnost dálkového ovládání a restartování chráněných zařízení přes síť, korektní shutdown operačních systémů |  |  |
| SW kompatibilita | UPS musí být plně podporovaná výrobcem pro použití v obvyklých virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky |  |  |
| Optimalizace | Integrované technologie pro maximalizaci životnosti baterií |  |  |
| Alerty | Real-time e-mailová upozornění na události |  |  |
| Záruka | Záruka min. 36 měsíců včetně baterií s opravou v místě instalace |  |  |
| **Datový rozvaděč 1 ks** | Rozměry | Interní prostor 42U Vnější šířka 800 mm Vnější hloubka 1000 mm |  |  |
| Provedení | serverový datový rozvaděč (rack), zatížitelnost min. 750 kg, kovové robustní (svařované) provedení. Seřizovací nožky pro ustavení vodorovná polohy. Provedení v souladu s ČSN 62208, resp. IEC 62208 v platném znění. |  |  |
| Barevné provedení | světlé |  |  |
| Přístup | snadno (jednou osobou) odnímatelné boční panely |  |  |
| Vnitřní uspořádání | Min. 6 vertikálních posuvných lišt pro upevnění zařízení |  |  |
| Kabeláž | Horní a dolní kanály pro vnější kabely, vnitřní prostor pro vedení kabelů na boku racku včetně min. 8 vidících ok. |  |  |
| Bezpečnost | Zámky v předních i zadních dveřích, možnost výměny vložek |  |  |
| Větrání | Perforované přední i zadní dveře, propustnost min. 85% plochy |  |  |
| Uzemnění | Vodivé pospojování všech kovových částí s centrálním přípojným bodem (svorkou) pro uzemnění |  |  |
| Záruka | min. 60 měsíců |  |  |
| **PDU 2 kusy** | Provedení | Rackové provedení, svislé montáž (0 RU) |  |  |
| Základní funkce | Rozvod elektrické energie uvnitř rozvaděče (racku), měření elektrických parametrů a ovládání jednotlivých zásuvek |  |  |
| Zásuvky | výstup min. 20x IEC C13 + 2x IEC C19, vstup kompatibilní s nabízenou UPS (IEC C20) |  |  |
| Elektrické parametry | jednofázový, 230 V, max. 16A |  |  |
| Komunikace LAN | možnost propojení a společného řízení PDU, protokoly http/s, ssh, SNMP, telnet. SMTP a SNMP zasílání informací |  |  |
| Řízení zásuvek | Zpoždění při zapnutí i vypnutí zásuvky, volitelné automatické zpoždění při převedení napájení, možnost vzdáleného řízení přes http, SNMP |  |  |
| Skupiny zásuvek | Vytváření skupiny zásuvek i napříč více propojených PDU, společné ovládání skupiny |  |  |
| Bezpečnost | Možnost nastavení uživatelských oprávnění pro ovládání jednotlivých zásuvek či skupin |  |  |
| Stavové informace | integrovaný grafický displej pro rychlý přehled o stavu napájení a zátěž |  |  |
| Měřené parametry | min. napětí, okamžitý proud a odběr (příkon), kumulativní odběr za období |  |  |
| Ochrana | Vestavěná ochrana proti přetížení, automatické upozornění při přetížení |  |  |
| Záruka | min. 24 měsíců |  |  |
| **Propojení datových rozvaděčů** | Komplet | 2 optické vany 19" s konektory SC (min. 24 ks každá), 20 m SM optického kabelu 24 vláken včetně zavaření vláken do van, montáže van do rozvaděčů a uložení kabelu do lišt v rámci jedné místnosti |  |  |
| Záruka | Záruka min. 3 roky s výměnou v místě instalace |  |  |
| **Síťové přepínače 2 kusy** | Provedení | do racku, rozměr max. 1RU, včetně montážního materiálu do racku |  |  |
| Určení | L2, L3 switch (přepínač), spravovatelný |  |  |
| Porty | 4x 10 Gb SFP+, 16x 1 Gb SFP, 48x 1Gb RJ-45, optické a metalické porty nesdílené |  |  |
| Podavač | podpora směrování a dynamických směrovacích protokolů (min. OSPF) |  |  |
| VLAN | podpora min. 1024 aktivních VLAN a to včetně L3 směrovaných rozhraní |  |  |
| Routování | podpora tvorby virtuálních směrovacích tabulek (VRF, virtual router apod.) |  |  |
| QoS | podpora QoS (min. 8 front na port) |  |  |
| Bezpečnost | podpora 802.1x |  |  |
| Rozšířené funkce | podpora MPLS a VPLS, včetně routování pro napojení na MAN |  |  |
| IPV6 | plný dual stack IPv4 a IPv6 včetně všech služeb směrování |  |  |
| Výkon | přepínání a routování min. 250 Gb/s, propustnost min 190 Mp/s |  |  |
| Sledování toků | integrovaná podpora sledování toků technologie sFlow a exportu toků Netflow nebo kompatibilní |  |  |
| Stohování | podpora rozšířeného stohování po standardizovaných 10Gb portech do minimálního počtu 8 přepínačů (technologie ekvivalentní s technologiemi VSS, IRF nebo VirtualChasis) |  |  |
| Linková agregace | Agregace portů napříč stohem včetně kombinace 10 Gb a 1 Gb, podpora LACP |  |  |
| Správa | podpora SNMP, Syslog, CLI |  |  |
| Záruka | Min. 5 let včetně nároku na nové verze firmware, oprava do 2 pracovních dnů v místě instalace |  |  |
| **Kabely, optické moduly** | Optické moduly | 20x 1Gb SFP SM, BiDi pro nabízené přepínače 4x 10 Gb SPF+ MM pro nabízené přepínače 4x 10 Gb SPF+ SM BiDi, 10 km, pro nabízené přepínače, shodné vlnové délky 2x 10 Gb SPF+ SM BiDi, 10 km, pro stávající přepínače HPE 5130 (JG934A) - komplementární vlnové délky k předchozím modulům 4x 10 Gb SPF+ MM pro stávající přepínače HPE 5130 (JG934A) všechny moduly včetně DMI diagnostiky optický konektor modulů LC záruka min. 36 měsíců |  |  |
| Kabely | 2x optický patch kabel 3m MM - LC-LC 26x optický patch kabel 3m SM - LC-SC záruka min. 36 měsíců |  |  |

| **Komodita K4 - Modernizace archivačních technologií** | | | | |
| --- | --- | --- | --- | --- |
| **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** |
|
| **Šifrování citlivých dat** | Funkce | Rozšíření platformy Microsoft Sharepoint o možnost šifrování ukládaných dat a dokumentů |  |  |
| Certifikáty | Podpora osobních certifikátů (min. 256 bit) pro šifrování a dešifrování osobních dat |  |  |
| Sdílení | Podpora sdílení šifrovaných dat - vlastník dat určuje, kdo je oprávněn data dešifrovat |  |  |
| Vícefaktorová autentizace | Pro přístup k zašifrovaným datům je vyžadována min. dvou-faktorová autentizace uživatele |  |  |
| Privilegovaní uživatelé | Zamezení přístupu k obsahu šifrovaných dat i privilegovaným uživatelům, tj. uživatelům s administrátorskými oprávněními k systému, platformě i infrastruktuře |  |  |
| Auditní log | Podrobné logování operací spojených s nakládáním s šifrovanými daty |  |  |
| Licencování | Licence pro 15 uživatelů, možnost rozšíření pro min. 50 uživatelů |  |  |
| Nouzové zpřístupnění | Možnost definování skupiny uživatelů (2 a více) s oprávněním ke zpřístupnění (dešifrování) dokumentů v nouzové situaci (např. vlastník dat opustil organizaci). Nouzové dešifrování musí být možno provést výhradně společným zadáním přístupových údajů (všechny faktory) všech členů skupiny. |  |  |
| Záruka | Min. 12 měsíců včetně nároku na nové verze |  |  |

| **Komodita K5 - Systém pro správu ICT zařízení** | | | | |
| --- | --- | --- | --- | --- |
| **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** |
| **Správa a evidence ICT zařízení** | Základní požadavky | Systém pro správu a technickou evidenci veškerého počítačového i ostatního ICT zařízení (aktiva). Systém bude určený technicky i licenčně pro podnikové nasazení s profesionální podporu výrobce |  |  |
| Podpora procesů dle ITIL | Systém musí pokrývat následující procesy dle doporučení ITIL:  - Asset and Configuration Management - Software Asset Management |  |  |
| Implementované procesy a funkce | Z procesu Asset and Configuration Management budou implementovány min. následující funkce: - podpora správy konfigurační databáze, musí být uchovávána historie konfiguračních položek  - podpora automatizace zjišťování informací o konfiguračních položkách hardware  Z procesu Software Asset Management budou implementovány min. následující funkce: - řízení životního cyklu spojeného se softwarovými aktivy - automatické zjišťování informací o konfiguračních položkách software  - automatizovaná podpora operativní práce IT správců spojená s řešením a udržením softwarové a licenční čistoty. |  |  |
| Typy majetku | Systém umožní evidovat a spravovat libovolný druh majetku |  |  |
| Automatický sběr dat | Systém umožní automatický neinvazivní (bezagentový) sběr údajů o hardware a software z počítačů |  |  |
| Neznámý software | Automatické odeslání vzorků nerozpoznaného software výrobci k analýze a automatické stažení aktualizovaných signatur pro rozpoznávání. |  |  |
| Mobilní zařízení | Počítače umístěné mimo LAN zadavatele budou se systémem komunikovat zabezpečeným protokolem prostřednictvím internetu bez nutnosti použití VPN |  |  |
| Vizualizace | Grafické zobrazení evidovaného ICT zařízení v hierarchické struktuře. Struktura musí být volně upravitelná podle potřeb Zadavatele |  |  |
| Řízení oprávnění | Systém umožní nastavit oprávnění na úrovní vlastností objektů - např. zamezit zobrazení pořizovací ceny uživatelům |  |  |
| Rozšiřitelnost | Systém umožní přidávat do systému libovolné objekty a přidávat k těmto objektům libovolné vlastnosti. |  |  |
| Dokumenty | V systému musí být možno ukládat libovolné elektronické dokumenty (faktury, licenční certifikáty apod.) a tyto dokumenty propojit s konkrétním objektem nebo více objekty. |  |  |
| Platnost dokumentů | Dokumenty bude možno v systému zneplatnit (vy systému zůstanou zachovány) |  |  |
| Dědičnost | Systém bude podporovat dědičnost vlastností objektů |  |  |
| Protokoly | Předpřipravené podpisové protokoly pro formální úkony při správě majetku (předání/převzetí/převod). |  |  |
| Zabezpečený přístupu | Umožnění bezpečného přístupu do aplikace včetně integrovaného přihlašování do uživatelského prostředí i konzol, řízení oprávnění přístupu k informacím. |  |  |
| Historie záznamů | Systém musí umožnit automaticky evidovat změny provedené s jednotlivými objekty. Rozsah změn min. přesuny, instalace, předávací protokoly včetně informace kdo, kdy změnu provedl. |  |  |
| Reporty | Systém musí umožnit vytváření vlastních pohledů, filtrů a exportů min. do Microsoft Excel. |  |  |
| Zaměstnanecký portál | Umožňuje zaměstnancům kdykoli zobrazit aktuální stav svěřeného ICT zařízení prostřednictvím webového prohlížeče |  |  |
| Intuitivné ovládání | Snadná orientace v přehledech ICT zařízení, možnost přetahování položek myší, podpora kontextových menu pro rychlé úpravy a eliminaci chyb |  |  |
| Lokalizace | Rozhraní systému pro uživatele i správce bude plně lokalizováno do českého jazyka |  |  |
| Vyhledávání | Integrované vyhledávání a filtrování |  |  |
| Automatické názvy | Systém musí umožnit automatické pojmenovávání spravovaných zařízení, min. pomocí definice (přednastavení) číselné řady. |  |  |
| Legislativa | Podpora plnění požadavků Usnesení vlády ČR č. 624/2001 - Pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů |  |  |
| Řízení změn konfigurace | Systém musí umožnit evidenci konfigurace systémů a zařízení. |  |  |
| Vzdálená správa | Systém bude možno integrovat s nástroji pro vzdálenou správu počítačů - min. Vzdálená plocha Windows, VNC a Microsoft Management Console |  |  |
| API | Systém musí umožnit rozšíření pomocí otevřeného rozhraní API na bázi webových služeb. |  |  |
| Import | Systém musí umožnit import ICT zařízení min. ze souborů csv |  |  |
| Správa uživatelů | Systém bude integrovány s Active Directory, bude přebírat uživatele včetně jejich vlastností a organizační hierarchie (nadřízený/podřízený) |  |  |
| Rozšiřitelnost | Systém musí být možno licenčně nebo standardními doplňkovými moduly (ne programovými úpravami) rozšiřitelný o podporu provádění inventarizace ICT zařízení: - integrace s mobilními čtečkami se skenerem čárových kódů pro inventarizaci ICT zařízení - možnost provádění inventur uživateli prostřednictvím uživatelského portálu |  |  |
| Licence | Licence musí umožnit spravovat 350 počítačů a serverů a min. 10 000 ostatních aktiv. Poskytnutá licence bude trvalá |  |  |
| Záruka | Záruka včetně nároku na nové verze a aktualizace signatur pro rozpoznání hw a sw min. 12 měsíců. |  |  |

### Požadavky na architekturu technického řešení

* + - 1. Architektura komodit musí být navržena tak, aby vhodně využívala a doplňovala stávající prostředky TC.
      2. Architektura komodity K1 bude řešena jako modulární, bude obsahovat veškeré obvyklé komponenty – delivery controller, databázové úložiště, publikační webové rozhraní, virtualizační servery, licenční server a další dle uchazečem navrženého designu - a bude umožňovat snadné budoucí rozšíření farmy.
      3. Architektura komodity K2 umožní virtualizovat libovolné běžné datového úložiště (interní úložiště virtualizační appliance, DAS (direct attached storage), SAN úložiště (FC, iSCSI) a publikovat virtualizovaná úložiště prostřednictvím FC (fibre channel – aktuálně používán) a iSCSI (plánované budoucí využití).
      4. Propojení mezi oběma lokalitami (LAN, SAN) bude provedeno jako redundantní. SAN infrastruktury lokalit budou propojeny min. dvěma trasami (2x 8 Gbit) s automatickým překlenutím výpadku jedné trasy při zachování kontinuálního provozu navázaných technologií. Za normálního provozu bude možné připojeným zařízeným nastavit preferovanou trasu. LAN infrastruktury lokalit budou propojeny min. dvěma trasami (2x 10 Gbit) s automatickým překlenutím výpadku jedné trasy při zachování kontinuálního provozu navázaných technologií. Za normálního provozu bude mezi trasami automticky rozkládána zátěž (tzv. load balancing).
      5. LAN architektura komodity K3 bude navazovat na stávající síťové prostředí a bude respektovat a rozvíjet jeho funkčnost (VLAN, routing, apod.).
      6. Architektura komodity K5 bude využívat stávajícího MS SQL serveru pro ukládání dat a konfigurací.

### Požadavky na rozhraní

* + - 1. Řešení komodity K1 (farmy) musí poskytovat uživatelům plně lokalizované (české) pracovní prostředí Windows.
      2. Veškeré nabízené aktivní hardwarové produkty musí disponovat rozhraním SNMP min v2 pro management a vzdálenou správu.

### Požadavky na kompatibilitu s ostatními systémy

* + - 1. Veškeré softwarové komponenty nabízeného řešení s výjimkou diskové virtualizace (K2) budou provozovány ve virtuálním prostředí VMware vSphere a musí být pro běh v tomto prostředí výrobcem podporovány.
      2. LAN přepínače budou kompatibilní s provozovaným systémem HP Intelligent Management Center.

### Požadavky na typy klientů

* + - 1. Řešení K1 (farma) musí umožnit přístup k virtualizovaným aplikacím z operačních systémů Windows 7 a vyšších, OS X, Linux a mobilních zařízení s IOS, Android.
      2. Webové rozhraní pro přístup k externě publikovaným aplikacím komodity K1 (farma) a K5 (Systém pro správu ICT zařízení) musí být funkční v obvyklých internetových prohlížečů – min. Internet Explorer, Edge, Chrome, Firefox, Safari.

### Požadavky na bezpečnost informací

* + - 1. Veškeré nástroje pro správu musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na Active Directory.
      2. Veškeré nástroje pro správu musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa)
      3. Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).
      4. Bezpečnost vnější komunikace webového portálu terminálové farmy a aplikací publikovaných prostřednictvím aplikačního firewallu bude zajištěna použitím tzv. „hvězdičkového“ (wildcard) certifikátu veřejné certifikační autority, tj. takové autority, jejíž kořenový certifikát je součástí běžných operačních systémů a je automaticky obnovován v rámci běžných updatů operačních systémů. Certifikát není předmětem dodávky.

## 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** |
| **Centrální řízení záložních napájecích zdrojů** | | | |
| 1 | Nabízené UPS budou plně kompatibilní se současným provozovaným systém pro správu UPS Eaton Intelligent Power Manager pro zajištění centrální správy serverových UPS a jednotné automatické řízení odstávek technologií u obou datových centrech Moskevská a U spořitelny |  |  |
| **Minimalizace nároků na provoz a správu systémů** | | | |
| 2 | Veškerá nabízená softwarová řešení včetně diskové virtualizace budou provozována v prostředí Microsoft Windows |  |  |
| 3 | Přepínače LAN přepínačů K3 budou založeny na systému Comware pro zachování jednotné správy LAN a MAN |  |  |
| 4 | Řešení komodity K4 pro šifrování dat a dokumentů bude disponovat rozhraním na bázi webových služeb nebo obdobné technologie na hromadné uložení a zašifrování dokumentů. |  |  |
| **Prokázání legislativní shody** | | | |
| 5 | Pro zajištění dodržování podmínek Usnesení vlády ČR č. 624/2001 bude systém komodity K5 pro správu ICT zařízení certifikován na shodu s tímto Usnesením oprávněnou certifikační autoritou. Certifikát bude součástí nabídky. |  |  |

## 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. 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 před zahájením realizace dodávek, tzn. po provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu a musí být výslovně schválena Zadavatelem.
         2. Dodávka a implementace předmětu plnění včetně technické podpory podle prováděcí dokumentace.
         3. Zajištění projektového vedení realizace předmětu plnění.
         4. Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.
         5. Zpracování materiálů pro školení a provedení školení
         6. Zajištění zkušebního provozu
         7. Návrh a provedení akceptačních testů.
         8. Předání do plného 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 MMKV, tj. mimo pracovní dny 7 – 17 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: Rekonstrukce terminálové farmy |
| * 1. Vytvoření detailního návrhu rekonstrukce terminálové farmy včetně plánu přechodu uživatelů a postupu rozšiřování farmy administrátory MMKV.   2. Zajištění souběžného provozu stávající a modernizované farmy a plynulého přechodu uživatelů na novou farmu s minimálním omezením jejich pracovní činnosti. Akceptovatelné je neopakované omezení práce uživatele max. na 15 min.   3. Provedení aplikačních testů všech publikovaných aplikaci a řešení případných neshod a nekompatibilit   4. Otestování výkonu a stability implementovaného řešení před započetím převodu uživatelů.   5. Zajištění funkčnosti tokenů s uživatelskými certifikáty připojených ke koncovým zařízením (tenkým klientům) v prostředí publikovaných aplikací   6. Zajištění funkčnosti periferních zařízení (flash disky, skenery, fotoaparáty) připojených ke koncovým zařízením (tenkým klientům) v prostředí publikovaných aplikací   7. Návrh a realizace konfiguračních změn infrastruktury (virtualizační platforma, LAN, SAN   8. Návrh a realizace vhodného začlenění aplikačního firewallu do stávajícího prostředí, zejména koexistence se stávajícími firewally – vymezení rolí a pravidel, využití synergií.   9. Návrh a realizace dvoufaktorové SMS autentizace uživatelů přistupující k publikovaným aplikacím mimo LAN, tj. prostřednictvím internetu, RKI, MAN (s výjimkou lokality U Spořitelny).   10. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti |
| K2: Modernizace datového úložiště |
| * 1. Detailní analýza současného způsobu ukládání dat, návrh a provedení optimalizace včetně vhodného rozložení veškerých datových úložišť (SAN, NAS, páskové knihovny, virtualizační appliance) do 2 lokalit – viz. K3   2. Modernizace diskové virtualizace včetně zachování (popř. plné migrace) stávajících dat včetně dat uložených v NAS.   3. Návrh a realizace implementačního postupu neomezujícího činnost uživatelů MMKV   4. Výkonová optimalizace pro klíčové a výkonově náročné systémy dle provedené analýzy – min. databáze, servery virtualizace aplikací terminálové farmy.   5. Implementace rozšířených funkcionalit pro serverovou virtualizaci – min. integrace správy diskové virtualizace do prostředí vCenter, zprovoznění VAAI.   6. Návrh a provedení související změn zálohovacích úloh   7. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti |
| K3: Modernizace lokality U spořitelny |
| * 1. Návrh a realizace vhodného rozložení technologií a jejich rolí mezi lokalitami včetně jejich umístění, propojení a konfigurace.   2. Veškeré hlavní komunikační trasy (SAN, páteřní a serverové LAN) a musí být provedeny redundantní s automatickým překlenutím výpadku jedné trasy   3. Návrh a realizace implementačního postupu neomezujícího činnost uživatelů MMKV   4. Začlenění UPS do centrální správy (bude-li podporovat), automatizace odstavení serverové virtualizace při výpadku napájení.   5. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti |
| K4: Upgrade archivačních technologií |
| * 1. Analýza požadavků na evidenci a správu současné konfigurace a uložených data, návrh a provedení upgrade na poslední dostupné verze software, související úpravy a optimalizace nastavení platforem a vytvořených aplikací   2. Realizace šifrování ukládaných dat pro platformu Sharepoint   3. Návrh a provedení akceptačních testů |
| K5: Systém pro správu ICT zařízení |
| * 1. Návrh konfigurační databáze pro zavedení do systému   2. Návrh vhodného způsobu iniciačního zavedení evidovaného ICT zařízení (naplnění databáze)   3. Implementace systému dle provedených návrhů a doporučení výrobce   4. Návrh a provedení akceptačních testů |

### Požadavky na předimplementační analýzu

* + - 1. Před implementací řešení zpracuje Uchazeč předimplementační analýzu, minimálně pro následující oblasti:
         1. Detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TC ORP.
         2. Způsob začlenění nabízených komodit do prostředí TC.
         3. Síťová infrastruktura ve vztahu k plánovanému využití.
         4. SAN infrastruktura ve vztahu k plánovanému využití.
         5. Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
         6. Integrace nabízených softwarových systémů.
         7. Rekonfigurace stávajících systémů.
         8. Dopady implementace na dostupnost a funkčnost stávajících služeb.
         9. Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).
         10. Integrace s virtualizační platformou VMware vSphere ve vysoce dostupném režimu a integrace s dohledovým systémem Zadavatele   
             min. doporučení parametrů pro sledování).
         11. Požadované součinnosti Zadavatele a jejich rozsah.
         12. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.
      2. Výstupem předimplementační analýzy bude písemná zpráva, která podléhá schválení Zadavatelem.

### 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 do stávajícího prostředí technologického centra.
      2. Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem.
      3. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
         1. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,
         2. Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TC ORP (vSphere, LAN, SAN atd.).
         3. Způsob zajištění potřebného HW a SW,
         4. Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
         5. Detailní návrh a popis postupu implementace předmětu plnění,
         6. Detailní popis zajištění bezpečnosti informací,
         7. Detailní harmonogram realizace včetně uvedení kritických milníků,
         8. Návrh designu síťového a bezpečnostního řešení a jeho konfigurace,
         9. Návrh designu aplikačních řešení,
         10. Vazby na stávající systémy a jejich konfigurace,
         11. Návrh akceptačních kritérií a akceptačních testů.

### Požadavky na zajištění projektového vedení

* + - 1. Uchazeč zajistí projektové vedení po celou dobu realizace zakázky certifikovaným specialistu. 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 podpisu smlouvy o dílo. Čísla značí počet kalendářních dnů.

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Etapa projektu – činnost** | **Zahájení etapy** | **Ukončení etapy** |
| 1 | Předimplementační analýza a zhotovení Prováděcí dokumentace | D | D+20 |
| 2 | Předání Prováděcí dokumentace Zadavateli, připomínkové řízení | D+20 | D+30 |
| 3 | Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem | D+30 | D+40 |
| 4 | Dodávky a implementace | D+40 | D+100 |
| 5 | Školení uživatelů a administrátorů | D+90 | D+120 |
| 6 | Zkušební provoz | D+90 | D+110 |
| 7 | Akceptační testy | D+100 | D+120 |
| 8 | Zahájení plného provozu | D+140 | - |

* + - 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.
      2. Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin
      3. Minimální rozsah školení je 24 hodin.
      4. Školení bude probíhat v sídle Zadavatele.
      5. Předpokládá se účast max. 4 administrátorů.
      6. Náklady na školení 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 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 20 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. Součástí technické podpory bude spolupráce s administrátory Zadavatele při řešení nekompatibilit aplikací a systémů.
      9. 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 TC ORP

* + - 1. Zadavatel požaduje detailní návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění a také stávajících technologií TC ORP 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 TC ORP nebo událost, která způsobila nehodu nebo potenciálně mohla způsobit omezení případně nefunkčnost TC ORP. 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 Dodavatele 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. **Incident**- událost způsobující odchylku od očekávané funkce Prvku IT, která způsobuje nebo může způsobit přerušení anebo snížení kvality této funkce.
      14. **Priorita Incidentu** - závažnost Incidentu dle klasifikace Kontaktní osoby Zadavatele.
      15. **Koncová zařízení** - počítače uživatelů, jejich programové vybavení a periferní zařízení k počítačům připojená (např. tiskárny, skenery).
      16. **Monitorování** - sledování Prvků IT prostředky Vzdáleného přístupu, zda jsou funkční. Sledování, zda provozní charakteristiky Prvků IT nepřesahují stanovené hodnoty, eventuálně neklesají pod stanovené hodnoty. Monitorováním se případně rozumí sledování a archivování jejich provozních charakteristik.
      17. **Proaktivní monitorování**-monitorování prováděné dle charakteru provozu a činnosti Prvku IT v režimu 24x7 (komunikační infrastruktura) nebo v režimu 9x5 (technologické centrum).
      18. **Náhradní zařízení** – zařízení podobných vlastností (parametrů).
      19. **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 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. **Monitorování –** jedná se o službu nepřetržitého online monitorování systémů s upozorněním na kritické nebo neobvyklé události, upozornění budou automaticky zasílána oprávněným pracovníkům Zadavatele. Součástí služby je vzdálený přístup k aktuálním i historickým údajům o stavu systému. Monitorování je souborem takových opatření, která umožňují v kterémkoli čase znát stav Systému a Systémů třetích stran, minimálně v rozsahu:
          1. monitoring operačních systémů
          2. monitoring sítě a síťových propojení Systému a Systémů třetích stran
          3. monitoring databázových systémů
          4. monitoring diskových úložišť
          5. monitoring Prvků IT třetích stran, které mohou ovlivňovat chod Systému, pokud jsou tyto Prvky IT součástí předmětu plnění nebo mohou mít na funkci a/nebo dostupnost Prvku IT negativní vliv způsobující incident kategorie A nebo B.
      23. **Profylaxe -** profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.

### Obecná pravidla provozu TC ORP

* + - 1. Provozem TC ORP se rozumí chod a udržování jeho jednotlivých částí, 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 MMKV. Technologické místnosti jsou vybaveny jednotnou platformou se stejným základním nastavením (práva, rozdělení disků, instalované aplikace). 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 MMKV 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.

### Inicializace – převzetí do provozu

* + - 1. Při zahájení poskytování služeb se uchazeč musí seznámit s jednotlivými prvky IT, které přebírá do provozu a s jejich specifickými provozními režimy.
      2. V období inicializace nebudou ze strany zadavatele uplatňovány sankce za nedodržení podmínek SLA.
      3. Uchazeč v nabídce detailně popíše způsob přebírání jednotlivých prvků IT do provozu, harmonogram přechodu jednotlivých prvků IT ze správy zadavatele do správy uchazeče a předpokládanou součinnost ze strany zadavatele.
      4. Uchazeč v průběhu inicializace připraví detailní matici potřebných přístupových účtů a požadovaných oprávnění k jednotlivým prvkům IT. Účty budou vytvářeny jmenné – pro konkrétní osoby – a ke každému požadavku na zřízení účtu bude přiložen profesní životopis osoby pro niž má být účet zřízen, prokazují odborné kompetence odpovídající požadovaným oprávněním.
      5. Délka období inicializace nesmí být delší než 3 měsíce, přičemž zahájení této doby se počítá od doby předání implementační části předmětu plnění do ostrého provozu.

### 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 byli identifikovány v rámci předimplementační analýzy. Počet sledovaných parametrů nesmí být prakticky omezen, administrátoři MMKV musí mít přístup ke sledovaným parametrům alespoň v režimu čtení.
         3. Řešení Požadavků a Incidentů – dle podmínek SLA
         4. Profylaxe a patch management
         5. Hotline podpora v režimu 9x5
         6. Odborná podpora v režimu 9x5 – vzdálené konzultace pro podporované služby/produkty
         7. Celkový rozsah služeb Hotline a Odborné podpory v rámci měsíčního paušálu 6 hodin.
         8. Minimální dostupnost služeb služeb Hotline a Odborné podpory v režimu 9x5.
         9. Služby Hotline a Odborné podpory budou poskytovány pro ad-hoc řešení požadavků a konzultací. Zadavatel požaduje dostupnost specialisty pro řešenou problematiku do 15 minut u služby Hotline a do 1 hodiny i služby Odborné podpory.
         10. Služby Hotline a Odborné podpory budou poskytovány na rámec služeb specifikovaných katalogovými listy (viz. bod (4)).
      2. Další služby v rámci měsíčního paušálu
         1. Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
         2. Servisní dispečink pro telefonické zadávání požadavků dostupný v pracovní dny 7-18 hod.
      3. Pro případ, že bude zadavatel požadovat služby odborné podpory podle odst. (1) písm. (g) (např. konzultace, servisní zásahy, instalace, konfigurace, řešení problémů atp.) nad rámec uvedeného rozsahu služeb zahrnutých v měsíčním paušálu (tj. nad rámec 6 hodin), dodavatel tyto služby nacení v kalkulaci nabídkové ceny též jako hodinovou sazbu za službu (označení služby „EXP-WRK“).
      4. Seznam prvků pokrývaných službou zabezpečení provoze je uveden v kapitole 7.11.
      5. Detailní specifikace požadavků a jejich rozsah pro jednotlivé kategorie prvků IT jsou v katalogových listech, v Příloze 3,b 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 TC ORP 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. Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS /tel)
      5. Report bude za příslušné období vždy obsahovat minimálně:
  1. Informace o provedených změnách v TC ORP 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 (disková a serverová virtualizace, diskové úložiště, terminálová farma, centrální síťové prvky, SQL databáze, řadiče Active Directory). Přítomnost technika vždy bude stanovena po vzájemné dohodě v předstihu nejméně 10 pracovních dnů předem.
      2. Zadavatel požaduje, aby při řešení Incidentu/vady kategorie A byl v lokalitě zadavatele (on-site) přítomen technik uchazeč, který bude schopen incident řešit a to takto:
         1. do jedné hodiny do nahlášení incidentu zadavatelem nebo zjištění incidentu uchazečem, nelze-li incident řešit vzdáleně,
         2. do jedné hodiny od vyžádání přítomnosti technika zadavatelem.

### 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 ke 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 | 1 hod | Nejpozději do 24 hod |
| B | 15 min | 4 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 niž je požadováno Zabezpečení provozu

| **Prvky IT** | | | | |
| --- | --- | --- | --- | --- |
| **Prvek** | **Popis** | **Počet** | **Platnost stávající záruky/ Požadovaná úroveň záruky** | **Poznámka** |
| **Hardware** | | | | |
| 1 | Veškeré hardwarové prvky dodané v rámci této zakázky | x | dle nabídky |  |
| 2 | Blade šasi HP C7000 včetně 2x SAN switch 8 Gb, 2x 1Gb pass-through modul, 2x management modul + příslušenství (ventilátory, zdroje, SFP apod.) | 2 | Do konce 2017 /  oprava NBD on-site |  |
| 3 | Blade server BL460 G7 | 7 | Bez záruky /  oprava NBD on-site |  |
| 4 | Blade server BL460 G8 | 2 | Do konce 2017 /  oprava NBD on-site |  |
| 5 | HP MSA 2000G3, 2x FC řadič, provedení 3,5" včetně HDD | 5 | Do konce 2017 /  oprava NBD on-site | disky 600GB/15krpm, 450GB/15krpm, 3TB/7.2TB, osazeno cca. 90% pozic |
| 6 | Expanzní police D2000 k MSA 2000G3 (2x 2,5", 4x3,5") | 6 | Do konce 2017 /  oprava NBD onsite | disky 600GB/15krpm (3.5"), 600GB/10krpm (2.5"), 3TB/7.2TB, osazeno cca. 90% pozic |
| 7 | HP DL 380p G8 8SFF | 3 | Bez záruky /  oprava NBD on-site |  |
| 8 | HP 8/8 (8) Full Fabric Ports Enabled SAN Switch s 12 aktivními porty, včetně 8 Gb SFP v aktivních portech | 2 | Bez záruky /  Oprava NBD on-site |  |
| 9 | HP MSL4048 2 LTO-5 3000 FC Tape Library | 1 | Do konce 2017 /odezva NBD on-site |  |
| **Software** | | | | |
| 10 | Veškeré softwarové prvky a systémy dodané v rámci této zakázky | x | dle nabídky |  |
| 11 | Terminálová farma Citrix | x | - | Platnost Maintenence zajišťuje Zadavatel na vlastní náklady mimo tuto zakázky, poskytne přístup Uchazeči |
| 12 | Zálohovací systém Veeam | x | - | Platnost Maintenence zajišťuje Zadavatel na vlastní náklady mimo tuto zakázky, poskytne přístup Uchazeči |
| 13 | Virtualizační platforma Vmware | x | - | Platnost Maintenence zajišťuje Zadavatel na vlastní náklady mimo tuto zakázky, poskytne přístup Uchazeči |
| 13 | Archivační platforma IBM FileNet | x | - |  |
| 14 | Dokumentová platforma Sharepoint + Nintex | x | - |  |
| 15 | Systémové služby platformy - řadiče Active Directory, Exchange, SQL server | x | - |  |

### 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.