|  |
| --- |
| Příloha č. 3d Dodávka a implementace komunikační infrastruktury - Technická specifikace |

# Vymezení předmětu plnění veřejné zakázky

## Předmět plnění veřejné zakázky

Předmětem veřejné zakázky je dodávka optické infrastruktury popř. prodej ideálního spoluvlastnického podílu spojeného s výlučným užíváním konkrétního páru optických vláken a dodávka aktivních a pasivních prvků s ní spojených pro vytvoření metropolitní datové sítě města Karlovy Vary. Součástí zakázky jsou služby dohledu nad kompletní sítí a služby konfigurace a reportingu veškerých dodaných aktivních prvků po dobu 60 měsíců od ukončení (předání) projektu, instalace, konfigurace, vytvoření požadované dokumentace a zajištění certifikovaného školení na dodané aktivní prvky.

V rámci dodávky optické infrastruktury bude každá lokalita napojena do metropolitní datové sítě minimálně 1 párem nenasvícených („dark-fiber“) optických vláken kategorie G.657A nebo G.652.D, které umožní plné využití ve všech 18 vlnových délkách specifikovaných v doporučení ITU-T G.694.2. To umožňuje budoucí nasazení optických technologií pro dělení vlnových délek. Optická vlákna musí být uložena vhodným způsobem v zemi (např. v HDPE trubkách, mikrotrubičkách apod.). Součástí dodávky optických vláken nebo ideálního spoluvlastnického podílu spojeného s výlučným užíváním konkrétního páru optických vláken, je vedle nenasvícených vláken také jejich příprava ve formě zemních spojek, odboček z tras včetně vyvázání a svaření do patchpanelů a další dodávky a služby potřebné pro realizaci metropolitní datové sítě. V maximálně 10% z celkového počtu lokalit je možné nahradit optickou infrastrukturu pro připojení koncové lokality bezdrátovým RadioReleovým spojem.

V rámci projektu bude propojeno 35 lokalit, projekt bude rozdělen do dvou fází, které budou následovat po sobě, nejprve Fáze I. a poté Fáze II.

Přehled lokalit připojených v rámci realizace Fáze I.

Centrální lokalita:

* + Magistrát města, Moskevská 1281/21, Karlovy Vary

Lokality metropolitní sítě:

* + Magistrát města Karlovy Vary, U Spořitelny 2
  + Městská policie Karlovy Vary, Moskevská 34
  + Správa přírodních léčivých zdrojů a kolonád, Lázeňská 18/2
  + ZŠ Karlovy Vary, Truhlářská 681/19
  + ZŠ J.A.Komenského, Kollárova 533/19
  + ZŠ pro žáky se specifickými poruchami učení, Mozartova 7
  + ZŠ Karlovy Vary, 1. Máje 1
  + Mateřská škola Komenského, Komenského 7
  + Mateřská škola "Notička", E. Destinové 1
  + Mateřská škola "Na KOPEČKU", Mozartova 4
  + Mateřská škola "Sluníčko", Východní 6
  + Mateřská škola, Javorová 211

Tyto lokality budou osazeny aktivními prvky a budou na nich poskytovány služby servisu optických vláken, instalace, konfigurace, monitoringu, reportingu a servisu aktivních prvků. Rovněž bude instalován a zprovozněn zákaznický dohledový systém a systém pro monitoring provozního prostředí. Fáze 1 bude zrealizována nejpozději do 6 měsíců od podpisu smlouvy.

Přehled lokalit připojených v rámci realizace Fáze II.:

Lokality metropolitní sítě:

* + Správa lázeňských parků, U Solivárny 2
  + Lázeňské lesy Karlovy Vary, Na Vyhlídce 35
  + Husovo náměstí 2
  + Městská policie Karlovy Vary, Školní 9
  + Základní škola jazyků, Libušina 1032/31
  + ZŠ Karlovy Vary, Krušnohorská 735/11
  + ZŠ Karlovy Vary, Konečná 917/25
  + ZŠ a ZUŠ Rybáře, Šmeralova 15
  + ZŠ Dukelských hrdinů, Moskevská 1117/25
  + ZŠ Karlovy Vary, Poštovní 1743/19
  + ZŠ Karlovy Vary (odloučené pracoviště), Modenská 15
  + Mateřská škola U brodu, U Brodu 73
  + Mateřská škola "Studánka", Krymská 10
  + Mateřská škola "Zdravá mateřská školka", Krymská 12
  + Mateřská škola Hornická, Hornická 66
  + Mateřská škola, Krušnohorská 16
  + Mateřská škola, Sedlecká 5
  + Mateřská škola, Fibichova 5
  + Mateřská škola, Truhlářská 11
  + Mateřská škola, Mládežnická 6
  + Mateřská škola, kpt. Jaroše 6
  + Mateřská škola, Vilová 1

Lokality budou osazeny aktivními prvky a budou na nich poskytovány služby servisu optických vláken, instalace, konfigurace, monitoringu, reportingu a servisu aktivních prvků. Fáze 2 bude zrealizována nejpozději do 12 měsíců od podpisu smlouvy.

Součástí zakázky je vybudování a zprovoznění metropolitní sítě a další správa aktivních prvků sítě po dobu 60 měsíců od ukončení (předání) projektu.

Na pasivní optickou infrastrukturu je požadována záruka 20 let od ukončení (předání) projektu.

## Popis stávajícího stavu

* + - 1. Centrální lokalita je hlavní budova Magistrátu města Karlovy Vary, adresa Moskevská 1281. Centrální lokalita je napojena optickým spojem do další budovy MMKV na adrese U Spořitelny 2.
      2. Optický spoj je realizovany SM 24 vláknovým optickým kabelem, ve vaně je zapojeno všech 24 vláken, v současné době jsou využity 3 páry tzn. 3x 1Gb FD, redundantně přes STP. Ve špičkách je traffic max 20Mb per spoj, dohled je zajištěný přes SNMP.

## Popis cílového stavu a specifikace předmětu plnění

* + - 1. Dodávka metropolitní sítě bude realizována dodávkou minimálně jednoho páru optických vláken v každé lokalitě resp. prodejem ideálního spoluvlastnického podílu spojeného s výlučným užíváním konkrétního páru optických vláken do vlastnictví města Karlovy Vary a jejich zasíťování prostřednictvím dodaných aktivních prvků.
      2. V maximálně 10% z celkového počtu lokalit je možné nahradit optickou infrastrukturu pro připojení koncové lokality bezdrátovým RadioReleovým spojem.
      3. Pro připojení lokality Magistrát města Karlovy Vary, U Spořitelny 2 k centrální lokalitě Magistrát města, Moskevská 1281/21, Karlovy Vary je možné využít 1 pár vláken stávajícího optického kabelu ve vlastnictví magistrátu města Karlových Varů. Tuto infrastrukturu je magistrát Karlových Varů připraven poskytnout bezplatně po celou dobu trvání projektu metropolitní sítě. Nad poskytnutou infrastrukturou je nutné provozovat poptávané služby (dodávka HW, SLA, instalace, dohled, servis) v plném rozsahu dle této zadávací dokumentace.
      4. Pro předmět plnění bude zabezpečena podpora provozu po dobu 60 měsíců od přechodu poslední lokality do plného provozu.
      5. Centrální lokalita Zadavatel požaduje řešení centra sítě formou modulární chassis. Pro řešení centrálního uzlu optické sítě je požadován aktivní prvek modulární koncepce s architekturou vylučující „single point of failure“. Tato architektura musí současně podporovat distribuované přepínání i směrování provozu na jednotlivých linkových kartách, tj. tzv. distribuovaný forwarding na L2 i L3 RM OSI. Modulární switch musí umožňovat redundantní osazení řídících / switching modulů i redundanci zdrojů. Současně je požadována podpora možnosti rozšíření o další modulární chassis připojitelné do jednoho logického / virtuálního celku. Z pohledu L2 i L3 protokolů je nutné, aby případný logický celek vystupoval jako uzel jediný. Případné logické spojení více chassis do jednoho virtuálního nesmí protokolově omezovat funkcionalitu chassis samotného. Kromě standardních L2 a L3 protokolů je v centrální lokalitě pro případné budoucí využití stanoven požadavek podpory MPLS, MPLS VPN a VPLS. Tato podpora je požadována již pro dodávaný HW centrální lokality.
      6. Koncové lokality slouží výhradně pro připojení jednotlivých koncových uzlů sítě. Tyto uzly budou připojeny spoji s minimální rychlostí 1GBit/s do centrální lokality. Architektura metropolitní sítě a zařízení musí umožnovat využítí více GE portů v linkové agregaci i 10GE propojení pro jakoukoliv lokalitu Výjimku tvoří RadioReleové spoje, kde je požadována minimální rychlost 100 Mbit/s. Požadována je podpora konceptu virtualizace více samostatných (standalone) prvků do jednoho logického celku. Pro L2 i L3 protokoly je požadováno, aby se případný logický celek více prvků choval jako jediný uzel sítě. Není požadováno modulární řešení chassis ani modulární zdroje. K dispozici však musí být jak metalické tak optické varianty switchů pro nabídnutou modelovou řadu. Pro případné budoucí rozšíření musí prvky disponovat možností rozšíření o 10GE porty v minimálním počtu 4. Uchazeč musí při návrhu architektury metropolitní sítě počítat s jejím budoucím rozšiřováním.
      7. Koncové lokality budou propojeny minimálně 1 párem single mode nenasvícených vláken („dark-fiber“) kategorie G.657A nebo G.652.D. Optické kabely budou uloženy v zemi v HDPE trubkách, s ohledem na bezpečnost optických tras.
      8. Topologie sítě fyzická topologie sítě musí být buď typu full-mesh anebo spojitá jedno nebo víceúrovňová hvězda z pohledu centrální lokality.
      9. Optická infrastruktura řešení aktivních prvků i pasivní optické infrastruktury musí umožnovat implementaci technologie CWDM nebo DWDM. Jedná se především o požadavek podpory „barevných“ optických transceiverů všemi nabízenými aktivními prvky a možnosti pasivní infrastruktury rozšířit přenášené kapacity využitím dalších vlnových délek.
      10. RadioReleové spoje (RR spoje) musí výhradně využívat licenčních pásem ČTU. Minimální požadovaná rychlost na těchto bezdrátových spojích je 100 Mbit/s.
      11. Řešení VPN a firewallu v rámci řešení centrálního bodu sítě je požadována implementace řešení terminace VPN (IPSec, VPN, SSL VPN) připojení a dodávka firewallu. Firewall zde bude plnit roli zabezpečovacího prvku s implementovanými bezpečnostními pravidly dle požadavku Zadavatele specifikovanými v průběhu tvorby prováděcí dokumentace jak pro směr dále do veřejné sítě, tak pro inspekci provozu mezi jednotlivými vnitřními sítěmi. Toto řešení musí umožňovat rozšíření o IPS funkcionalitu.
      12. Součástí řešení je dodávka HW a SW (včetně operačního systému a databáze), kterým se zabezpečuje: monitoring všech aktivních prků v síti. Monitoring musí poskytnout detailní informace o stavu jednotlivých zařízení, musí umožňovat integraci dalších prvků třetích stran, statistiku provozu každého z dohlížených prvků a provozní parametry ve formě grafických sestav, které lze z dohledovacího SW exportovat. Tento systém musí nutně podporovat i monitoring prvků třetích stran díky předpokládanému monitoringu dalších komponent nad rámec této dokumentace zejména po ukončení doby udržitelnosti projektu. Tento systém bude součástí Fáze I.
      13. Součástí řešení je dodávka HW a SW (včetně operačního systému a databáze), kterým se budou ověřovat identity uživatelů v síti. Tento nástroj bude rovněž zprostředkovávat ověřování identity vzdálených uživatelů, kteří budou do síti přistupovat přes VPN. Konkrétní autentizační schémata budou dodána ve fázi přípravy prováděcí dokumentace Zadavatelem. Tento systém bude součástí Fáze I.
      14. Systém pro monitoring prostředí a zabezpečení - Pro zabezpečení provozních podmínek instalovaných aktivních prvků na jednotlivých lokalitách s výjimkou centrální lokality je požadována dodávka systému, který umožní sledovat provozní podmínky (teplota, vlhkost,). Při překročení definovaných provozních rozsahů nebo změně „bezpečných“ stavů budou automaticky informováni zodpovědní pracovníci. Systém bude v databázi uchovávat veškeré sledované provozní hodnoty, stavy. Záznamy v databázi budou obsahovat pravidelná měření a kontroly stavů a veškeré alarmové stavy (překročení bezpečných rozsahů, nebezpečné stavy) včetně časové identifikace. Systém monitoringu prostředí bude implementován do dohledového systému aktivních prvků na úrovni zobrazení provozních podmínek a alarmingu/notifikací o kritických událostech. Tento systém bude součástí Fáze I.
      15. Zadavatel požaduje implementaci systému monitoringu prostředí do dohledového systému aktivních prvků na úrovni zobrazení provozních podmínek a alarmingu/notifikací o kritických událostech.
      16. Zadavatel požaduje v centrální lokalitě instalaci rozvaděče, který bude vybaven modulární střechou a podlahou, podporující individuální konfiguraci krytů a kabelových průchodek. Kabelové prostupy ve střeše a podlaze rozvaděče musí přímo navazovat na vertikální vyvazovací management a podporovat přímé vedení kabeláže do přední či zadní roviny aktivních prvků instalovaných v rozvaděči. Tyto trasy musí být bez jakýchkoliv překážek či ostrých hran, všechny kabelové průchodky budou vybaveny krytím IP54. Tato část bude součástí Fáze I.

### Minimální požadavky na aktivní prvky

V rámci realizace předmětu plnění zajistí dodávku následujících aktivních prvků minimálně s následujícími parametry:

|  |  |
| --- | --- |
| **1. Aktivní prvky v centrální lokalitě** | |
| a. Chassis koncepce hardwaru  b. Podpora spojení více HW chassis do jednoho virtuálního; pro fyzické propojení těchto chassis nutno použít pouze standardizovaných rozhraní  c. Podpora L2 i L3 protokolů nad virtual chassis, tj. pro L2 i L3 protokoly je virtual chassis jedním uzlem  d. Jednotný operační systém aktivních prvků centrálních lokalit a přístupových bodů (nebude akceptováno řešení s více druhy OS těchto komponent)  e. Operační systém musí umožňovat restart jednotlivých služeb (procesů), neakceptuje se reboot celého prvku pro restart jednotlivé služby  f. Funkcionalita nesmí být omezena licencemi (Operační systém nesmí být licencován po jednotlivých funkcionalitách nebo musí být v neomezené licenční verzi)  g. Switchovací výkon minimálně 380 Gbit/s  h. Forwarding rate minimálně 450 Mpps  i. Osazení chassis redundantním napájením  j. Osazení chassis redundantními řídícími kartami  k. Možnost osazení chassis Modul/moduly VPN/FW/SSL/IPS  l. Min. 8 portů 1000Base-T, lze i jako osazené SFP šachty. Podpora v chassis 1000 Base-T portů až 280 (jedná se o požadavek na podporu v chassis celkově, chassis bude zatím osazeno min. 8 porty).  m. Min. 36 portů 1000Base-X. Podpora až 280 portů 1000Base-X per chassis.  Pozn. Požadavek na 280 portů 1000Base-T a 280 portů 1000Base-X není stanoven jako současně, tj. dostačující je celkový počet min. 280 gigabitových portů.  n. Podpora chassis až pro 24 neblokujících 10G-Base-X (jedná se o požadavek na podporu v chassis celkově, chassis bude zatím osazeno min. 4 porty)  o. Podpora standardizovaných optických rozhraní (SFP, XFP, Xenpak, SFP+), zařízení musí být osazeno pouze standardními rozhraními s možností snadné rozšiřitelnosti optické sítě v budoucnu  p. Optická rozhraní pro optické moduly musí podporovat vložné moduly výrobců třetích stran (tj. podpora SFP, SFP+, XFP apod.)  q. Plně distribuovaná architektura L2/L3 (v rámci chassis i v rámci virtual chassis)  r. Variantně musí platforma podporovat MPLS a MPLS L2 i L3 VPN. Tato funkcionalita musí být k dispozici již na dodávaném HW, tj. pro spuštění MPLS / MPLS VPN služeb nebude nutné měnit HW komponenty.  s. Všechny LPU karty musí být Hot-Swap  t. Příkon maximálně 1500W na jeden zdroj | |
| **2. Moduly VPN a FW** | |
| Moduly pro VPN a FW jsou součástí plnění, technologie centrální lokality však musí nabízet i možnost rozšíření i o IPS modul do budoucna  SSL VPN   1. Vyžadována dodávka servisního modulu (příp. více modulů) s podporou VPN i SSL VPN 2. Propustnost VPN modulu minimálně 750 Mbps 3. Podpora IPSec VPN tunelů a L2TP tunelu, minimálně 3000 tunelů 4. SSL VPN modul musí disponovat minimálně 256 licencemi 5. Podpora modulu až pro 3000 SSL uživatelů   FW/VPN   1. Vyžadována dodávka servisního modulu s podporou Firewall 2. Servisní modul Firewall musí podporovat virtuální firewally a plný rozsah VLAN (tj. 4094). 3. Propustnost modulu Firewall minimálně 5 Gbps   IPS  a. Vyžadována podpora servisního modulu s IPS funkcemi (požadováno v rámci nabízených boxu/chassis nikoli jako standalone řešení) | |
| **3. Aktivní prvky v ostatních lokalitách** | |
| a. Switchovací výkon minimálně 128 Gbit/s  b. Forwarding rate minimálně 85 Mpps  c. Podpora spojení více HW chassis / boxů do jednoho virtuálního; pro fyzické propojení těchto chassis nutno použít pouze standardizovaných rozhraní  d. Požadována podpora min. 5 boxů do jednoho virtual chassis  e. Podpora L2 i L3 protokolů nad virtual chassis, tj. pro L2 i L3 protokoly je virtual chassis jedním uzlem  f. Jednotný operační systém aktivních prvků centrálních lokalit i agregačních a přístupových bodů (nebude akceptováno řešení s více druhy OS těchto komponent)  g. Operační systém musí umožňovat restart jednotlivých služeb (procesů), neakceptuje se reboot celého prvku pro restart jednotlivé služby  h. Aktivní prvky obsahují plnou funkcionalitu operačního systému, která není omezena licencemi za jednotlivé funkce nebo je v neomezené licenční verzi.Počet 10G-BaseX portů na jedno zařízení min. 4 (built in nebo jako modulární rozšíření; není součástí této poptávky)  i. Min. 24 portů 10/100/1000Base-T  j. Podpora standardizovaných optických rozhraní (SFP, XFP, Xenpak, SFP+), neakceptují se proprietální optická rozhraní  k. Optická rozhraní pro optické moduly, musí podporovat vložné moduly výrobců třetích stran (tj. podpora SFP, SFP+, XFP apod.)  l. Plně distribuovaná architektura L2/L3 (v rámci chassis i v rámci virtual chassis)  m. Příkon max 150W na jeden zdroj |
| **4. Autentizační server** |
| 1. Nutná podpora řešení Autentizačního serveru na platformě Microsoft Windows nebo Linux 2. Uchazeč zajistí podporu autentifikačních schémat na dodávaných HW prvcích (tj. primární a sekundární Autentizační server) 3. Autentizační server musí podporovat min. databázi min. 1000 uživatelů 4. Řešení Autentizačního serveru musí podporovat práci s vendor specific options |
| **5. Dohledový systém** |
| 1. Podpora platforem Windows nebo Linux pro dohledový systém 2. Klient – server koncept, klient nesmí vyžadovat instalaci speciálních klientských SW (tj. dostupnost klienta pro http protokol) 3. Grafické zobrazení mapy sítě 4. Automatické skenování sítě 5. Automatické (plánované) zálohy konfigurací síťových prvků 6. Možnost přidat zařízení třetích stran, Možnost importu MIB zařízení třetích stran 7. Možnost rozšíření o moduly typu: wireless, QoS, VPN 8. Monitoring zařízení a spojení a notifikací 9. Možnost přidání vlastních map a zařízení 10. Podporu SNMP, ICMP, DNS a TCP monitoringu 11. Monitoring a grafické zobrazení využití linek 12. Přímý přístup ke vzdálenému managementu zařízení z jedné konzole 13. Možnost propojení (plugin) s nástrojem na virtualizaci 14. Podpora komerčních i volně šiřitelných databázových systémů 15. Podpora managementu incidentu 16. Možnost rozdělení zátěže mezi více serverů (master/slaves) |

### Minimální požadavky na rozvaděč a systém pro monitoring prostředí a zabezpečení

|  |
| --- |
| **1. Rozvaděč v centrální lokalitě** |
| Komunikační rozvaděč musí splňovat tyto základní parametry:   1. Výška 42U, šířka 800mm, hloubka 1000mm 2. Rozvaděč a všechny jeho odmontovatelné části musí být vybaveny těsnící páskou, tak aby rozvaděč získal krytí IP54 3. Statická nosnost rozvaděče minimálně 500 kg 4. Možnost spojování rozvaděčů do řady bez nutnosti demontáže bočních panelů 5. Přední a zadní dveře vybavené bezpečnostním sklem EN 12150-1. Elektronický zámek na dveřích musí umožnit vícebodové uzavření dveří a umožní instalaci vložek dle konkrétních specifikací zadavatele. 6. 19“ lišty umožní instalaci všech kompatibilních IT zařízení 7. Rozvaděč umožní instalaci 19“ napájecích PDU, tak aby nezabíraly 19“ rovinu určenou pro servery a jiná zařízení 8. Rozvaděč umožní instalaci horizontálních a vertikálních vysokokapacitních vyvazovacích panelů   Rozvaděč bude kompatibilní s:   1. systémy pro management vysokorychlostní strukturované kabeláže, zejména metalické kabeláže cat. 6 a vyšší a optické rozvody OM3 a OS1. Kompatibilita jak s horizontálními, tak i vertikálními systémy, které umožní zároveň předo-zadní vedení propojovacích kabelů a také umožní oddělení studené a horké uličky. Systém musí být uživatelsky přívětivý a umožní pohodlnou manipulaci s patch cordy, včetně jejich svazkování. 2. Prvky pro zajištění kompletního oddělení studeného a horkého vzduchu (separační rámy o hloubce 15cm od čela rozvaděče a beznástrojové záslepky, umožňující rychlou a pohodlnou demontáž a montáž těchto prvků zpět do rozvaděče. Tyto prvky jsou nutné pro správné a efektivní fungování datového centra a instalovaných serverových zařízení. |
| **2. Monitoring prostředí na ostatních lokalitách** |
| Monitoring prostředí na lokalitách:   1. - Řídící jednotka se síťovým rozhraním pro Ethernet 10/100 Mbps 2. - podpora protokolů a technologií WEB/SNMP/SMTP/XML 3. - podpora dvou 1-Wire čidel (teplota/vlhkost) 4. - plná vzdálená správa po IP 5. - rozsah provozních podmínek: Teplota -10..60 °C   Požadovaná čidla:  Teplota (do rozvaděče)   1. - 1-Wire sběrnice 2. - Rozsah měřené teploty -10°C až +80°C, Přesnost měření +/- 0,5 °C   Vlhkost   1. - Vstupní rozsah vlhkosti: 20 % - 90 % RH (relativní vlhkost) 2. - nasákavý detekční kabel délky 10m 3. - detekce zaplavení nebo průsaku vody po celé délce detekčního kabelu 4. - po zaplavení a následném vyschnutí musí být kabel opět připraven k detekci 5. - možnost rozšíření délky detekčního kabelu až na 85m 6. - provozní teplota: -10°C až 65°C 7. - 1Wire RJ11 |

### Implementační služby

* + - 1. V rámci realizace předmětu plnění uchazeč realizuje alespoň následující služby:
         1. Provedení předimplementační analýzy
         2. Provedení detailního návrhu cílového stavu
         3. Dodávka a implementace předmětu plnění včetně technické podpory. Předpokládají se minimálně následující činnosti:
    1. HW příprava
       1. Uchazeč kompletně sestaví HW z jednotlivých komponent a provede jeho úvodní inicializaci – zahoření.
    2. Aktualizace
       1. Uchazeč provede kompletní aktualizace SW dodaných HW i SW řešení. Uchazeč současně provede unifikaci SW na jednotlivých řadách-platformách. Takto použité SW a konfigurace budou součástí předávací dokumentace, resp. její elektronické verze.
    3. Inicializace systému (HW příprava a aktualizace) a základní konfigurace
       1. Po inicializaci HW i SW (HW příprava a aktualizace) provede Uchazeč základní nastavení HW i SW do základního funkčního stavu. Tento stav je definován jako zakomponování HW i SW řešení do dohledového systému a základní nastavení služeb HW i SW řešení.
    4. Optimalizace
       1. Uchazeč je povinen poskytnout minimální nutnou podporu pro optimalizaci, tj. vzájemné sladění funkčnosti stávajících systémů a nově dodaného řešení. Fáze optimalizace je chápána jako podpora v přípravné fázi a fázi testování z pohledu časového průběhu projektu.
       2. Podpora ve fázi provozní je definována samostatně.
    5. Projektová dokumentace
       1. Uchazeč povede v průběhu přípravné i testovací fáze projektovou dokumentaci. Po ukončení testovací fáze bude tato projektová dokumentace finalizovaná a jako předávací dokumentace bude součástí akceptace celého systému.
       2. V elektronické podobě bude součástí projektové dokumentace i veškerý použitý SW a licence.
       3. Projektová dokumentace bude udržovaná v aktuálním stavu po dobu 60 měsíců od akceptace celého systému.
    6. Bezpečnostní dokumentace
       1. Uchazeč povede v průběhu přípravné i testovací fáze bezpečnostní dokumentaci sítě. Bude se jednat o dokument popisující stávající i navržená bezpečnostní pravidla z pohledu fyzické i síťové bezpečnosti ve vztahu k použitým prvkům a dodaným technologiím. Po ukončení testovací fáze bude tato bezpečnostní dokumentace finalizovaná a bude součástí akceptace celého systému.
          - Základní požadovaný obsah bezpečnostní dokumentace

Směrnice pro řešení incidentů

Bezpečnostní směrnice IT s popisem implementovaných a provozovaných bezpečnostních mechanismů a zásadami pro bezpečný provoz sítě

Havarijní plány

Návaznost na již existující bezpečnostní směrnice zadavatele jak z pohledu IT infrastruktury tak i fyzické bezpečnosti

* + - 1. V elektronické podobě bude součástí bezpečnostní dokumentace i veškerý použitý HW a SW.
      2. Bezpečnostní dokumentace bude udržovaná v aktuálním stavu po dobu 60 měsíců od akceptace celého systému.
    1. Předávací dokumentace
       1. Uchazeč připraví v elektronické podobě kompletní předávací dokumentaci monitorující stav k začátku provozní fáze.
          - Požadované součásti předávací dokumentace

Detailní schéma připojované sítě včetně adresního plánu

Použitý SW a licence

Dokumentace k použitému HW

Konfigurace jednotlivých prvků

Bezpečnostní dokumentace

* + 1. Akceptace
       1. Uchazeč je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
          1. Zajištění projektového vedení realizace předmětu plnění
          2. Zajištění konfigurace všech dodaných aktivních prvků a zprovoznění metropolitní sítě města Karlovy Vary. Konfigurace bude zahrnovat minimálně tyto celky:

1. Sestavení HW, jeho aktualizace, aktivace a základní zahoření všech komponent
2. Montáž kompletního HW a jeho fyzické propojení na infrastrukturu, včetně ověření propustnosti mezi jednotlivými body sítě
3. Základní nastavení všech aktivních prvků ve smyslu managementu
4. Instalace, aktualizace a zahoření systému managementu sítě
5. Nastavení jednotlivých segmentů sítě, nastavení routingu a základních politik mezi jednotlivými segmenty sítě
6. Propojení do dalších definovaných celků (konektivita, další MAN a VPN sítě)
7. Základní nastavení zabezpečení sítě, vzdáleného připojení, příp. VPN
8. Kompletní archivace a uložení konfigurací, softwaru a dokumentace provedení
   * + - 1. Zpracování prováděcí dokumentace
         2. Zpracování technologické dokumentace včetně parametrů a konfigurací
         3. Zpracování provozní dokumentace
         4. Zpracování materiálů pro školení minimálně pro kategorie: uživatelé, administrátoři
         5. Provedení školení v definovaném rozsahu
         6. Provedení akceptačních testů
         7. Zajištění zkušebního provozu v délce minimálně 4 týdnů včetně technické podpory minimálně 2 specialistů na dané zařízení/službu s dostupností maximálně 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h a s průběžným vyhodnocováním minimálně 1x týdně
         8. Předání do plného provozu
         9. Zajištění ostatních služeb potřebných pro realizaci projektu
       1. Uchazeč dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.
       2. Zadavatel požaduje před zahájením implementačních prací zpracování prováděcí dokumentace, která bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění do stávajícího prostředí technologického centra. Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
          1. Komplexní analýzu stávajícího prostředí
          2. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému
          3. Způsob zajištění potřebných dodávek včetně technické podpory
          4. Způsob zajištění projektového řízení na straně uchazeče pro realizaci předmětu plnění
          5. Detailní návrh a popis postupu implementace předmětu plnění
          6. Detailní popis zajištění bezpečnosti informací
          7. Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně tyto aktivity s uvedením konkrétních termínů, uchazeč vhodným způsobem rozšíří kritické milníky o další aktivity, které mohou být pro projekt klíčové. Jedná se o tyto aktivity:

Zahájení projektu

Provedení předimplementační analýzy

Předání prováděcí dokumentace

Zahájení realizace předmětu plnění

Školení

Zahájení zkušebního provozu

Akceptační testy

Zahájení plného provozu.

* + - * 1. Návrh akceptačních kritérií a akceptačních testů
        2. Detailní popis navrhovaných školení
        3. Detailní popis údržby systémů
        4. Obsah provozní dokumentace (technická, uživatelská, administrátorská)
      1. Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standartních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem na datovém nosiči a 1x kopii v papírové formě.
      2. Součástí prováděcí dokumentace bude čestné prohlášení uchazeče, že má vyřešeny nebo v řešení majetkoprávní vztahy k pozemkům, přes které povedou optická vlákna.
      3. Zadavatel požaduje v rámci plnění Fáze I. zpracování studie rozvoje komunikační infrastruktury MMKV, která bude sloužit jako základní dokument pro další rozvoj. Dokument bude obsahovat části týkající se celkové koncepce sítě, cílů návrhu, katalog služeb poskytovaných síťovou infrastrukturou, popis páteřní infrastruktury s uvedením základních charakteristik, infrastrukturu sítě, obecné požadavky na aktivní prvky, koncepci bezpečnosti komunikační infrastruktury, popis realizace tj. fáze, připojování subjektů, přístupová místa a také popis zajištění provozu včetně uvedení požadavků na zajištění, varianty a aplikační zajištění chodu sítě. Studie rozvoje komunikační infrastruktury bude obsahovat v detailu dostatečném pro další rozvoj a provoz komunikační infrastruktury MMKV alespoň následující body:
         1. KONCEPCE
         2. CÍLE NÁVRHU

Varianty řešení

Rizika realizace koncepce

* + - * 1. KATALOG SLUŽEB POSKYTOVANÝCH SÍŤOVOU INFRASTRUKTUROU

Vztah sítě k externímu prostředí

Služby poskytované sítí

Služby, ke kterým síť zprostředkovává přístup

Stručná charakteristika služeb

Služby třetím stranám

IP telefonie, hlasové a multimediální služby

Internet

Směrovací oblast pro Internet

Poskytování připojení do Internetu externím organizacím

Logické postavení síťového perimetru

VPN

Technologické centrum

Požadavky na zavedení nových služeb

* + - * 1. PÁTEŘNÍ INFRASTRUKTURA
        2. ZÁKLADNÍ TECHNOLOGIE

Kvalita služby - QoS

* + - * 1. ZÁKLADNÍ CHARAKTERISTIKY SÍTĚ
        2. INFRASTRUKTURA SÍTĚ

Fyzická infrastruktura

Páteř sítě

Hraniční směrovače

CE směrovače

L2 infrastruktura

* + - * 1. OBECNÉ POŽADAVKY NA AKTIVNÍ PRVKY

Páteřní směrovače

Hraniční směrovače ě

Standardy pro CE směrovače

* + - * 1. BEZPEČNOST KOMUNIKAČNÍ INFRASTRUKTURY

Požadavky na síťovou bezpečnost

Ohrožení a rizika

Realizace bezpečné infrastruktury

* + - * 1. REALIZACE
        2. FILOZOFIE NOVÉ INFRASTRUKTURY

Filozofie síťové infrastruktury

Požadavky na připojované lokality

Typy lokalit a jejich připojení

* + - * 1. PROPOJENÍ S DALŠÍMI SUBJEKTY
        2. DESIGN PŘÍSTUPOVÝCH MÍST (POP)
        3. PROVOZ
        4. PROVOZ A PERSONÁLNÍ ZABEZPEČENÍ PROVOZU KI
        5. REALIZACE KI
        6. POŽADAVKY NA PERSONÁLNÍ ZABEZPEČENÍ PROVOZU KI

Pracovník dohledového centra

Specialista datového centra

Specialista datové sítě

* + - * 1. APLIKAČNÍ ZABEZPEČENÍ CHODU

Management sítě

Element management systém (EMS)

Management přístupů

Shromažďování a vyhodnocování logů (žurnál)

Sledování bezpečnostních nastavení a jejich souladu s bezpečnostní politikou

Zálohování konfigurací

* + - * 1. INTEGRACE KI DO INFORMAČNÍ PLATFORMY MMKV
        2. DALŠÍ ROZVOJ

Koncepce připojení bodů zájmu do KI

Provozní řád

Bezpečnostní pravidla

Koncept zabezpečení KI a koncových lokalit

Koncept koordinace rozvojových aktivit KI na regionální úrovni

Koncept koordinace složek IZS a krizového řízení

Koncept zajištění provozu a správy služeb KI

Možnosti připojení dalších systémů

### Školení

* + - 1. Uchazeč zajistí školení pracovníků Zadavatele v minimální počtu 10 osob na všechny typy dodaných aktivních prvků a problematiku provozu metropolitní datové sítě. Školení musí zahrnovat alespoň následující témata v dostatečném detailu pro porozumění architektury a způsobu provozu metropolitní sítě:
         1. Základní produktové seznámení s jednotlivými dílčími technologickými celky
         2. Zaškolení do celkového schématu sítě
         3. Principy řešení pasivní části sítě, seznámení se schématy a použitými komponentami
         4. Úvod do správy komponent napájení a monitoringu
         5. Základní zaškolení do správy aktivních prvků řešení
         6. Zaškolení na použitá nastavení sítě, detailnější rozbor použitých protokolů, konfigurací
         7. Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů
      2. Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandartních stavů systému a jejich příčin – školení bude zakončeno písemnou zkouškou potvrzující požadovanou úroveň znalostí Pracovníků a úspěšným pracovníkům bude vystaveno osvědčení o školení.
      3. Minimální rozsah školení je 76 hodin.

## Záruky a servisní podmínky

* + - 1. Zadavatel požaduje záruku na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce trvání minimálně 60 měsíců (není-li u konkrétní technologie uvedeno jinak) od okamžiku ukončení implementace a předání do produkčního provozu. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele. Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky.
      2. Záruka bude složena ze standardní záruky, která se běžně k dané dodávce zajišťuje a je součástí pořizovací ceny a z rozšířené záruky, která pokrývá období od konce platnosti standardní záruky do konce doby udržitelnosti. Uchazeč ve své nabídce výslovně uvede všechny podmínky standartních záruk a podmínky a cenu za rozšířené záruky.
      3. Zadavatel požaduje záruku na optickou infrastrukturu tj. optická vlákna v délce trvání minimálně 20 let.
      4. Po uplynutí záruky až do konce udržitelnosti projektu budou komponenty pro opravy i práce poskytovány v rámci zabezpečení podpory provozu.
      5. Po dobu udržitelnosti projektu, tj. 60 měsíců od předání díla jako celku do ostrého provozu, musí dodavatel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu, jako součást garance dodavatel prokáže podporu dodavatele popř. výrobce dodávaných zařízení.
      6. Uchazeč prokáže způsob zajištění shody dodávaných systémů s platnou legislativou.
      7. Uchazeč uvede provozní a servisní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému.

## Požadavky na zabezpečení provozu

Zadavatel požaduje detailní návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění na dobu 60 měsíců 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 Dodavatele 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 nezvyklá událost v 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,
          4. s platnou místní legislativou Zákazníka (vyhlášky, interní normy) 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 verzí software, 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 polí
          5. 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.
      23. **Profylaxe -** profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.

### Specifikace rozsahu poskytované podpory provozu

* + - 1. Základní rozsah systémové podpory v rámci měsíčního paušálu:
         1. Pravidelné servisní prohlídky a revize předepsané výrobci
         2. Proaktivní monitoring v režimu 7x24 stav sítě z pohledu aktivní i pasivní infrastruktury, bezpečnosti, analýza logů, proaktivní návrhy na upgrade řešení
         3. Provádění hardwarových oprav prvků pokrývaných v rámci smlouvy minimálně v kvalitě a parametrech jako po dobu záruky. Cena náhradních dílů je zahrnuta v paušální ceně.
         4. Řešení Incidentů dle podmínek SLA
         5. Profylaxe minimálně každých 6 měsíců
         6. Hotline podpora v režimu 7x24
         7. Patch management
         8. Rekonfigurace v rozsahu max 30 požadavků měsíčně (aktivní prvky – síťové služby, bezpečnost, QoS).
         9. Odborná podpora v režimu 9x5 – vzdálené konzultace pro dodané služby/produkty
      2. Další služby v rámci měsíčního paušálu
         1. Zajištění tj. instalaci a zprovoznění maintenance (nových verzí software a přístup k technické podpoře výrobce) a aktualizací pro veškerý dodaný software
         2. Zajištění tj. instalaci a zprovoznění maintenance (nových verzí firmware a ovládacího software a přístup k technické podpoře výrobce) a aktualizací pro veškerý dodaný hardware
         3. Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
         4. Legislativní servis
         5. Měsíčního reportingu provozu (analýza logů a poruch, zjištění celkové i konkrétní dostupnosti sítě)
      3. Součástí poskytovaných služeb budou také služby dedikovaného servisního manažera zodpovědného za provozní záležitosti (reporting, konfigurace, servis) v rozsahu alespoň 8 hodin měsíčně.
      4. Seznam prvků IT pokrývaných v rámci smlouvy vyplývá ze Zadávací dokumentace a jejích příloh, detailní seznam je součástí Prováděcí dokumentace.
      5. Uchazeč v rámci zpracování Prováděcí dokumentace stanoví kontaktní osoby a způsoby hlášení požadavků minimálně v rozsahu: emailová komunikace, telefonní komunikace, internetová komunikace a podle svého uvážení doplní další možné komunikační kanály pro zabezpečení podpory provozu a technické požadavky na jejich využití. Odpovědné osoby Zadavatele budou stanoveny v průběhu realizace I.etapy tj. Prováděcí dokumentace.

### 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.

### 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. jednoznačná identifikace Požadavku
         2. navrhovaná kategorizace a závažnost,
         3. popis Incidentu nebo Požadavku,
         4. jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh,
         5. 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 software 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 | Pasivní prvky nejpozději do 24 hod  Aktivní prvky nejpozději do 12 hod |
| B | 15 min | 4 hod | NBD |
| C | 15 min | NBD | 5BD |
| D | 15 min | NBD | BE |

* + - 1. Zadavatel si vyhrazuje právo udělit Uchazeči smluvní pokutu při nedodržení garantovaných parametrů definovaných v SLA formou poskytnutí slevy ve výši 1 (jedné) měsíční platby.
      2. Zadavatel si vyhrazuje právo navýšit smluvní pokutu v případě opakovaného nedodržení garantovaných parametrů definovaných v SLA v období 6 po sobě následujících měsíců až na 5(pět) měsíčních plateb.
      3. Pro předání požadavků na plnění závazků vyplývajících z SLA je požadováno použití technologie umožňující nepřetržitý dálkový přístup v českém jazyce.
      4. 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.