Popis nabízeného technického řešení

Obsah dokumentu

Metodika implementace

Obecné podmínky implementace

Následující podmínky vycházejí z obecných zásad řízení implementačních projektů a zahrnují zkušenosti uchazeče získané z velkého množství (stovky) projektů obdobného zaměření. Popis je použitými pojmy koncipován jako materiál nevyžadující formální vzdělání v oblasti projektového řízení a řízení IT služeb a orientuje se především na praktickou stránku a srozumitelnost implementačního postupu.

Řízení implementace

Z pohledu implementace bude uchazeč přistupovat k veřejné zakázce jako k jednomu projektu složenému z více vzájemně provázaných částí – jednotlivých komodit. Výhodou toho přístupu pro zadavatele je jednotné řízení celého projektu jedním **projektovým manažerem**, který zajišťuje plnění smluvních a dalších sjednaných činností a koordinuje činnosti jednotlivých specialistů uchazeče a jeho subdodavatelů. Projektový manažer je tak hlavním komunikačním kontaktem pro zadavatele v oblasti organizace projektu – tímto způsobem jsou minimalizovány nároky na projektový tým zadavatele z pohledu komunikace a koordinace projektu. Projektový manažer dále zajišťuje dodržování časového harmonogramu, organizaci projektových a technických schůzek, pořizování a schvalování zápisů a pravidelný reporting o průběhu projektu – tyto činnosti tak probíhají v režii uchazeče a zadavatel jimi není zatěžován. Projektový manažer je správcem případných změnových požadavků navrhovaných uchazečem či zadavatelem. V případě potřeby je projektový manažer eskalačním kontaktem první úrovně.

Pro zajištění technické konzistence celého řešení a postupu bude v implementačním týmu ustanovena role **architekta řešení** – jde o technickou roli zastřešující odbornými znalostmi celou šíři implementovaného řešení a zajišťující optimální integraci (provázání) jednotlivých technologií a částí projektu (komodit) na technické úrovni. Architekt řešení je hlavním komunikačním kontaktem zadavatele v technických záležitostech - tímto způsobem jsou minimalizovány nároky na projektový tým zadavatele z pohledu komunikace a koordinace projektu v technických záležitostech.

Zajištění vysoké odbornosti implementace a přenosu know-how

Základní úroveň využití a uplatnění doporučených postupů výrobců bude zajištěna prováděním implementačních činností specialisty certifikovanými výrobci pro danou oblast implementace. Prokázání znalostí a pochopení implementačních postupů a pravidel spolu s prokázáním technických znalostí produktů a technologií je stěžejním cílem certifikačních procesů výrobců.

Vedle technických certifikací budou všichni specialisté uchazeče i jeho poddodavatelů disponovat praktickými zkušenostmi z implementací technicky i rozsahem obdobných projektů, které uplatní v analytické, návrhové i instalační fázi projektu. Zadavatel tak získá významnou přidanou hodnotu současně v několika oblastech:

- uplatnění osvědčených postupů a řešení z obdobných projektů (tzv. best practice)
- zkrácení všech fází projektu na minimum – eliminace nevhodných variant a postupů
- minimální zátěž projektového týmu zadavatele – předkládání konkrétních návrhů či malého počtu jasně vyhodnotitelných variant namísto dotazů

Zajištění bezpečnosti

Kromě smluvního zajištění důvěrnosti dat a informací a obvyklého dodržování bezpečnostních norem a pravidel bude uchazeč v průběhu implementace klást důraz na následující oblasti bezpečnosti:

- zajištění kontinuity provozu – vzhledem k prostředí vyžadujícímu trvalý provoz IT technologií bude implementační tým nasazovat nové technologie tak, aby byl v případě potřeby schopen rychle obnovit předchozí (tzv. poslední funkční) stav
- zajištění technické ochrany dat – vzhledem k rozsáhlosti projektu a počtu změn bude uchazeč průběžně provádět zálohy dat

Dodavatele bude respektovat provozní podmínky zadavatele a činnosti vyžadující omezení provozu bude provádět v předem sjednaných časech, ve kterých bude omezení provozu zadavatele minimální. Dodavatel bude preferovat technologické postupy a řešení, které v maximální možné míře eliminují omezení provozu zadavatele a případné součinnostní kroky uživatelů či administrátorů (např. při migracích dat) umožní rozložit v čase tak, aby jejich vykonáváním nebyl omezen běžný provoz.

Implementační fáze projektu

Jednotlivé fáze projektu budou vycházet z doporučení ITIL, které pro zavádění ICT služeb (definuje následující procesy (fáze):

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement - CSI

Analytická – Service strategy

V rámci této fáze proběhne požadovaná **předimplementační analýza**. Součástí fáze je úvodní technický workshop technických specialistů uchazeče a zadavatele. Náplní workshopu je moderovaná diskuze zaměřená na technickou stránku projektu – zejména detailní specifikaci cílů projektu a očekávání jeho příjemců/uživatelů. Důležitou částí je specifikace objektivních podmínek, pravidel a zvyklostí, v nichž bude projekt realizován.

V analytické části specialisté uchazeče detailně zdokumentují stávající stav IT infrastruktury a aplikací včetně konfigurací, verzí a vzájemných vazeb.

Výstupem předimplementační analýzy bude dokument, který bude pokrývat minimálně následující oblasti:

a) Stávající stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TC.
b) MAN – řízení a zabezpečení provozu.
c) Bezpečnostní systém – zabezpečení internetové komunikace MMKV a jeho organizací, zabezpečení komunikace uvnitř MAN.
d) Provádění vzdálené správy a související nástroje.
e) Způsob začlenění nabízených komodit do prostředí TC.
f) Síťová infrastruktura ve vztahu k plánovanému využití.
g) SAN infrastruktura ve vztahu k plánovanému využití.
h) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
i) Integrace nabízených systémů.
j) Dopady implementace na dostupnost a funkčnost stávajících služeb.
k) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).
l) Požadované součinnosti zadavatele a jejich rozsah.
m) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Návrhová – Service design

Na základě zdokumentovaného stavu jednotliví specialisté pod vedením architekta řešení navrhnou detailní postupy dosažení cílového stavu včetně potřebných konfigurací jednotlivých technologií a nezbytných součinností zadavatele. V průběhu návrhu postupů budou zvažována rizika spojená s uplatněním postupu. V případě nezanedbatelného rizika bude součástí postup návrh na odstranění či zmírnění rizika. Postupy budou zpracovány do dokumentu **Prováděcí dokumentace**, který bude zadavateli prezentován a předán ke schválení. Po schválení Prováděcí dokumentace bude uchazeč podle této dokumentace realizovat instalační fázi projektu. Dokument bude zahrnovat minimálně následující oblasti:

a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,
b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TC (vSphere, LAN, SAN, zálohování, monitorování, SIEM atd.),
c) Způsob zajištění potřebného HW a SW,
d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
e) Detailní návrh a popis postupu implementace předmětu plnění,
f) Detailní popis zajištění bezpečnosti informací,
g) Detailní harmonogram realizace včetně uvedení kritických milníků,
h) Návrh designu síťového a bezpečnostního řešení a jeho konfigurace,
i) Návrh designu aplikačních řešení,
j) Vazby na stávající systémy a jejich konfigurace,
k) Návrh akceptačních kritérií a akceptačních testů.

Instalační - Service Transition

V rámci této fáze proběhne dodávka, montáž, oživení, konfigurace a otestování veškerých dodaných komponent (hw i sw) dle Prováděcí dokumentace. Pro zachování přehlednosti dokumentu neuvádíme popis této fáze jako soupis prováděných služeb dle Technické specifikace a potvrzení provedení každé z nich. Veškeré požadované služby budou uchazečem provedeny přesně dle poptávky. Pro prokázání jednoznačnosti navrženého implementačního postupu dále uvádíme chronologický seznam jednotlivých instalačních činností/kroků v doporučeném pořadí realizace, které povede k úspěšnému splnění předmětu plnění – je patrné, že projekt není vhodné (ani možné) implementovat v pořadí dle komodit a dokonce je nezbytné některé komodity implementovat ve více fázích proložených implementací jiné komodity. Všechny činnosti/kroky jsou řazeny sériově (za sebou), v průběhu implementace však budou některé z nich z důvodů urychlení implementace prováděny paralelně (souběžně), pokud to bude možné.

Implementační kroky budou vycházet z návrhové části a týkají se následujících oblastí (komodit):

K1 - Virtualizační platforma

V rámci komodity provede uchazeče implementaci nových a rozšíření stávajících technologií TC ORP tak, aby byla zajištěna výkonná a spolehlivá systémová platforma pro implementaci a provoz řešení dalších komodit – především management nástrojů K2 a K3. Konkrétně bude instalován další Blade server do stávajícího šasi v lokalitě Moskevská. Pro provoz nového server budou zkonfigurovány související technologie – LAN, SAN, diskové úložiště, blade management a záložní napájení. Pro začlenění nového serveru do TC ORP využijeme stávající licence VMware vSphere a Veeam Backup & Recovery poskytnuté zadavatelem. Pro provoz virtuálních serverů na platformě Windows Server bude sloužit dodaná licence Windows Server 2019 v edici Datacenter. Implementací komodity nebude negativně ovlivněna dostupnost ani omezena funkčnost aplikací uživatelů.

V rámci komodity budou využita doporučení výrobců především v oblasti výkonové optimalizace serverové virtualizace Performance best practices vSphere.

K2 – Komunikační infrastruktura

Prvním implementačním krokem bude rozšíření stávajícího stohu centrálních přepínačů HPE 5800. Přepínače budou zkonfigurovány dle současné konfigurace centrálního prvku MAN HP 7500. Současné konfigurace bude revidována a optimalizována z pohledu výkonu, bezpečnosti a jednoduchosti následné správy a případného dalšího rozšiřování celého řešení.

Následujícím krokem bude konfigurační příprava hraničních přepínačů ve vzdálených lokalitách na propojení se centrálním stohem. Po dokončení a otestování přípravných prací budou postupně přepojovány jednotlivé lokality na centrální stoh. Po úspěšném přepojení všech lokalit bude stávající centrální prvek HP 7500 vypnut a vyjmut z produkčního provozu.

Součástí komodity bude revize stávajících management nástrojů MAN (především HP IMC a radius serveru). Podle výsledků revize budou nástroje aktualizovány, rekonfigurovány a zachovány v provozu nebo nahrazeny jinými nástroji TC ORP. Veškerá nově dodaná zařízení a hraniční prvky lokalit budou začleněny do monitoringu TC ORP.

Při návrhu a implementaci síťových přepínačů a konfigurace MAN budou uplatněna doporučení výrobce HPE a jeho ověřených praktik tak, jak jsou specifikovány v manuálech a příručkách

a

V průběhu přepojování lokalit bude docházek ke krátkodobým výpadkům konektivity v lokalitě. Doba výpadku bude vždy v předstihu konzultována a odsouhlasena se zástupcem přepojované lokality tak, aby bylo minimalizováno (optimálně eliminováno) narušení provozu lokality.

K3 – Bezpečnostní systém

Architektura současného bezpečnostního systému (vysoce dostupný cluster dvojice NGFW firewallů) bude zachován. Konfigurace stávajících firewallů bude analyzována a v rámci předimplementační analýzy navrhneme vhodná vylepšení s důrazem na využití nových funkcionalit obsažených v aktuálních verzích firmware a zvýšení úrovně zabezpečení. Součástí nové konfigurace bude vytvoření virtuálního kontextu pro nově připojované organizace (dosud centrální firewall nevyužívají) a návrh a zapracování vhodných pravidel řízení a monitorování uživatelského provozu.

Navržené konfigurace budou otestovány a vlastní výměna firewallů proběhne mimo hlavní provoz Zadavatele a jeho organizací tak, aby bylo minimalizováno omezení jejich provozu.

Pro návrh a implementaci komodity K3 budou využiti doporučené postupy a praktiky pro aktuální verzi operačního systému (firmware) nabízených firewallů -

Součinnosti

Časová náročnost

Nezbytnou podmínkou úspěšné implementace je kvalitní součinnost specialistů, ale i uživatelů zadavatele. Uchazeč si je vědom velkého časového vytížení zaměstnanců zadavatele, proto omezí požadavky na součinnost na nezbytné minimum. Vzhledem k rozsahu projektu předpokládáme následující časové nároky na činnosti, u nichž je nezbytné součinnost (účast) specialistů zadavatele:

- Projektové schůzky, úvodní workshopy – 10 hod
- Připomínkování, schvalování dokumentace – 8 hod
- Akceptační testy – 8 hod
- Školení – 16 hodin
- Jiná součinnost (zajištění přístupů, komunikace s organizacemi, poskytnutí dokumentací apod.) – 10 hod

Vedle technických certifikací budou všichni specialisté zájemce disponovat praktickými zkušenostmi z implementací technicky i rozsahem obdobných projektů, které uplatní v analytické, návrhové, instalační i provozní fázi projektu.

Odborná náročnost

V rámci požadované součinnosti nebudou po zaměstnancích – zejména administrátorech – zadavatele požadovány žádné speciální odborné znalosti či dovednosti nad rámec aktuálně rutinně prováděných činností. Klíčovým přínosem administrátorů pro úspěch projektu je celková znalost prostředí zadavatele, způsobů využívání IT technologií, pracovních zvyklostí uživatelů a technických omezení či slabých míst stávajících technologií a řešení.

Kvalita implementace

Uchazeč splněním technických kritérií rozumí zprovoznění a nastavení dodaných technologií jednak v souladu s naplněním požadavků zadavatele na provedení služby či konkrétní funkčnost a jednak v souladu s doporučenými postupy výrobců, které de facto reprezentují technické předpisy pro

používání dodaných technologií. Dodržování obecných technický norem a předpisů (typicky Vyhláška č. 50/1978 Sb a další) je dáno certifikacemi o zavedení systém řízení jakosti uchazeče a jeho subdodavatelů dle ISO 9001 a dalších – 

Kompatibilita se současným prostředím

Uchazeč v nabídce prokazuje, že implementované řešení je plně kompatibilní se současným prostředím zadavatele. Technická kompatibilita navrženého řešení je splněna ve všech bodech podstatných pro bezproblémovou funkčnost celé ICT infrastruktury TC ORP:

- Nabízené síťové prvky jsou od stejného výrobce jako stávající - je zaručena kompatibilita na úrovni technické a funkční (VLAN, porty atd.) i na úrovni managementu pro snadné osvojení správy administrátory zadavatele
- Nabízené firewally jsou od stejného výrobce jako stávající – je zaručena kompatibilita na úrovni technické a funkční (firewallová pravidla, VPN atd.) i na úrovni managementu pro snadné osvojení správy administrátory zadavatele
- Nabízené server je od stejného výrobce jako stávající servery – je zaručena 100% kompatibilita se serverovým šasi a bezproblémové začlenění do virtualizované infrastruktury TC ORP.

Ochrana stávajících investic

Nabízené řešení významným způsobem ochraňuje zejména investice do know-how Zadavatele – znalostí a zkušeností jeho správců. Nabízené řešení je kompletně založeno na produktech, jejich používání a správa je totožné nebo velmi obdobná stávajícím produktům. Je tak zaručeno bezproblémové převzetí běžné provozní správy specialisty uživatele bez nutnosti investic do nových školení. Práce s (dlouhodobě) známými nástroji také minimalizuje riziko chyby obsluhy při jejich používání a přispívá tak k vyšší provozní bezpečnosti a efektivitě.

1. Plnění povinných parametrů technického řešení

1.1. Obecné požadavky

(1) Uchazeč v rámci zakázky navrhne:

a) způsob navýšení výpočetního výkonu TC ORP a začlenění nových zařízení do TC bez omezení poskytování jeho služeb,

b) způsob konsolidace a zvýšení dostupnosti centrální infrastruktury KI, včetně souvisejících rekonfigurací a přepojení městských organizací (jejich hraničních zařízení)

c) 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) Veškerá dokumentace vytvořená v rámci veřejné zakázky, bude zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF). Struktura i forma dokumentace bude před předáním předána ke kontrole a výslovně schválena Zadavatelem.

1.2. Specifické požadavky K1 – Virtualizační platforma

(1) Pro navýšení výpočetní kapacity TC bude dodán nový server HP BL460c Gen 10 do stávajícího Blade šasi.

(2) Pro provoz systémů a aplikací budou na nový serveru dodány licence operačních systémů Windows Server 2019 Datacenter 16core.

(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.

1.3. Specifické požadavky K2 – Komunikační infrastruktura

(1) V rámci komodity budou dodány síťové přepínače HPE 5800 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, [redacted] – centrální lokalita	1	ANO
Magistrát města [redacted] U [redacted] 2	1	ANO
Městská policie [redacted]	1	ANO
Správa přírodních léčivých zdrojů a kolonád, [redacted]	1	ANO
ZŠ Karlovy Vary, [redacted]	2	NE / Závazek dodržení standardu konektivity
ZŠ J. A. Komenského, [redacted]	2	NE / Závazek dodržení standardu konektivity

ZŠ pro žáky se specifickými poruchami učení, 	2	ANO
ZŠ Karlovy Vary, 	2	NE / Závazek dodržení standardu konektivity
Mateřská škola Komenského, 	2	ANO
Mateřská škola "Notička", 	2	ANO
Mateřská škola "Na KOPEČKU", 	2	ANO
Mateřská škola "Sluníčko", 	2	ANO
Mateřská škola, 	2	ANO
Správa lázeňských parků, 	1	ANO
Lázeňské lesy Karlovy Vary, 	1	ANO
	1	ANO
Městská policie Karlovy 	1	ANO
Základní škola jazyků, 	2	NE / Závazek dodržení standardu konektivity
ZŠ Karlovy Vary, 	2	NE / Závazek dodržení standardu konektivity
ZŠ Karlovy Vary, 	2	NE / Závazek dodržení standardu konektivity
ZŠ a ZUŠ Rybáře, 	2	ANO
ZŠ Dukelských hrdinů, 	2	NE / Závazek dodržení standardu konektivity
ZŠ Karlovy Vary, 	2	NE / Závazek dodržení standardu konektivity
ZŠ Karlovy Vary (odloučené pracoviště), 	2	ANO
Mateřská škola 	2	ANO
Mateřská škola "Studánka", 	2	ANO
Mateřská škola "Zdravá mateřská školka", 	2	ANO
Mateřská škola Hornická, 	2	ANO
Mateřská škola, 	2	ANO
Mateřská škola, 	2	ANO
Mateřská škola, 	2	ANO
Mateřská škola, 	2	ANO
Mateřská škola, 	2	ANO

Mateřská škola, [redacted]	2	ANO
Mateřská škola, [redacted]	2	ANO

(4) U lokalit, kde je uveden „Závazek dodržení standardu konektivity“, bude zajištěno 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. V nezbytných případech zajistí Uchazeč provedení validačních testů podle Standardu konektivity.

(5) Konfigurace prvků komunikační infrastruktury budou vycházet ze stávajících konfigurací, které budou optimalizovány s ohledem na aktuální doporučení výrobců a osvědčené praktiky (best practice), zejména v oblasti kybernetické bezpečnosti.

(6) Součástí komodity bude převzetí stávajících monitorovacích a notifikačních pravidel ze systému IMC a jejich úprava a přenesení do monitorovacího systému TC.

1.4. Specifické požadavky K3 – Bezpečnostní systém

(1) Nabízené řešení bude tvořit kombinace dvou nově pořízených firewallů FortiGate 201E, 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 bude 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.

1.5. Popis povinných parametrů dodávaného řešení

(1) V dále uvedené tabulce tabulkách jsou uvedeny minimální povinné a nabízené 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 server 1 ks HP BL460c Gen10	Provedení	Blade server	Blade server	Příloha **07 Datový list HPE Proliant BL460c Gen10 Server Blade.pdf**
	Procesor	Minimálně 2x procesor osmi-jádrový (dohromady tedy min 16 jader). Výkon serveru dle http://www.spec.org: SPECrate2017_int_base min 105 bodů SSPECrate2017_fp_base min 120 bodů	2x procesor osmi-jádrový **Intel Xeon Gold 6134**. Výkon serveru dle http://www.spec.org/: SPECrate2017_int_base = 106 bodů SPECrate2017_fp_base = 122	
	Pevné disky	2x SSD, min. 240 GB pro hypervizor	2x SSD, 240 GB pro hypervizor	
	Paměť	minimálně 384 GB RAM, min. 2600 MT/s	384 GB RAM, 2666 MT/s	
	Rozšiřitelnost	rozšiřitelnost RAM min. na 700 GB bez výměny RAM modulů	rozšiřitelnost RAM na 896 GB bez výměny RAM modulů	
	RAID	řadič RAID 0,1, 10, zálohovaná vyrovnávací paměť pro zápis min. 1 GB	řadič RAID 0,1, 10, zálohovaná vyrovnávací paměť pro zápis 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	LAN 2x10Gb s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. Podpora partitioningu – rozdělení fyzického LAN adaptéru na více virtuálních adaptérů - 4 virtuální adaptéry na každý port	
	FC porty	2x FC (fibre channel) port min. 16 Gb	2x FC (fibre channel) port 16 Gb	
	Vzdálená správa	Podpora vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média.	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)	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	Plně kompatibilní se stávajícím Blade šasi HP C7000 na fyzické i elektrické úrovni	
	Vysoká dostupnost	Podpora a licence pro clusterový provoz	Podpora a licence pro clusterový provoz	
	Management	Plná integrace s management modulem HP Blade šasi HP 7000	Plná integrace s management modulem HP Blade šasi HP 7000	
	Záruka	Záruka 36 měsíců, oprava následující pracovní den v místě instalace	Záruka 36 měsíců, oprava následující pracovní den v místě instalace	
SW licence operačních systémů Windows Server 2019	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	Licence 64 - bitového serverového operačního systému v aktuální verzi pro nabízený server Windows Server 2019 Datacenter 16 core. Licence umožňuje provoz neomezeného počtu virtuálních serverů stejné verze v prostředí stávající serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů a systémů. Licence umožňuje instalaci a provoz předchozích verzí systému - tzv. downgrade	Příloha **07 Datový list Windows_Server_2019.pdf**

Datacenter 16 core				

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 HPE FlexFabric 5800 (JC100B + modul JC091A)	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U	L2/L3 přepínač v rackovém provedení 1U	**Příloha 07 Datový list HPE FlexFabric 5800.pdf**
	Propustnost	neblokovaná architektura, propustnost min. 200 Gb	neblokovaná architektura, propustnost 200 Gb	
	Porty	8x 10 Gb SFP+, 24x 1 GbE	8x 10 Gb SFP+, 24x 1 GbE (s expanzním modulem JC091A 4x 10 Gb SFP+)	
	Agregace portů	podpora LACP	podpora LACP	
	Směrování	statické a dynamické routování, policy based routing	statické a dynamické routování, policy based routing	
	Řízení provozu	víceúrovňový QoS	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	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	podpora 802.1X	
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS	plný IPv4 a IPv6 dualstack včetně směrování a QoS	
	Pokročilé funkce	plná podpora MPLS a VPLS včetně L2 a L3 MPLS VPN	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)	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	kompatibilní s přepínači HPE 5800 na úrovni pokročilého stohování	
	Sledování toků	export síťových toků (Netflow nebo ekvivalent)	export síťových toků (Netflow nebo ekvivalent)	
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní	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	60 měsíců, oprava/výměna zařízení 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	**6 ks modulů SFP+ 10 Gb, MM včetně DMI diagnostiky pro nabízený centrální přepínač, LC konektor**	Standardní OEM výrobky kompatibilní s nabízenými a stávajícími výrobky
	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	**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 m 28 ks kabel SM s konekrory LC-E2000, délka 10 m	**4 ks kabel MM s konektory LC-LC, délka 1 m** **2 ks kabel MM s konektory LC-LC, délka 5 m** **28 ks kabel SM s konekrory LC-E2000, délka 10 m**	
	Záruka	36 měsíců	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**
Firewall 2x FortiGate FG-201E	Provedení	hardwarový firewall pro umístění do datového rozvaděče 19", výška max. 1U, včetně montážního materiálu	hardwarový firewall pro umístění do datového rozvaděče 19", výška 1U, včetně montážního materiálu	Příloha **07 Datový list FortiGate200E Series.pdf**
	NGFW	zařízení typu next generation firewall - https://en.wikipedia.org/wiki/Next-generation_firewall	zařízení typu next generation firewall	
	Porty	min 14x 1GbE (min. 2x WAN) a 4x 1 Gb SFP (nesdílené), USB pro ext. modem	14x 1GbE (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	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	20 Gbps pro pakety 512b	
	Úložiště	interní úložiště typu SSD pro ukládání logů, reportů apod., velikost min. 450 GB	interní úložiště typu SSD pro ukládání logů, reportů apod., velikost 480 GB	
	Počet současných spojení	min. 2 milióny	2 milióny	
	Propustnost SSL VPN	min. 500 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 současně připojených klientů	900 Mbps, 500 současných VPN 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)	7,2 Gbps, bez licenčního a technické omezení počtu klientů	
	Propustnost IPS	min. 2 Gbps pro vzorový provoz (tzv. Enterprise mix) - aktivní firewall, aplikační kontrola, ochrana proti škodlivému kódu, logování	2,2 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	1.8 Gbps - aktivní firewall, aplikační kontrola, IPS, logování	
	Propustnost SSL inspekce	min. 800 Mbps při aktivní IPS	820 Mbps při aktivní IPS	
	Kombinovaná propustnost	Firewall + aktivní IPS + aplikační kontrola + antimalware min. 1 Gbps pro běžný provoz	Firewall + aktivní IPS + aplikační kontrola + antimalware 1,2 Gbps pro běžný provoz	
	Politiky, pravidla	podpora min. 8000 politik/pravidel firewallu	podpora 10 000 politik/pravidel firewallu	
	Virtualizace	min. 10 virtuálních kontextů	10 virtuálních kontextů	
	Vysoká dostupnost	režimy Active/Passive i Active/Active se společnou konfigurací, vyhrazené porty pro v	režimy Active/Passive i Active/Active se společnou konfigurací, vyhrazené porty pro v	
	Dualstack	podpora současného běhu IPv4 a IPv6	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.	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 portu	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...)	

Komodita K3 - Bezpečnostní systém				
		Kontrola 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)	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	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	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	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	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	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.	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,	HTTP/S, SSH, SNMP, syslog,	
	Reporty	Integrované logování a reporting, možnost vytváření vlastních reportů	Integrované logování a reporting, možnost vytváření vlastních reportů	
	Sledování toků	export síťových toků (Netflow nebo ekvivalent)	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)	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	NAT, statické a dynamické routování, publikace interních serverů	
	Certifikace	doložení certifikace nabízeného řešení obecně uznávanou autoritou. např. ICSA Labs apod.	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)	12 měsíců v režimu 24x7. Odesláním náhradního zařízení následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a UTM (URL filtrace, IPS, antimalvare, antispam, aplikační kontrola, sandbox)	

1.6. Architektura technického řešení

(1) Architektura komodit bude navržena tak, aby vhodně využívala a doplňovala stávající prostředky TC.

1.7. Rozhraní

(1) Veškeré nabízené aktivní hardwarové produkty disponují rozhraním SNMP v2 a v3 pro management a vzdálenou správu.

1.8. Kompatibilita s ostatními systémy

(1) Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí VMware vSphere a jsou pro běh v tomto prostředí výrobcem podporovány.

(2) Řešení komodity K2 a K3 bude plně kompatibilní se stávajícím řešením SIEM na úrovni zasílání/sběru logů a událostí.

1.9. Typy klientů

(1) Webová rozhraní všech komodit budou kompatibilní s prohlížeči Microsoft Edge, Firefox a Chrome v aktuálních verzích.

1.10. Bezpečnost informací

(1) Veškeré nástroje pro správu hardware umožňují správu interních účtů (jméno a heslo) a/nebo napojení na Active Directory.

(2) Veškeré nástroje pro správu hardware umožňují definici s 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa).

(3) Veškeré nástroje pro správu hardware komunikují se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) bude použita šifrovaná komunikace (např. HTTPS).

1.11. Obecné požadavky na implementační služby

(1) Budou provedeny následující implementační práce na dodaných komponentech a případně dalších zařízeních. Implementační služby budou v následujícím rozsahu:

a) Zajištění projektového vedení realizace předmětu plnění.
b) Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je i provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu.
c) Dodávku nabízených zařízení a kompletní implementaci řešení splňující povinné parametry technického řešení,
d) Provedení školení,
e) Zajištění zkušebního provozu,
f) Provedení akceptačních testů,
g) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.
h) Předání do plného provozu,

(2) Veškerá dokumentace bude zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

(3) Činnost omezující práci uživatelů budou prováděny mimo běžnou pracovní MMKV a organizací, tj. mimo pracovní dny 7 – 17 hod.

(4) Provedemee specifické služby a požadavky specifikované v následujících tabulkách.

K1: Virtualizační platforma
a) Návrh a kompletní provedení rozšíření serverové virtualizační platformy TC ORP. b) Implementace pořízených technologií c) Analýza dat a systémů na stávajících serverech škol a jejich migrace na novou platformu d) Návrh a provedení rozšíření zálohovacího řešení e) Návrh a realizace konfiguračních změn infrastruktury (virtualizační platforma, LAN, SAN) f) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti
K2: Komunikační infrastruktura
a) Analýza stávajícího síťového prostředí a návrh nové architektury MAN s využitím poskytnutých konfiguračních souborů a dokumentace současného provedení b) Optimalizace architektury MAN – bezpečnost, dostupnost, výkon c) Revize a optimalizace segmentace – VLAN, adresování, routování d) Návrh monitorování MAN e) Realizace navrženého a schváleného řešení včetně konfigurací stávajících systémů f) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti
K3: Bezpečnostní systém
a) Návrh a realizace vhodného začlenění nabízeného firewallu do stávajícího prostředí, zejména způsob náhrady stávajících firewallů – vymezení rolí a pravidel, politik, využití synergií b) 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 c) Optimalizace převzatých konfigurací a politik/pravidel s ohledem na aktuální možnosti nabízeného řešení a rizika kybernetické bezpečnosti d) Vybudování VPN pro vzdálený přístup uživatelů na bázi webového portálu e) Konfigurace logování pro SIEM – zohlednění nově začleněných organizací f) Návrh a provedení konfigurací dotčených a souvisejících systémů g) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti.

1.12. Zpracování prováděcí dokumentace

(1) Před zahájením implementačních prací bude zpracována prováděcí dokumentace, 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 bude provedena předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění, zejména pak s ohledem na použité technické řešení, pro následující oblasti:

a) Stávající stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TC.
b) MAN – řízení a zabezpečení provozu.
c) Bezpečnostní systém – zabezpečení internetové komunikace MMKV a jeho organizací, zabezpečení komunikace uvnitř MAN.
d) Provádění vzdálené správy a související nástroje.

e) Způsob začlenění nabízených komodit do prostředí TC.
f) Síťová infrastruktura ve vztahu k plánovanému využití.
g) SAN infrastruktura ve vztahu k plánovanému využití.
h) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
i) Integrace nabízených systémů.
j) Dopady implementace na dostupnost a funkčnost stávajících služeb.
k) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).
l) Požadované součinnosti zadavatele a jejich rozsah.
m) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(3) Prováděcí dokumentace zohlední podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního nabízeného technického řešení a bude obsahovat tyto části:

a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,
b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TC (vSphere, LAN, SAN, zálohování, monitorování, SIEM atd.),
c) Způsob zajištění potřebného HW a SW,
d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
e) Detailní návrh a popis postupu implementace předmětu plnění,
f) Detailní popis zajištění bezpečnosti informací,
g) Detailní harmonogram realizace včetně uvedení kritických milníků,
h) Návrh designu síťového a bezpečnostního řešení a jeho konfigurace,
i) Návrh designu aplikačních řešení,
j) Vazby na stávající systémy a jejich konfigurace,
k) Návrh akceptačních kritérií a akceptačních testů.

(4) Prováděcí dokumentace bude 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.

1.13. Harmonogram realizace

(1) Bude zajištěno 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) Harmonogramu plnění – zde jsou uvedeny 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

1.14. Školení

(1) Bude zajištěno školení pracovníků zadavatele – administrátorů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to 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) Rozsah školení bude 16 hodin v oblastech

a) Architektura a správa MAN, zálohování a obnova firmware

b) Monitoring a management, nástroje a použití

c) Firewall – nové funkcionality, základní správa a analýza provozu a událostí

(4) Školení bude probíhat v sídle zadavatele.

(5) Předpokládá se účast max. 4 administrátorů.

1.15. Testovací prostředí

(1) Není požadováno testovací prostředí

1.16. Provedení akceptačních testů, zkušební provoz a přechod do ostrého provozu

(1) Bude navržen způsob a provedení akceptačních testů.

(2) Součástí akceptačních testů budou pro každou komoditu:

a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

(3) Pro každou komoditu budou navrženy vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení.

(4) Akceptačním kritériem pro akceptaci díla jako celku bude prokázání zajištění požadavků Standardu konektivity dle manuálu uveřejněného na [redacted] včetně úspěšného provedení a doložení testu [redacted] 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.

(5) O provedení akceptace a jejím výsledku bude vyhotoven písemný protokol.

(6) Bude zajištěn zkušební provoz v délce 10 dnů včetně technické podpory 1 specialisty na dodané řešení s dojezdem 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.

(8) Akceptační scénáře (nad rámec základních akceptačních testů):

a) Výkonnostní testy – průchodnost MAN pro lokality

b) Výkonností testy – průchodnost firewallu při běžném http a https provozu

c) Základní bezpečnostní testy firewallu – antivirová kontrola, skenování portu apod.

2. Záruky a servisní podmínky

(1) Záruka na veškeré dodané služby v délce trvání 3 měsíců a zařízení 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, nabízí uchazeč 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) Bezplatný k aktualizacím software a firmware dodaných komodit bude poskytován minimálně po dobu záruky.

(5) Prodloužená záruky na všechna dodaná zařízení s výjimkou operačních systémů a optických prvků je nabízena na 60 měsíců, a to v kvalitě a parametrech shodných se základní požadovanou zárukou.

(6) Součástí technické podpory je spolupráce s administrátory zadavatele při řešení nekompatibilit aplikací a systémů.

(7) Pro hlášení servisní požadavků bude poskytnut Zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Provozní doba helpdeskového systému je 7-17 hod. v pracovních dnech.

(8) Popis obluhy helpdeskového systému je obsažen v příloze 07 Helpdeskový systém-manuál pro zákazníka.pdf

3. Zabezpečení provozu

Detailní návrh podmínek podpory zajištění provozu, zajišťující garantovanou úroveň služeb podpory zajištění provozu předmětu plnění od doby předání do plného provozu.

3.1. 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:

a) žádost o odstranění závady (nefunkční Prvek IT nebo nesprávná činnost Prvku IT) - incidentu

b) žádost o poskytnutí konzultace

c) žádost o provedení Změny

Požadavek může:

d) být zadán zadavatelem jako jednorázový

e) být zadán zadavatelem jako opakující se činnost

f) vzniknout jako výstup Monitorování

g) vzniknout na základě Správy a údržby Prvku IT

(19) **NBD**-**Next Business Day** – následující pracovní den

(20) **Neprodleně** – bez zbytečného odkladu, s vyvinutím maximálního úsilí na zjednání nápravy nebo zajištění činnosti, nejpozději však následující Pracovní den.

(21) **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.

(22) **Prvek IT** - zařízení (Koncové zařízení, server či jiný hardware), program (software) nebo komunikační linka.

(23) **Rozsah poskytovaných služeb** – specifikace Služby a kvantifikace rozsahu Služby

(24) **Řešitel** - Pracovník uchazeče, podílející se na řešení Požadavku.

(25) **Report** – přehledový dokument, ve kterém je popsán průběh realizace Plnění za uplynulé období a hodnoty sledovaných parametrů.

(26) **SLA (Service Level Agreement)** - definice kvalitativních parametrů/metrik Služby

(27) **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.

(28) **Služby** – činnosti potřebné pro řádné zabezpečení podpory provozu díla

(29) **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.

(30) **Vzdálená správa** – provádění činností na Prvcích IT, přičemž činnosti nejsou prováděny v místě provozovny zadavatele, ale prostřednictvím Vzdáleného přístupu z místa provozovny uchazeče.

(31) **Vzdálený přístup** – připojení z provozovny uchazeče k zařízení zadavatele pomocí komunikační linky, na které je vytvořeno dočasné nebo trvalé spojení.

(32) **Zprovoznění náhradním způsobem** - se rozumí zajištění základních funkcí systému, tedy dosažení stavu, kdy není vážně omezena funkčnost informačního systému nebo jeho částí.

(33) **Změna** - změna parametrů Prvku IT nebo instalace, přemístění či odinstalace Prvku IT.

(34) **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.

(35) **Reklamace -** reklamací je požadavek vznesený na přezkoumání a odstranění vlastnosti Prvku IT v čase záruční doby, která je v rozporu:

a) se standardní funkčností Prvku IT a tento rozpor je vůči uživatelské dokumentaci produktu,

b) s funkcionalitou definovanou ve smlouvě (jejích přílohách), případně akceptačním protokolu funkcionality Prvku IT,

c) s platnou legislativou ČR k datu podání požadavku.

(36) **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.

(37) **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.

(38) **Hotline podpora** - jde o službu zajišťující poradenství po telefonu nebo elektronické komunikaci

(39) **Maintenance –** jedná se o zajištění nových a opravných verzí software (včetně hlavních verzí), nových verzí firmware, přístupu k technické podpoře výrobce a přístupu k databázi řešených problémů.

(40) **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:

a) monitoring operačních systémů,

b) monitoring sítě a síťových propojení Systému a Systémů třetích stran,

c) monitoring bezpečnostních systémů,

d) 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.

(41) **Profylaxe -** profylaxe zahrnuje aktualizace firmware zařízení, aktualizace administrátorských nástrojů, kontrolu logů, kontrolu vytížení a využití, kontrolu kapacit.

3.2. Specifikace rozsahu nabízené 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 –1x ročně nebo bezodkladně v případě kritických bezpečnostních aktualizací, změn legislativy či změn navázaných systémů.

(2) V rámci zabezpečení provozu budou poskytnuty následující služby:

a) Pravidelné servisní prohlídky a revize předepsané výrobci.

b) 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 budou přístup ke sledovaným parametrům alespoň v režimu čtení.
c) Řešení incidentů – dle podmínek SLA, 4 hod. v rámci měsíčního paušálu
d) Řešení Požadavků – 2 hodiny v rámci měsíčního paušálu.
e) Profylaxe – každých 6 měsíců.
f) Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.
g) Hotline podpora a Odborná podpora – vzdálené konzultace pro podporované služby/produkty. Celkový rozsah služeb Hotline a Odborné podpory v rámci měsíčního paušálu je 2 hodiny. Dostupnost Hotline a Odborné podpory v režimu 9x5.

(3) Seznam prvků pokrývaných službou zabezpečení provozu je uveden v 3.5.

3.3. 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 TC ORP a prevenci incidentů.

(2) Souhrn informací o poskytovaných službách (report) bude obsahovat informace o jednotlivých službách a jejich provádění (dle povahy jednotlivých služeb a definice dle katalogových listů služeb).

(3) Měsíční report bude vyhotovován výhradně v elektronické formě a bude obsahovat souhrn činností provedených za vykazované období.

(4) Report bude za příslušné období vždy obsahovat:

a. Informace o provedených změnách v TC spojených s poskytováním služby.
b. Požadavek na součinnosti zadavatele, požadované uchazečem, k tomu, aby mohl dostát svým závazkům v poskytování předmětné služby.

3.4. Způsob poskytování plnění

(1) Plnění je poskytováno zejména následujícím způsobem:

a) Prostřednictvím pracovníka uchazeče přímo na pracovišti zadavatele,
b) Prostřednictvím pracovníka uchazeče Vzdálenou správou,
c) Prostřednictvím pracovníka uchazeče formou vzdálené konzultace,
d) 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 podmínky pro řádné plnění, zejména

a) v případě Monitorování a Vzdálené správy zajistit a udržovat podmínky pro Vzdálený přístup uchazeče k prvkům IT,
b) zajistit dostupnost nebo odpovídající zástup Odpovědné osoby zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby zadavatele a zajištění efektivní součinnosti odborných pracovníků zadavatele,
c) 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,

d) 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,

e) umožnit uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,

f) 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

a) písemně či elektronicky potvrdit uchazeči provedení služby,

b) 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,

c) 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.

3.5. Seznam prvků IT

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

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

3.6. 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:

a) navrhovaná kategorizace a závažnost,

b) popis incidentu nebo Požadavku,

c) jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh,

d) kontaktní osoba.

(3) Používaný systém pro HelpDesk bude pokrývat uvedené informace pro nahlášení požadavku.

(4) Incidenty budou 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.

(5) 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.

(6) 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).

(7) 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.

(8) 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.

(9) 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.

(10) V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora incidentu informuje o:

a) čase vyřešení požadavku,

b) v případě incidentu specifikuje příčinu (pokud je známa),

c) vyzve iniciátora k ověření funkčnosti služby.

(11) Po ověření funkčnosti ze strany zadavatele se Požadavek považuje za vyřešený.

(12) 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.

(13) 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.

3.7. 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

(2) Pro předání požadavků na plnění závazků vyplývajících z SLA, je bude využito technologie umožňující nepřetržitý dálkový přístup v českém jazyce.

4. Hodnocené parametry technického řešení

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,	Webový portál My Networking společnosti HPE (Hewlett Packard Enterprise)	Příloha **07 My Networking.pdf**
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,	Webový portál My Networking společnosti HPE (Hewlett Packard Enterprise)	Příloha **07 My Networking.pdf**
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,	Webový portál My Networking společnosti HPE (Hewlett Packard Enterprise)	Příloha **07 My Networking.pdf**
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:	Webový portál My Networking společnosti HPE (Hewlett Packard Enterprise)	Příloha **07 My Networking.pdf**

Hodnocené parametry			
	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	Nabízené firewally využívají shodný operační systém (firmware) FortiOS. Přiložený dokument FortiOS_release_notes.pdf v sekci Supported models uvádí podporu FortiOS pro stávající i nabízené firewally. Využitím shodné verze FortiOS je zajištěna 100% kompatibilita a přenositelnost konfiguračních nastavení a souborů i podpora využití jednotných skriptů pro správu. Shodný OS zajišťuje také zcela shodné příkazy CLI ve stávajícím i nabízeném firewallu. –	Příloha **07 FortiOS_release_notes.pdf**