# Vymezení předmětu plnění veřejné zakázky

## Předmět plnění veřejné zakázky

* + - 1. Předmětem plnění veřejné zakázky jsou **dodávky zařízení a návazných služeb** (dále také jen „řešení“) pro zajištění výměny centrálních přístupových prvků.
			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 | Virtualizační platforma | 1 |
| K2 | Komunikační infrastruktura | 1 |
| K3 | Bezpečnostní systém | 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 ORP situováno v lokalitě Moskevská, jeho záloha pak v lokalitě U Spořitelny.
			2. Technologické centrum bylo vybudováno z původní serverovny úřadu v roce 2012 v rámci Výzvy 06 IOP, dále rozšířeno v rámci Výzvy 09 IOP, 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, G8 a G10. 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 pásková knihovna MSL 4048, obě Blade šasi, zálohovací server a 2 appliance diskové virtualizace Datacore 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 vSpherev 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 technologií je v lokalitě Moskevská 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 4048. 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 2012.
			10. Síťová infrastruktura LAN je osazena převážně aktivními prvky HP (HPE) řad 51xx, 55xx a 5800.
			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 XenApp provozovanou na virtuálních serverech Windows 2016. Pro vzdálený přístup k aplikacím je využívána technologie Citrix Netscaler, který slouží také jako aplikační firewall.
			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. 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, 5800 a 75xx a je monitorována HP Intelligent Management Center (IMC), který je částečně využíván i pro monitoring LAN.
			17. Ve 2018-2019 byl zadavatelem realizován projekt „Zajištění konektivity a pořízení vybavení odborných učeben pro základní školy Karlovy Vary – vnitřní konektivita ZŠ – sdílená část“, financovaný z výzvy IROP č. 47, cílem projektu bylo zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol[[1]](#footnote-1) (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí základních škol zřizovaných Zadavatelem.
			18. 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 obdobně jako KI.
			19. Pro účely správy dokumentů a provoz specifických aplikací (např. Registr dlužníků) využívá MMKV platformy Microsoft Sharepoint Foundation 2013.
			20. Pro účely archivace dokumentů (např. stavebního archivu) využívá MMKV platformu IBM FileNet - Business proces manager.
			21. Pro sledování bezpečnostních událostí je využíván systém SIEM USM - Unified Security Management (AT&T Cybersecurity)
			22. Pro evidenci organizační struktury a vytváření a správu uživatelských účtů na základně informací z personálního systému FLUXPAM (FLUX, spol. s r.o.) je využíván systém IDM AC Identita (AUTOCONT a.s.)
			23. Hlavním informačním systémem využívaným úřadem je GINIS (GORDIC spol. s r.o.).
			24. Pro správu dokumentů a spisů je využívána elektronická spisová služba AthenA s rozšiřujícím modulem iUsnesení pro správu dokumentů rady a zastupitelstva (S&T PilsCom s.r.o.).
			25. 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 uchazeče 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 uchazeče.

### 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 navýšení výpočetního výkonu TC ORP a začlenění nových zařízení do TC bez omezení poskytování jeho služeb,
				2. způsob konsolidace a zvýšení dostupnosti centrální infrastruktury KI, včetně souvisejících rekonfigurací a přepojení městských organizací (jejich hraničních zařízení)
				3. způsob zavedení bezpečnostní služby typu NGFW (next generation firewall) městským organizacím na KI včetně náhrady stávajícího NGFW
			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. Uchazeč ve své nabídce detailně popíše vazby na stávající systémy Zadavatele, které jsou nezbytné pro správné fungování řešení nabízeného Uchazečem.
			6. Pokud uchazečem navržené řešení vyžaduje využití konkrétních softwarových produktů, neobsažených v popisu předmětu plnění, a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
			7. 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.
			8. 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.
			9. Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů preferuje 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.
			10. Uchazeč bude při implementaci respektovat provozní řád zadavatele, vítězný uchazeč bude s provozním řádem seznámen před podpisem Smlouvy o dílo.
			11. Veškeré produkty, které uchazeč dodává v rámci plnění Zadavateli, musí splňovat následující podmínky:
				1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
				2. mají plnou záruku od výrobce,
				3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
				4. obsahují všechny nezbytné licence na používání příslušného softwaru,
				5. jsou určeny pro provoz v České republice,
				6. z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

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

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

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). Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena Zadavatelem.

### Specifické požadavky K1 – Virtualizační platforma

* + - 1. Pro navýšení výpočetní kapacity TC bude pořízen nový server do stávajícího Blade šasi.
			2. Pro provoz systémů a aplikací budou na novém serveru pořízeny licence operačních systémů.
			3. Pro virtualizaci serveru a zálohování hostovaných systémů budou využity stávající licence virtualizačního a zálohovacího software.
			4. Součástí dodávky je kompletní zprovoznění serveru včetně jeho virtualizace, napojení na síťovou infrastrukturu, diskové úložiště, zálohovací systém a monitorovací systém.

### Specifické požadavky K2 – Komunikační infrastruktura

* + - 1. V rámci komodity budou dodány síťové přepínače pro rozšíření stávajícího vysoce dostupného stohu a provedena rekonfigurace stohu pro roli centrálního vysoce dostupného aktivního prvku KI.
			2. V rámci komodity dojde k nahrazení současného centrálního prvku KI (HP 7500) rekonfigurovaným stohem. Součástí dodávky budou veškeré analytické, návrhové a konfigurační služby včetně souvisejících konfigurací aktivních prvků HP 5500 ve vzdálených lokalitách (organizacích zadavatele), přepojení tras a otestování kvality a stability komunikace.
			3. V rámci předmětu plnění budou přepojeny příspěvkové organizace města a budovy zadavatele, celkem se jedná o 27x lokalit:

|  |  |  |
| --- | --- | --- |
| **Adresa, popř. typ lokality** | **Kategorie lokality** | **Bude přepojeno v rámci předmětu plnění** |
| Magistrát města, Moskevská 1281/21, Karlovy Vary – centrální lokalita | 1 | ANO |
| Magistrát města Karlovy Vary, U Spořitelny 2 | 1 | ANO |
| Městská policie Karlovy Vary, Moskevská 34 | 1 | ANO |
| Správa přírodních léčivých zdrojů a kolonád, Lázeňská 18/2 | 1 | ANO |
| ZŠ Karlovy Vary, Truhlářská 681/19 | 2 | NE / Závazek dodržení standardu konektivity  |
| ZŠ J. A. Komenského, Kollárova 533/19 | 2 | NE / Závazek dodržení standardu konektivity |
| ZŠ pro žáky se specifickými poruchami učení, Mozartova 7 | 2 | ANO |
| ZŠ Karlovy Vary, 1. Máje 1 | 2 | NE / Závazek dodržení standardu konektivity |
| Mateřská škola Komenského, Komenského 7 | 2 | ANO |
| Mateřská škola "Notička", E. Destinové 1 | 2 | ANO |
| Mateřská škola "Na KOPEČKU", Mozartova 4 | 2 | ANO |
| Mateřská škola "Sluníčko", Východní 6 | 2 | ANO |
| Mateřská škola, Javorová 211 | 2 | ANO |
| Správa lázeňských parků, U Solivárny 2 | 1 | ANO |
| Lázeňské lesy Karlovy Vary, Na Vyhlídce 35 | 1 | ANO |
| Husovo náměstí 2 | 1 | ANO |
| Městská policie Karlovy Vary, Školní 9 | 1 | ANO |
| Základní škola jazyků, Libušina 1032/31 | 2 | NE / Závazek dodržení standardu konektivity  |
| ZŠ Karlovy Vary, Krušnohorská 735/11 | 2 | NE / Závazek dodržení standardu konektivity  |
| ZŠ Karlovy Vary, Konečná 917/25 | 2 | NE / Závazek dodržení standardu konektivity  |
| ZŠ a ZUŠ Rybáře, Šmeralova 15 | 2 | ANO |
| ZŠ Dukelských hrdinů, Moskevská 1117/25 | 2 | NE / Závazek dodržení standardu konektivity  |
| ZŠ Karlovy Vary, Poštovní 1743/19 | 2 | NE / Závazek dodržení standardu konektivity  |
| ZŠ Karlovy Vary (odloučené pracoviště), Modenská 15 | 2 | ANO |
| Mateřská škola U brodu, U Brodu 73 | 2 | ANO |
| Mateřská škola "Studánka", Krymská 10 | 2 | ANO |
| Mateřská škola "Zdravá mateřská školka", Krymská 12 | 2 | ANO |
| Mateřská škola Hornická, Hornická 66 | 2 | ANO |
| Mateřská škola, Krušnohorská 16 | 2 | ANO |
| Mateřská škola, Sedlecká 5 | 2 | ANO |
| Mateřská škola, Fibichova 5 | 2 | ANO |
| Mateřská škola, Truhlářská 11 | 2 | ANO |
| Mateřská škola, Mládežnická 6 | 2 | ANO |
| Mateřská škola, kpt. Jaroše 6 | 2 | ANO |
| Mateřská škola, Vilová 1 | 2 | ANO |

* + - 1. U lokalit, kde je uveden „Závazek dodržení standardu konektivity“, je nutné zajistit splnění všech podmínek standardu konektivity dle IROP (podmínka poskytovatele dotace) i po realizaci předmětu plnění této veřejné zakázky, které technicky ovlivní část zařízení, využívaných výše označenými lokalitami.
			2. Konfigurace prvků komunikační infrastruktury budou vycházet ze stávajících konfigurací (konfigurační soubory a dokumentace KI bude poskytnuta vítěznému uchazeči), které budou optimalizovány s ohledem na aktuální doporučení výrobců a osvědčené praktiky (best practice), zejména v oblasti kybernetické bezpečnosti.
			3. Součástí komodity bude převzetí stávajících monitorovacích a notifikačních pravidel ze systému IMC a jejich úprava a přenesení do monitorovacího systému TC.

### Specifické požadavky K3 – Bezpečnostní systém

* + - 1. Nabízené řešení bude tvořit kombinace dvou nově pořízených firewallů sestavená a zkonfigurovaná do vysoce dostupného firewallu-clusteru, tím bude zajištěna dostatečná ochrana směrem dovnitř MMKV a jeho organizací a stejně tak bude možné zamezit nežádoucí aktivitě směrem ven. Firewally budou shodně typu NGFW (Next Generation Firewall). Takové firewally umožňují při konfiguraci pravidel intuitivně využívat logické objekty srozumitelné i bez speciálních znalostí (např. názvy aplikací místo portů, jména uživatelů/počítačů místo IP adres apod.). Významným způsobem se tak zjednodušuje správa těchto sofistikovaných zařízení a současně snižuje riziko možného omylu obsluhy.
			2. Firewall-cluster bude v souladu s celkovou filosofií komunikační infrastruktury zapojen do páteřních přepínačů vícenásobnými 1Gb spoji, aby byla zachována koncepce redundance klíčových centrálních prvků, stejně jako v návrhu virtualizační platformy.
			3. Firewall umožní vytváření tzv. virtuálních kontextů (virtuálních firewallů) a tyto budou využity pro specifická nastavení pravidel a politik pro MMKV a jeho organizace (resp. skupiny organizací). Virtuální kontexty dále umožní delegovat správu kontextu v přesně definovaném rozsahu na správce v organizacích.
			4. Integrovaný antivirus musí odhalovat a odstraňovat viry, červy a spyware v reálném čase. Bude kontrolovat přílohy příchozích a odchozích emailů (SMTP, POP3, IMAP) a veškerý provoz přes FTP a HTTP včetně webových emailů, to vše bez snížení výkonu zaznamenatelného uživateli. Antivirové gateway zastavují viry a červy dříve, než mohou vniknout dovnitř sítě.
			5. Firewall bude zastavovat útoky, které obcházejí běžné host-based antivirové systémy, přičemž musí reagovat v reálném čase na rychle se šířící útoky.
			6. Zařízení poskytne podporu VPN standardů IPSec, PPTP a L2TP a umožní bezpečnou komunikaci mezi sítí a klienty a ověří uživatele, zašifruje data a spravuje relace.
			7. Zařízení umožní díky profilování provozu kontrolovat síťový provoz za účelem optimalizace nebo garance výkonu, nízké čekací doby a šířky pásma pro danou službu.
			8. Zařízení umožní třídění paketů, systém řazení ve frontě, prosazování pravidel, regulaci přetížení, kvalitu služby (QoS) a dostupnost. Jelikož šířka pásma je limitovaný zdroj, profilování provozu pomáhá seřadit síťové služby podle důležitosti a prioritizovat je. Racionálně spravované profilování provozu zlepšuje dobu odezvy, dostupnost služby a využití celého pásma bez výpadků způsobených intenzivním multimediálním či peer-to-peer provozem.
			9. Firewall dále bude testovat veškerý webový obsah na výskyt známých nežádoucích URL, blokuje nevhodný obsah a nebezpečné Java aplety, cookies, Active X skripty před jejich vstupem do sítě. Filtrace budou také uživatelsky přizpůsobitelná, aby umožnily síti přidat další URL pro zabránění přístupu k dalším nežádoucím stránkám.
			10. Stávají firewall nemá již dostatečný výkon pro zajištění plné bezpečností kontroly (SSL inspekci, aplikační kontrolu) aktuálního provozu a bude v rámci projektu nahrazen a vyřazen.

### 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 - Virtualizační platforma**  |
|  **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 server1 ks**  |  Provedení  |  Blade server  |   |   |
|  Procesor  |  Minimálně 2x procesor osmi-jádrový (dohromady tedy min 16 jader). Výkon serveru dle http://www.spec.org:SPECrate2017\_int\_base min 105 bodůSSPECrate2017\_fp\_base min 120 bodů  |   |   |
|  Pevné disky  |  2x SSD, min. 240 GB pro hypervizor  |   |   |
|  Paměť  |  minimálně 384 GB RAM, min. 2600 MT/s  |   |   |
|  Rozšiřitelnost  |  rozšiřitelnost RAM min. na 700 GB bez výměny RAM modulů  |   |   |
|  RAID  |  řadič RAID 0,1, 10, 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 36 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 systémů. Licence musí umožnit provoz předchozích verzí systému - tzv. downgrade |   |   |

| **Komodita K2 - Komunikační infrastruktura**  |
| --- |
|  **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**  |
|  **Centrální přepínač 2 ks**  |  Základní parametry  |  L2/L3 přepínač v rackovém provedení max. 1U  |   |   |
|  Propustnost  |  neblokovaná architektura, propustnost min. 200 Gb  |   |   |
|  Porty  |  8x 10 Gb SFP+, 24x 1 GbE  |  |   |
|  Agregace portů  |  podpora LACP  |  |   |
|  Směrování  |  statické a dynamické routování, policy based routing  |   |   |
|  Řízení provozu  |  víceúrovňový QoS  |   |   |
|  VLAN  |  VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření  |   |   |
|  Ověřování uživatelů a zařízení  |  podpora 802.1X  |   |   |
|  Dualstack  |  plný IPv4 a IPv6 dualstack včetně směrování a QoS  |   |   |
|  Pokročilé funkce  |  plná podpora MPLS a VPLS včetně L2 a L3 MPLS VPN  |   |   |
|  Stohování  |  pokročilé stohování - 2 (a více) přepínačů ve stohu se chovají jako jeden z pohledu správy i připojených zařízení (min. 8 zařízení ve stohu)  |   |   |
|  Kompatibilita  |  kompatibilní s přepínači HPE 5800 na úrovni pokročilého stohování  |   |   |
|  Sledování toků  |  export síťových toků (Netflow nebo ekvivalent)  |   |   |
|  Monitoring a správa  |  plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní  |   |   |
|  Záruka  |  min. 60 měsíců, oprava/výměna zařízení max. do 2 pracovních dnů po nahlášení závady, včetně nároku na opravné verze firmware  |   |   |
|  **Optické prvky a kabely**  |  SFP+ moduly  |  6 ks modulů SFP+ 10 Gb, MM včetně DMI diagnostiky pro nabízený centrální přepínač, LC konektor  |   |   |
|  SFP moduly  |  56 ks modulů SFP 1 Gb, SM 20 Km,WDM BiDi, včetně DMI diagnostiky pro nabízený centrální přepínač a přepínače HP 5500, LC konektor. 28 párů 1310 a 1490 nebo 1550 nm  |   |   |
|  Optické patch kabely  |  4 ks kabel MM s konektory LC-LC, délka 1 m 2 ks kabel MM s konektory LC-LC, délka 5 m28 ks kabel SM s konekrory LC-E2000, délka 10 m  |   |   |
|  Záruka  |  36 měsíců  |   |   |

| **Komodita K3 - Bezpečnostní systém**  |
| --- |
|  **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**  |
|  **Firewall2x**  |  Provedení  |  hardwarový firewall pro umístění do datového rozvaděče 19", výška max. 1U, včetně montážního materiálu  |   |   |
|  NGFW  |  zařízení typu next generation firewall - https://en.wikipedia.org/wiki/Next-generation\_firewall  |   |   |
|  Porty  |  min 14x 1GbE (min. 2x WAN) a 4x 1 Gb SFP (nesdílené), USB pro ext. modem  |   |   |
| Agregace portů | Podpora agregace (slučování) portů pro rozkládání zátěže a vysokou dostupnost – podpora IEEE 802.3ad, LACP. Podpora VLAN na agregovaných portech |  |  |
|  Propustnost  |  min. 20 Gbps pro pakety 512b  |   |   |
|  Úložiště  |  interní úložiště typu SSD pro ukládání logů, reportů apod., velikost min. 450 GB  |   |   |
|  Počet současných spojení  |  min. 2 milióny  |   |   |
|  Propustnost SSL VPN  |  min. 500 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 současně připojených klientů  |   |   |
|  Propustnost IPSec VPN  |  min. 5 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 současně připojených klientů a 50 sítí (site-to-site VPN)  |   |   |
|  Propustnost IPS  |  min. 2 Gbps pro vzorový provoz (tzv. Enterprise mix) - aktivní firewall, aplikační kontrola, ochrana proti škodlivému kódu, logování  |   |   |
|  Propustnost NGFW  |  min 1.8 Gbps - aktivní firewall, aplikační kontrola, IPS, logování  |   |   |
|  Propustnost SSL inspekce  |  min. 800 Mbps při aktivní IPS  |   |   |
|  Kombinovaná propustnost  |  Firewall + aktivní IPS + aplikační kontrola + antimalware min. 1 Gbps pro běžný provoz  |   |   |
|  Politiky, pravidla  |  podpora min. 8000 politik/pravidel firewallu  |   |   |
|  Virtualizace  |  min. 10 virtuálních kontextů  |   |   |
|  Vysoká dostupnost  |  režimy Active/Passive i Active/Active se společnou konfigurací, vyhrazené porty pro v  |   |   |
|  Dualstack  |  podpora současného běhu IPv4 a IPv6  |   |   |
|  IPS  |  Intrusion Protection System (IPS) – detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.  |   |   |
|  Aplikační kontrola  |  detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portuKontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…)  |   |   |
|  Antivir  |  antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)  |   |   |
|  Kategorizace a blokace provozu  |  založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne  |   |   |
|  Antispam  |  antispamová a antivirová inspekce elektronické pošty  |   |   |
|  Sandbox  |  integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení  |   |   |
|  Bezpečnost  |  automatická aktualizace UTM funkcí poskytovaná výrobcem zařízení  |   |   |
|  Ověřování uživatelů  |  LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, TACACS+, Ověřování na základě certifikátu. Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – Token pro dvoufaktorovou autentizaci  |   |   |
|  Uživatelské profily  |  podpora Identity based policy – nastavení bezpečnosti (bezpečnostního profilu/politiky) uživatelů na základě členství ve skupině na doménovém kontroléru Active Directory.  |   |   |
|  Management a monitoring  |  HTTP/S, SSH, SNMP, syslog,  |   |   |
|  Reporty  |  Integrované logování a reporting, možnost vytváření vlastních reportů  |   |   |
|  Sledování toků  |  export síťových toků (Netflow nebo ekvivalent)  |   |   |
|  SD WAN  |  integrovaná podpora SD WAN - min. rozkládání zátěže a vysoká dostupnost více internetových přípojek a vícecestných VPN (provoz VPN přes více internetových přípojek současně)  |   |   |
|  Standardní funkce  |  NAT, statické a dynamické routování, publikace interních serverů  |   |   |
|  Certifikace  |  doložení certifikace nabízeného řešení obecně uznávanou autoritou. např. ICSA Labs apod.  |   |   |
|  Záruka  |  min. 12 měsíců v režimu 24x7. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a UTM (URL filtrace, IPS, antimalvare, antispam, aplikační kontrola, sandbox)  |   |   |

### Požadavky na architekturu technického řešení

* + - 1. Architektura komodit musí navržena tak, aby vhodně využívala a doplňovala stávající prostředky TC.

### Požadavky na rozhraní

* + - 1. 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 budou provozovány ve virtuálním prostředí VMware vSphere a musí být pro běh v tomto prostředí výrobcem podporovány.
			2. Řešení komodity K2 a K3 bude kompatibilní se stávajícím řešením SIEM na úrovni zasílání/sběru logů a událostí.

### Požadavky na typy klientů

* + - 1. Webová rozhraní všech komodit budou kompatibilní s prohlížeči Microsoft Edge, Firefox a Chrome v aktuálních verzích.

### Požadavky na bezpečnost informací

* + - 1. Veškeré nástroje pro správu hardware musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na Active Directory.
			2. Veškeré nástroje pro správu hardware musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa).
			3. Veškeré nástroje pro správu hardware musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).

## Hodnocené parametry technického řešení

### Požadavky na vlastnosti technického řešení

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

|  |
| --- |
| **Hodnocené parametry**  |
| **Parametr** | **Popis** | **Uchazeč popíše způsob naplnění tohoto hodnoceného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Snížení nároků na správu systémů** |
| 1 | Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti požaduje zadavatel poskytnutí jednotného online nástroje pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů). Nástroj musí disponovat min. následujícími funkcemi: 1) vyhledávání zařízení podle názvu a sériového čísla,  |   |   |
| 2 | Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti požaduje zadavatel poskytnutí jednotného online nástroje pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů). Nástroj musí disponovat min. následujícími funkcemi: 2) možnost stažení aktuálního firmware a uživatelských příruček,  |  |  |
| 3 | Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti požaduje zadavatel poskytnutí jednotného online nástroje pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů). Nástroj musí disponovat min. následujícími funkcemi: 3) ověření záruky a znalostní bázi známých problémů,  |  |  |
| 4 | Pro snížení nároků na správu síťové infrastruktury a zajištění její bezpečnosti požaduje zadavatel poskytnutí jednotného online nástroje pro poskytování technické podpory síťových prvků komodity K2 (tj. Centrálních přepínačů). Nástroj musí disponovat min. následujícími funkcemi: 4) možnost automatického zasílání upozornění na aktualizace firmware k pořízeným zařízením |  |  |
| 5 | Bezpečnostní systém K3-vysoce dostupný cluster firewallů-bude kompatibilní se stávajícím firewallem na úrovní příkazů CLI (Command Line Interface) pro vzájemný přenos konfiguračních nastavení a využití jednotných skriptů pro správu |  |  |

## Implementační služby

### Obecné požadavky

* + - 1. Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. 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. Implementační služby budou minimálně v následujícím rozsahu:
				1. Zajištění projektového vedení realizace předmětu plnění.
				2. Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu.
				3. Dodávku nabízených zařízení a kompletní implementaci řešení splňující povinné parametry technického řešení,
				4. Provedení školení,
				5. Zajištění zkušebního provozu,
				6. Provedení akceptačních testů,
				7. Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.
				8. Předání do plného provozu,
			2. Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.
			3. Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (např. MS Office) používaných zadavatelem.
			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 a organizací, 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: Virtualizační platforma |
| * 1. Návrh a kompletní provedení rozšíření serverové virtualizační platformy TCORP.
	2. Implementace pořízených technologií
	3. Analýza dat a systémů na stávajících serverech škol a jejich migrace na novou platformu
	4. Návrh a provedení rozšíření zálohovacího řešení
	5. Návrh a realizace konfiguračních změn infrastruktury (virtualizační platforma, LAN, SAN)
	6. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti
 |
| K2: Komunikační infrastruktura |
| * 1. Analýza stávajícího síťového prostředí a návrh nové architektury MAN s využitím poskytnutých konfiguračních souborů a dokumentace současného provedení
	2. Optimalizace architektury MAN – bezpečnost, dostupnost, výkon
	3. Revize a optimalizace segmentace – VLAN, adresování, routování
	4. Návrh monitorování MAN
	5. Realizace navrženého a schváleného řešení včetně konfigurací stávajících systémů
	6. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti
 |
| K3: Bezpečnostní systém |
| * 1. Návrh a realizace vhodného začlenění nabízeného firewallu do stávajícího prostředí, zejména způsob náhrady stávajících firewallů – vymezení rolí a pravidel, politik, využití synergií
	2. Návrh a provedení konfigurace firewallu včetně vhodné struktury virtuálních kontextů a konfigurací UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro MMKV a organizace
	3. Optimalizace převzatých konfigurací a politik/pravidel s ohledem na aktuální možnosti nabízeného řešení a rizika kybernetické bezpečnosti
	4. Vybudování VPN pro vzdálený přístup uživatelů na bázi webového portálu
	5. Konfigurace logování pro SIEM – zohlednění nově začleněných organizací
	6. Návrh a provedení konfigurací dotčených a souvisejících systémů
	7. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti.
 |

### Požadavky na zpracování prováděcí dokumentace

* + - 1. Uchazeč před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.
			2. Jako podklad pro zpracování prováděcí dokumentace provede uchazeč předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, minimálně pro následující oblasti:
				1. Stávající stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TC.
				2. MAN – řízení a zabezpečení provozu.
				3. Bezpečnostní systém – zabezpečení internetové komunikace MMKV a jeho organizací, zabezpečení komunikace uvnitř MAN.
				4. Provádění vzdálené správy a související nástroje.
				5. Způsob začlenění nabízených komodit do prostředí TC.
				6. Síťová infrastruktura ve vztahu k plánovanému využití.
				7. SAN infrastruktura ve vztahu k plánovanému využití.
				8. Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
				9. Integrace nabízených systémů.
				10. Dopady implementace na dostupnost a funkčnost stávajících služeb.
				11. Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).
				12. Požadované součinnosti zadavatele a jejich rozsah.
				13. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.
			3. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a musí obsahovat minimálně tyto části:
				1. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,
				2. Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TC (vSphere, LAN, SAN, zálohování, monitorování, SIEM 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.
			4. Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně schválena zadavatelem.
			5. Prováděcí dokumentace bude před ukončením zkušebního provozu aktualizována dle skutečného stavu a následně bude součástí provozní dokumentace.

### Harmonogram realizace

* + - 1. Uchazeč zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.
			2. Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo. Čísla značí počet kalendářních dnů.

|  |  |  |
| --- | --- | --- |
| **Č.** | **Etapa projektu – činnost** | **Ukončení etapy nejpozději:** |
| 1 | Předimplementační analýza a zhotovení Prováděcí dokumentace včetně vypořádání připomínek a akceptace Objednatelem | D+30 |
| 2 | Dodávky a implementace | D+90 |
| 3 | Školení administrátorů | D+120 |
| 4 | Zkušební provoz | D+120 |
| 5 | Akceptační testy | D+120 |
| 6 | Zahájení plného provozu | D+130 |

* + - 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 16 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. Povinným akceptačním kritériem pro akceptaci díla jako celku bude prokázání zajištění požadavků Standardu konektivity dle manuálu uveřejněného na <http://www.irop.mmr.cz/cs/Ostatni/Web/Novinky/Zverejneni-doporucujiciho-manualu-k-postupum-pri-p> včetně úspěšného provedení a doložení testu <https://www.standardkonektivity.cz/> na dvou zadavatelem vybraných lokalitách, ze seznamu lokalit se závazkem dodržení standardu konektivity. Prokázání naplnění požadavků Standardu konektivity poskytne dodavatel v písemné formě vhodné jako příloha k akceptačnímu protokolu. **Uchazeč již v nabídce předloží čestné prohlášení potvrzující, že výše uvedené požadavky jím navržené technické řešení splňuje.**
			5. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
			6. Uchazeč zajistí zkušební provoz v délce minimálně 10 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
			7. 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 10-ti pracovních dnů nebo poskytnutí náhradního prvku shodných nebo lepších parametrů po dobu opravy.
			3. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
			4. Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
			5. Zadavatel dále požaduje poskytnutí prodloužené záruky na všechna dodaná zařízení s výjimkou operačních systémů a optických prvků min. na 60 měsíců, a to v kvalitě a parametrech shodných se základní požadovanou zárukou. Cenu zahrne uchazeč v Části 5 Zadávací dokumentace (Kalkulace nabídkové ceny) do položky Rozšířená záruka HW.
			6. Součástí technické podpory bude spolupráce s administrátory zadavatele při řešení nekompatibilit aplikací a systémů.
			7. 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.
			8. Uchazeč ve své nabídce výslovně uvede všechny podmínky záruk.

## Požadavky na zabezpečení provozu

Zadavatel požaduje detailní návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění 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. **Běžná pracovní doba** – čas mezi 8:00 a 17:00 v Pracovní dny.
			6. **Člověkohodina** - práce Pracovníka uchazeče v rozsahu jedné (1) hodiny v rámci Pracovního dne.
			7. **Člověkoden** - práce Pracovníka uchazeče v rozsahu jednoho (1) Pracovního dne.
			8. **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 Uchazeče směřující k odstranění incidentu, zodpovězení Dotazu nebo přípravy Nového požadavku.
			9. **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
			10. **HelpDesk** – nepřetržitě dostupný automatizovaný systém pro vzdálené zadávání a správu požadavků,
			11. **Hot-line** –pracoviště uchazeče přijímající Požadavky od zadavatele na definovaných telefonních číslech nebo elektronických komunikačních kanálech.
			12. **Incident**- událost způsobující odchylku od očekávané funkce Prvku IT, která způsobuje nebo může způsobit přerušení anebo snížení kvality této funkce.
			13. **Priorita incidentu** - závažnost incidentu dle klasifikace Kontaktní osoby zadavatele.
			14. **Koncová zařízení** - počítače uživatelů, jejich programové vybavení a periferní zařízení k počítačům připojená (např. tiskárny, skenery).
			15. **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.
			16. **Proaktivní monitorování**-monitorování prováděné dle charakteru provozu a činnosti Prvku IT v režimu 24x7 (komunikační infrastruktura) nebo v režimu 9x5 (technologické centrum).
			17. **Náhradní zařízení** – zařízení podobných vlastností (parametrů).
			18. **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 díla
			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 je 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 bezpečnostních systémů,
				4. monitoring prvků IT třetích stran, které mohou ovlivňovat chod Systému, pokud jsou tyto Prvky IT součástí Dodávky 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.

### Specifikace rozsahu požadované podpory provozu

* + - 1. Instalace a zprovoznění maintenance (nových verzí firmware, obslužného software a bezpečnostních či funkčních aktualizací, na které má zadavatel nárok v rámci platných záruk) pro veškerý dodaný hardware – min. 1x ročně nebo bezodkladně v případě kritických bezpečnostních aktualizací, změn legislativy či změn navázaných systémů.
			2. Uchazeč v rámci zabezpečení provozu poskytne alespoň následující služby (kalkulaci za tyto služby zahrne do nabídkové ceny do položky „Zabezpečení podpory provozu“:
				1. Pravidelné servisní prohlídky a revize předepsané výrobci.
				2. Průběžné monitorování prvků IT pokrývaných touto smlouvou dalších, popř. prvků IT, které mohou ovlivnit jejich chod. Počet sledovaných parametrů nesmí být prakticky omezen (min. stovky), administrátoři MMKV musí mít přístup ke sledovaným parametrům alespoň v režimu čtení.
				3. Řešení incidentů – dle podmínek SLA, min 4 hod. v rámci měsíčního paušálu
				4. Řešení Požadavků – min. 2 hodiny v rámci měsíčního paušálu.
				5. Profylaxe – minimálně každých 6 měsíců.
				6. Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
				7. Hotline podpora a Odborná podpora – vzdálené konzultace pro podporované služby/produkty. Celkový rozsah služeb Hotline a Odborné podpory v rámci měsíčního paušálu je min. 2 hodiny. Minimální dostupnost Hotline a Odborné podpory v režimu 9x5.
			3. Seznam prvků pokrývaných službou zabezpečení provozu je uveden v 7.5.

### 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, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti a dostupnosti TCORP a prevenci incidentů.
			2. Souhrn informací o poskytovaných službách (report) bude obsahovat informace o jednotlivých službách a jejich provádění (dle povahy jednotlivých služeb a definice dle katalogových listů služeb).
			3. Měsíční report bude vyhotovován výhradně v elektronické formě a bude obsahovat souhrn činností provedených za vykazované období.
			4. Report bude za příslušné období vždy obsahovat minimálně:
	1. Informace o provedených změnách v TC spojených s poskytováním služby.
	2. 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.

### Seznam prvků IT

Následující tabulka obsahuje seznam prvků IT, u niž je požadováno Zabezpečení provozu

|  |
| --- |
| **Prvky IT** |
| **Prvek** | **Popis** | **Počet** |
| **Hardware** |
| 1 | Server Blade | 1 |
| 2 | Centrální přepínač | 2 |
| 3 | Firewally | 2 |

### 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. 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.
1. Viz <http://www.irop.mmr.cz/cs/Vyzvy/Seznam/Vyzva-c-47-Infrastruktura-zakladnich-skol-SVL> - Přílohy\_Specifická pravidla pro žadatele a příjemce\_výzva č. 47\_7.2.2017.zip – dokument P9\_Standard konektivity škol \_ZŠ\_- 47. výzva\_ v.1.5.docx [↑](#footnote-ref-1)