

Projektový záměr „Konsolidace IT a nové služby TC ORP Přelouč“**TECHNICKÁ SPECIFIKACE**

Vymezení předmětu plnění

1. Předmět plnění

(1) Předmětem plnění veřejné zakázky jsou dodávky a služby pro realizaci projektu „Konsolidace IT a nové služby TC ORP Přelouč“, reg.č. CZ. 1.06./2.1.00/22.09510, včetně podpory po dobu udržitelnosti, dále také jen "řešení".

(2) Předmětem plnění veřejné zakázky jsou tři celky uvedené v následující tabulce:

Označení	Název	Počet
K1	Virtualizační platforma	1
K2	Bezpečnostní infrastruktura	1
K3	Elektronizace procesů	1

2. Popis současného stavu

2.1. Popis stávajícího HW prostředí

(1) Zadavatel v současnosti disponuje technologickým centrem i řádnou ICT infrastrukturou pro implementaci a provoz plánovaných řešení, kterou je však nutné doplnit o další zařízení.

(2) Ve stávajících rackových skříních je k dispozici místo pro doplnění nově pořizovaných HW jednotek. Serverová místnost je řádně klimatizovaná a s dostatečnou kapacitou pro chlazení nově pořizovaných technologií, k dispozici jsou 2x klimatizační jednotky. Sít'ová infrastruktura je ve stavu, který umožňuje provoz nově pořizovaných systémů a aplikací.

(3) Serverová infrastruktura je postavena na hardware společnosti IBM. Obsahuje 2 servery IBM x3690 X5 (2x CPU E6540/ 48 GB RAM / 2x HDD 73 GB/ FC 8 Gb 2port) ve virtualizačním clusteru s virtualizační platformou VMware ESXi 4.1 upgrade na ver. 5.0 (licencována jako VMware vSphere Essential Plus Kit pro max. 3 ks serverů s celkem 6 procesory včetně management SW VCenter Essential). Do tohoto virtualizačního clusteru bude připojen server pro virtualizaci.

(4) Další server IBM x3250 M3 (1x CPU X3460 / 4 GB RAM / 2x HDD 146 GB/ FC 8 Gb 2port) je využit jako management server bez nasazené virtualizace. Servery jsou propojeny redundantně do SAN přes 2 SAN switche IBM SAN24B s rozhraním FC 8 Gb, k těmto switchům je připojeno diskové pole IBM Systém Storage DS3512 s 12 ks HDD 600 GB, dále je také připojena pásková knihovna IBM TS3100, která při plánované konsolidaci zálohování bude využita jako druhý stupeň zálohy.

(5) Sít'ová infrastruktura je založena na 5 switchích Juniper EX-4200 (5x 48 port) propojených tak, aby tvořily jeden virtuální switch. Hraničním zařízením na straně Městského úřadu jsou dva firewally Juniper SRX 240.

(6) Tyto firewally nejsou z povahy věci určeny pro zamýšlené nasazení, neposkytují možnost zvýšení bezpečnosti doplněním o integrované IPS a Anti-X ochranu. Rovněž vyžadují vysoké nároky na administraci, proto budou využity pouze jako firewally technologického centra ORP. Budou tedy zabezpečovat připojení uživatelů k serverům. Jako hraniční firewally k internetu a vnějším sítím budou použity Next Generation Firewall modely.

2.2. Popis stávajícího SW prostředí

- (1) Systémové služby jsou provozovány především na platformě Microsoft.
- (2) Operační systém serverů ve virtuálním prostředí je Microsoft Windows Server 2003 a 2008, dále pak linuxové servery.
- (3) V síti je implementována adresářová služba Microsoft Active Directory a jsou aktivně využívány tyto platformy: Microsoft Exchange 2010 jako groupware, Microsoft SharePoint (bezplatná verze) jako platforma pro specializovaná portálová řešení, Microsoft SQL Server pro informační systém.
- (4) Standardním kancelářským balíkem využívaným zadavatelem je Microsoft Office, s ohledem na sjednocení uživatelského rozhraní a kompatibilitu dokumentů ve verzi 2007 a vyšší. Standardně jsou využívány aplikace Word, Excel, Outlook a OneNote.
- (5) Informační systém (spisová služba, ekonomický subsystém) je postaven na jádře GINIS od firmy Gordic Jihlava

3. Povinné parametry technického řešení

3.1. Obecné požadavky

- (1) Nabízená řešení nesmí negativně ovlivnit stávající parametry TC.
- (2) Zadavatel při výstavbě, správě a provozu ICT technologií striktně dodržuje hledisko technologické neutrálnosti tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.
- (3) Pokud uchazeč vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
- (4) Za předpokladu, že uchazečem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, komunikační prvky, atd.) neobsaženou v popisu předmětu plnění, zahrne uchazeč do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.
- (5) Pro každý softwarový produkt, který uchazeč nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury na které bude řešení provozováno.
- (6) Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky - není přípustné implementovat např. další serverovou virtualizační platformu apod.
- (7) Dodavatel prokáže, že všechny výrobky, které dodá Zadavateli:
 - (a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
 - (b) mají plnou záruku od výrobce,
 - (c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
 - (d) obsahují licenci na používání příslušného softwaru,
 - (e) jsou v databázi výrobce uvedeny jako prodaná Zadavateli,

(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. uchazečem samotným, nelze-li prohlášení distributora získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

3.2. Požadavky na kompatibilitu s ostatními systémy

(1) Technické řešení musí být plně kompatibilní se stávající serverovou i LAN infrastrukturou na úrovni standardních protokolů a funkcionalit včetně VLAN.

3.3. K1- Virtualizační platforma

(1) Položka K1 je tvořena 3x nově dodávanými servery, rozšířením RAM stávajících serverů, 2x nově dodávanými zdroji UPS a zálohovacím SW.

(2) Server pro disaster recovery bude využit v případě výpadku hlavní lokality pro spuštění kritických aplikací, tak aby případný výpadek hlavní lokality neohrozil fungování úřadu.

(3) Výše popsané servery je nutné doplnit o 2 záložní zdroje (1 bude umístěn v hlavní lokalitě, 1 v záložní lokalitě) s dostatečnou kapacitou pro korektní vypnutí systémů při výpadku elektrické energie nebo pro běh systémů před přepnutím na záložní motorgenerátor.

(4) Pro zálohování celé virtualizované infrastruktury (3 ks HW serverů s celkem 6 procesory, z toho jeden nově dodaný) je nutné nasadit sofistikovaný zálohovací systém (zálohovací SW), který komplexně pokryje veškerou zálohovací agendu včetně disaster recovery – obnovení po havárii.

3.4. K2 - Bezpečnostní infrastruktura

(1) Položka K2 je tvořena 2x firewally, systémem pro bezpečnost a řízení datových toků (Network Behaviour Analyser), monitorovacím SW a systémem SIEM.

(2) Bezpečnost a řízení datových toků bude zastřešováno dvojicí centrálních firewallů – (jeden pro hlavní datové připojení k internetu, druhý pro záložní datové připojení k internetu). Na centrálních firewallích bude řízen provoz mezi jednotlivými VLAN segmenty, DMZ zónami resp. mezi zónami s rozdílnou úrovní důvěryhodnosti (například Internet vs. DMZ, uživatelé vs. DMZ, uživatelé vs. Interní servery).

(3) Vzhledem k předpokládanému využití firewallů pro ochranu serverových systémů v datovém centru jsou vyžadovány vysokorychlostní firewally. Firewally musí garantovaně podporovat rychlosti v řádech Gigabitů za vteřinu.

(4) Firewally bude v souladu s celkovou filosofií komunikační infrastruktury zapojeny do páteřních přepínačů agregovanými vícenásobnými 1GE (až 16x1GE) prostřednictvím Etherchannel (802.3ad).

(5) Firewally musí disponovat rozšířeními ochrany před útoky na síťovou infrastrukturu, tzn. vlastnosti UTM firewallu (URL filtering, Anti-Virus, Anti-Spam, Anti-Bot).

(6) Další požadovanou funkcí je detekce a prevence před útoky IPS sondami, které budou nasazeny pro hloubkovou ochranu vybraných segmentů sítě (typicky např. síť v datovém centru).

(7) Firewall musí podporovat integraci s monitorovacím SW a SIEM systémem.

(8) Implementace systému pro sledování datových toků zahrnuje rozmístění pasivních sond do vybraných částí sítě (pomocí zařízení TAP nebo mirror portu na switchích). Tyto sondy budou analyzovat veškerý provoz v dané části sítě a získané a předzpracované hodnoty zasílat na centrální systém (kolektor), kde bude probíhat jejich další zpracování a vyhodnocování.

(9) Sondy i kolektor budou připojeny přímo do vyhrazené sítě určené pro monitorování infrastruktury.

(10) Systém pro bezpečnost a řízení datových toků bude zahrnovat sondu, na kterou bude zrcadlen zájmový provoz. Vzhledem k plánovanému nasazení je požadováno, aby disponovala minimálně čtyřmi 10/100/1000 Mb ethernet porty. Na každý z portů lze zrcadlit jiný segment sítě (např. internet, DMZ, VPN provoz apod.). Je vhodné, aby funkcionality kolektoru byla pouze jako SW modul na samotné sondě (náklady na provoz a údržbu dalšího HW apod.). Naopak sonda bude ve formě HW zařízení a to primárně z důvodu velkého výpočetního zatížení při analýze provozu.

(11) Vzhledem k tomu, že s virtualizací aplikací přichází větší závislost na fungování infrastruktury, bude součástí technické řešení monitorovací nástroj, který umožní aktuální i historický přehled o fungování infrastruktury. Cílem je integrovat všechny klíčové součásti infrastruktury, což zahrnuje:

- Síťové komponenty
- Servery
- HW monitoring serverů
- Disková pole
- UPS
- Teplotní čidla
- Bezdrátovou síť
- Firewall
- RMS systém

(12) Monitorovací systém musí podporovat standardizované technologie monitoringu, jako jsou SNMP, WMI, ICMP, TCP a UDP testování.

(13) Monitorovací systém bude disponovat předpřipravenými šablonami pro cílové zařízení včetně prahových hodnot chybových stavů.

(14) SIEM (Security Information and Event Management) je systém, který automaticky sbírá, archivuje a analyzuje logy bezpečnostní povahy napříč celou infrastrukturou od síťových prvků přes různé operační systémy až po aplikace. Nad těmito daty pak bude probíhat pokročilá analýza, korelace a notifikace vyhodnocených bezpečnostních událostí a fenoménů.

(15) Díky tomuto systému bude možné mít aktuální přehled o potencionálních i skutečných anomáliích, hrozbách a bezpečnostních incidentech sledovaného prostředí. K nim poskytuje zdrojová data pro daný kontext a řešení.

(16) SIEM je řízen sadou pravidel vzniklých z předem popsanych modelových situací.

(17) Systém SIEM obsahuje také předdefinované pohledy a reporty podle mezinárodních standardů jako PCI-DSS, HIPAA, NERC-CIP, FISMA a další pro účely auditu.

(18) SIEM - sběr logů - formy sběru dat lze definovat do několika kategorií:

- (a) Obecné protokoly: TCP a UDP Syslog, SNMP, Netflow, SCP, FTP
- (b) Proprietární protokoly: OPSEC, WMI, MSSQL apod.
- (c) Lokální agent na serveru

(19) Komunikace mezi agentem a SIEM systémem bude probíhat šifrovaně a pro úsporu přenosové kapacity budou přenášena data komprimována.

(20) Zdroje dat pro SIEM systém budou zahrnovat:

- (a) (7 stávajících + 5 nových na virtuální aplikaci) Windows serverů (verze 2008, 2012) - stávající zakoupeny v roce 2011
- (b) 1 Linux server
- (c) 1 MS SQL server
- (d) NextGeneration firewall – součástí dodávky
- (e) 2x pátevní přepínače
- (f) cca 20 přepínačů

(21) Analýza rozsahu a způsobu sběru logů bude součástí implementačních prací, jejich rozsah bude přesně definován v prováděcím projektu před samotnou implementací. Nad takto definovaným rozsahem pak budou stanovena bezpečnostní pravidla pro Correlation engine.

(22) SIEM - archivace logů - logy se primárně ukládají do databáze dohledového systému. Nad databází budou nastavena retenční pravidla, která po definovaném čase odkládají data na externí úložiště k archivaci. Archivní data budou chráněna proti neoprávněné manipulaci a také komprimována. Celý systém managementu logů bude bezúdržbový a tedy nevyžadující zásah administrátora.

(23) SIEM - analýza logů - systém normalizuje logy podle typu (např. login) a nad těmito normalizovanými daty pak provádí korelace. Zpracování je pak možné několika způsoby:

- (a) **Online sledování**-filtruje pohled na události podle zařízení, uživatele nebo dalších atributů
- (b) **Korelaci událostí**-normalizace, klasifikace a korelace událostí v čase z jednoho nebo více zdrojů. Pravidla pro korelaci popisují vztahy mezi souvisejícími událostmi v jednom systému nebo i napříč infrastrukturou. Zobrazení je možné přes interaktivní grafické rozhraní SIEM systému.
- (c) **Alerty**-na základě definovaných pravidel je možné vygenerovat alert, který může být odeslán emailem, syslogem, SNMP trapem nebo zobrazen interaktivně v grafickém rozhraní, případně zaslán do interního ticketovacího systému SEIM řešení.
- (d) **Akce**-za vygenerovaným alertem může stát uživatelsky definovaný skript, pro aktivní nápravu nalezeného stavu.

(24) Reporting - SIEM systém umožní pravidelně informovat o stavu infrastruktury generovanými reporty. Tyto mohou být již předdefinované podle standardů, jako jsou PCI-DSS, HIPAA, NERC-CIP, FISMA, nebo uživatelsky definované.

3.5. K3 - Elektronizace procesů

(1) Položka K3 - se skládá ze tří částí - skenovací linky, propojení eZAK a stávající spisové služby a rozklikávacího rozpočtu.

(2) MěÚ momentálně zpracovává dokumenty v analogové (fyzické) podobě pouze evidenčním způsobem, bez skenování a ukládání elektronického obrazu a příloh jednotlivých analogových dokumentů přicházejících na úřad. Evidenční údaje jsou zaznamenávány v informačním systému Elektronické spisové služby. Oběh analogových dokumentů probíhá fyzicky předáváním v papírové podobě mezi jednotlivými odbory a jejich pracovníky. Elektronické dokumenty typu datových zpráv jsou též zpracovávány v informačním systému Elektronické spisové služby, včetně uložení digitálních dokumentů a zásilek.

(3) Cílem skenovací linky je zavést digitalizaci potřebných dokumentů a jejich zpracování ve spisové službě. Pomocí skenovací linky bude dokument digitalizován a automatizovaně zaevidován do Elektronické spisové služby na základě jednoznačného identifikátoru. Veškeré další úkony budou prováděny již jen s elektronickým obrazem v rámci spisové služby. Tímto se

zefektivní a zrychlí oběh a další zpracování dokumentů vstupujících na úřad v analogové podobě. Zároveň se zvýší zabezpečení originálních dokumentů před případnou ztrátou. Elektronické dokumenty budou dostupné všem pověřeným pracovníkům v elektronické spisové službě z jakéhokoli místa. Výsledkem bude sjednocení práce s veškerými sledovanými dokumenty a jejich komplexní správa v rámci elektronické spisové služby.

(4) Pomocí skenovací linky bude možné zpracovávat všechny analogové dokumenty, nebo jen vybrané, např. s vyšší očekávanou zátěží na rozkopírovávání a předávání. Výhodou takového řešení je snížení objemu předávaných analogových dokumentů, zmenšení množství rozkopírovaných dokumentů, minimalizace rizika ztráty dokumentů, výrazně vyšší dohledatelnost dokumentů a možnost provázanosti na plnotextové prohledávání obsahu dokumentů.

(5) Součástí technického řešení je realizace rozhraní, které propojí současnou elektronickou spisovou službu MěÚ s elektronickým nástrojem na podporu zadávání veřejných zakázek eZAK.

(6) Rozklikávací rozpočet je nástroj, který umožňuje městům, aby projevily svůj vstřícný přístup a transparentní chování k občanům. Tento nástroj zobrazuje schválené informace z informačního systému města přímo na portál.

(7) Aplikace (Rozklikávací rozpočet) bude dostupná prostřednictvím webového prohlížeče.

(8) Informace o rozpočtu jsou řízeným způsobem publikovány z ekonomického systému (modul Rozpočet), přičemž se jedná o omezenou množinu údajů nezbytných pro prezentaci informací k rozpočtu. Požadováno je řešení, které oddělí „ostrá“ data od dat určených pro prezentaci z důvodů výkonu (dotazy na veřejný rozpočet nezatěžují provozní prostředí rozpočtu) a bezpečnosti.

(9) Aplikace (Rozklikávací rozpočet) umožní prostřednictvím konfigurace nastavit pro každou akci počet úrovní, které jsou zobrazovány. Zároveň je možné pro libovolnou akci nastavit příznak „anonymizovat“, který zajistí, že daná akce bude zobrazena (a v případě více anonymizovaných akcí na stejné úrovni nasčítána) jako akce „Ostatní“. Aplikace (Rozklikávací rozpočet) bude mít takové technické parametry, aby navazovala na systém GORDIC GINIS používaný zadavatelem.

3.6. Popis povinných parametrů dodávaného řešení

- (1) V dále uvedených tabulkách jsou uvedeny minimální povinné parametry dodávaného řešení.
- (2) Uchazeč musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena.

Tabulka č.1 : K1 - Virtualizační platforma - Server pro virtualizaci			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Minimálně 2x procesor osmijádrový architektury x86, L3 cache alespoň 20MB, každý procesor s výkonem nejméně 13000 podle http://www.cpubenchmark.net/		
2	Velikost RAM 256 GB: s rozšiřitelností až na 768 GB, minimálně 24 DIMM slotu		
3	Chipkill ochrana paměti, podpora online spare paměti a memory mirroringu		
4	Disková kapacita minimálně: 2x HDD 300 GB 10 krpm pro systém s možností rozšíření až na 16 ks HDD		
5	Podpora RAID 0,1,10,5,50,6,60, řadič s nejméně 1 GB Cache		
6	Minimálně 4x 1Gb ethernet port onboard s možností rozšíření o 2x 10Gb port, bez osazení PCIe slotu		
7	HBA card FC 8 Gb 2 porty		
8	Minimálně 3x PCIe 3.0 slot		
9	Redundantní hot-swap chlazení a napájení		
10	Predikce chyby na všech kritických komponentech - procesory, RAM, HDD, zdroje, ventilátory		
11	Diagnostický panel umožňující okamžitě určení vadné komponenty i při odpojení serveru od napájení		

Tabulka č.1 : K1 - Virtualizační platforma - Server pro virtualizaci

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
12	Montáž do racku, velikost max. 2U		
13	Management software		
14	<p>Součástí dodávky musí být také operační systém, který musí podporovat virtualizaci a obsahovat licence pro neomezený počet virtuálních serverů. Pokud operační systémy vyžadují klientské licence pro přístup uživatelů, je nutné dodat takové licence pro všechny uživatele na Městském úřadu Přelouč.</p> <p>Dále musí splňovat tyto vlastnosti:</p> <ul style="list-style-type: none"> • Adresářové služby kompatibilní s X.509 • Adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další • Autentizace protokoly Kerberos V5, NTLMv2, NTLM • Centrálně řízené politiky uživatelů a počítačů • Možnost funkcí DNS, DHCP, WINS • Možnost sdílení souborů a nastavování práv na objekty adresářové služby • Sdílení souborů pomocí protokolu CIFS • Distribuovaný souborový systém a delta replikace • Možnost sdílení tiskáren a nastavování práv na objekty adresářové služby • Možnost grafického uživatelského rozhraní v češtině 		
15	Záruka minimálně 60 měsíců s garantovaným dokončením opravy následující pracovní den		

Tabulka č.2 : K1 - Virtualizační platforma - Server pro zálohování			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Minimálně 1x procesor šestijádrový architektury x86, L3 cache alespoň 15MB, procesor s výkonem nejméně 8500 podle http://www.cpubenchmark.net/		
2	Velikost RAM 32 GB: s rozšiřitelností až na 512 GB, minimálně 16 DIMM slotu		
3	Chipkill ochrana paměti, podpora online spare paměti a memory mirroringu		
4	Disková kapacita minimálně: 2x HDD 300 GB 10 krpm pro systém, 6x HDD 3 TB 7,2 krpm 3,5" pro zálohy, s možností rozšíření pro minimálně dalších 6 ks 3,5" HDD		
5	Podpora RAID 0,1,10,5,50,6,60, řadič s nejméně 1 GB Cache		
6	Minimálně 4x 1Gb ethernet port onboard s možností rozšíření o 2x 10Gb port, bez osazení PCIe slotu		
7	HBA card FC 8 Gb 2x porty		
8	Minimálně 3x PCIe 3.0 slot		
9	Redundantní hot-swap chlazení a napájení		
10	Predikce chyby na všech kritických komponentech - procesory, RAM, HDD, zdroje, ventilátory		
11	Diagnostický panel umožňující okamžité určení vadné komponenty i při odpojení serveru od napájení		
12	Management software		
13	Montáž do racku, velikost max. 2U		
14	Operační systém musí podporovat virtualizaci a mít licence alespoň pro dva virtuální servery. Pokud operační systémy vyžadují klientské licence pro přístup uživatelů, je nutné dodat takové licence pro všechny uživatele na Městském úřadu Přelouč. Dále musí splňovat tyto vlastnosti:		

Tabulka č.2 : K1 - Virtualizační platforma - Server pro zálohování

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
	<ul style="list-style-type: none"> Adresářové služby kompatibilní s X.509 Adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další Autentizace protokoly Kerberos V5, NTLMv2, NTLM Centrálně řízené politiky uživatelů a počítačů Možnost funkcí DNS, DHCP, WINS Možnost sdílení souborů a nastavování práv na objekty adresářové služby Sdílení souborů pomocí protokolu CIFS Distribuovaný souborový systém a delta replikace Možnost sdílení tiskáren a nastavování práv na objekty adresářové služby Možnost grafického uživatelského rozhraní v češtině 		
15	Záruka minimálně 60 měsíců s garantovaným dokončením opravy následující pracovní den		

Tabulka č.3 : K1 - Virtualizační platforma - Server pro disaster recovery

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Minimálně 2x procesor dvanáctiádrový architektury x86, L3 cache alespoň 30MB, každý procesor s výkonem nejméně 17300 podle http://www.cpubenchmark.net/		
2	Velikost RAM 384 GB: s rozšiřitelností až na 768 GB, minimálně 24 DIMM slotu		
3	Chipkill ochrana paměti, podpora online spare paměti a memory mirroringu		

Tabulka č.3 : K1 - Virtualizační platforma - Server pro disaster recovery			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
4	Disková kapacita minimálně: 2x HDD 300 GB 10 krpm pro systém, 6 x HDD 900 GB 10 krpm pro data s možností rozšíření min o dalších 8 ks HDD		
5	Podpora RAID 0,1,10,5,50,6,60, řadič s nejméně 2 GB Cache		
6	Minimálně 4x 1Gb ethernet port onboard s možností rozšíření o 2x 10Gb port, bez osazení PCIe slotu		
7	Minimálně 3x PCIe 3.0 slot		
8	Redundantní hot-swap chlazení a napájení		
9	Predikce chyby na všech kritických komponentech - procesory, RAM, HDD, zdroje, ventilátory		
10	Diagnostický panel umožňující okamžité určení vadné komponenty i při odpojení serveru od napájení		
11	Management software		
12	Montáž do racku, velikost max. 2U		
13	<p>Operační systém musí podporovat virtualizaci a obsahovat licence pro neomezený počet virtuálních serverů. Pokud operační systémy vyžadují klientské licence pro přístup uživatelů, je nutné dodat takové licence pro všechny uživatele na Městském úřadu Přelouč.</p> <p>Dále musí splňovat tyto vlastnosti:</p> <ul style="list-style-type: none"> • Adresářové služby kompatibilní s X.509 • Adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další • Autentizace protokoly Kerberos V5, NTLMv2, NTLM • Centrálně řízené politiky uživatelů a počítačů • Možnost funkcí DNS, DHCP, WINS • Možnost sdílení souborů a nastavování práv na objekty adresářové služby 		

Projektový záměr „Konsolidace IT a nové služby TC ORP Přelouč“**TECHNICKÁ SPECIFIKACE****Tabulka č.3 : K1 - Virtualizační platforma - Server pro disaster recovery**

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
	<ul style="list-style-type: none">• Sdílení souborů pomocí protokolu CIFS• Distribuovaný souborový systém a delta replikace• Možnost sdílení tiskáren a nastavování práv na objekty adresářové služby Možnost grafického uživatelského rozhraní v češtině		
14	Součástí dodávky serveru pro disaster recovery musí být i licence virtualizační platformy, kterou aktuálně úřad využívá, tzn. licence nejméně pro 2 CPU.		
15	Záruka minimálně 60 měsíců s garantovaným dokončením opravy následující pracovní den		

Tabulka č.4 : K1 - Virtualizační platforma - Rozšíření RAM

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Pro nasazení jednotné virtualizační platformy v poslední dostupné verzi je nutné povýšit kapacity paměti RAM u stávajících serverů v Technologickém centru. Minimální hodnota je 2x256 GB RAM (po provedeném rozšíření - pro 2 stávající servery ve virtualizačním clusteru).		
2	Rozšíření musí být provedeno originálními moduly výrobce, tak aby nedošlo ke ztrátě záruky u těchto serverů - současně je nutné realizovat takovou formu rozšíření, aby bylo možné dále přidávat další paměťové moduly.		

Tabulka č.5 : K1 - Virtualizační platforma - Záložní zdroje UPS

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Min 6 minut chodu na baterie při plné zátěži 2700W (bez přídatných bat. modulů)		
2	Online s dvojitou konverzí		
3	Provedení Tower (samostatně stojící)		
4	Výměna baterií uživatelem a za provozu		
5	Možnost startu na baterie		
6	Automatický bypass		
7	Automatická stabilizace napětí		
8	Čistě sinusový výstup		
9	Možnost rozšíření až o 4 ks bateriových modulů		
10	Sériová a USB komunikace		
11	Web/SNMP komunikace		
12	Zátěž (VA/W): 3000/2700		
13	Tolerance vstupního napětí: až176-276V bez poklesu jmenovitého výkonu		
14	Kmitočet: Automatická volba 50/60Hz		
15	Výstupní napětí: 200/208/220/230/240V +/- 1%		
16	Přetížitelnost: až 110%		
17	Účinnost: min 94%		
18	Záruka minimálně na elektroniku 60 měsíců a na baterie 24 měsíců		

Projektový záměr „Konsolidace IT a nové služby TC ORP Přelouč“**TECHNICKÁ SPECIFIKACE****Tabulka č.6 : K1 - Virtualizační platforma - Zálohovací SW**

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Zálohování a replikace pomocí bitové kopie v sjednoceném, na úložišti nezávislém řešení		
2	Podpora stávajícího hypervizoru VMware vSphere		
3	Syntetické kompletní zálohy (eliminace potřeby periodických kompletních záloh)		
4	Zabudovaná deduplikace a komprese pro snížení kapacitních nároků na zálohy		
5	Bez nutnosti licencovat agentský SW na hostitelích nebo na virtuálních strojích		
6	Licence bez omezení počtu virtuálních strojů		
7	Obnovení na úrovni objektů pro jakoukoli aplikaci, na jakémkoli OS		
8	Obnovení souboru do Windows OS a do non-Windows OS pomocí jedno kliknutí myší		
9	Obnovování jednotlivých položek bez instalace agenta pro tyto stávající SW platformy nasazené v TC Města Přelouč: Microsoft Exchange (např. e-mailů a kontaktů), Microsoft SharePoint, Microsoft Active Directory (např. uživatelů a skupin), Microsoft SQL Server (např. tabulek a záznamů)		
10	Automatizované testování záloh v předem definovaných časech a formou startu zálohovaných virtuálních počítačů v izolované síti		
11	Start virtuálního stroje přímo ze souboru zálohy		

Tabulka č.7 : K2 - Bezpečnostní infrastruktura - Firewall

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
----------	-------	--	--

Tabulka č.7 : K2 - Bezpečnostní infrastruktura - Firewall			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Firewall musí v budoucnu umožnit vytvoření clusteru minimálně v Active/Passive módu. V clusteru musí mít společnou konfiguraci a tvořit tak jeden logický celek.		
2	Firewall musí umožnit rozdělení firewallu pomocí tzv. virtuálních kontextů (nebo také domén), minimálně je požadováno 10 kontextů.		
3	Firewall bude možné ve vybraných VLAN používat jako DNS a DHCP server. Musí být připraven i na funkce zajišťující proxy server min. pro http/https/ftp protokoly.		
4	Zařízení bude disponovat grafickým rozhraním pro kompletní správu firewallu a online monitorování aktuálního stavu.		
5	Počet metalických síťových rozhraní, RJ45, 10/100/1000 - min 16x		
6	Podpora linkové agregace (LACP/teaming) 802.3ad (v rámci clusteru přes oba boxy v HA)		
7	Podpora více WAN linek. Dual WAN (záloha nebo load balancing primárního připojení do internetu se sekundárním)		
8	Výkonnost FW nezávislá na velikosti paketu		
	Propustnost zařízení minimálně		
9	- celková 3 Gbps		
10	- IPS 1,6 Gbps		
11	- IPSec VPN 1,2 Gbps		
12	- SSL VPN 350 Mbps		
13	- Antivirus (Proxy/Flow - based) 600/1000 Mbps		
14	Bez licenčního omezení počtu chráněných uživatelů či stanic (IP adres), včetně IPS, web filtering, antivir.		

Tabulka č.7 : K2 - Bezpečnostní infrastruktura - Firewall

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
15	Zařízení charakteru UTM (unified threat management) – pravidla a politiky musí být možno vytvářet jednoduše a intuitivně v grafickém prostředí využíváním objektů aplikace, uživatel/skupina, počítač apod. bez nutnosti znalosti konkrétních IP adres, protokolů apod.		
16	Režim vysoké dostupnosti, L2, Active Active, Active Passive, VRRP, synchronizace stavové tabulky mezi nody v clusteru		
17	Podpora Vulnerability Managementu - aktivní skenování sítě a detekce zranitelnosti a problémů; možnost nastavit skenování v pravidelných časových intervalech		
18	Režim fungování L2 – transparentní režim, L3 – NAT/Router		
19	Podopora multicast, vytváření politiky pro multicast routování		
20	Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN,		
21	Podpora IPv6,		
22	Možnost nastavovat firewall politiku na základě geografických údajů		
23	Podpora tvorby Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru		
24	Funkce Load Balancing – možnost rozdělování zátěže směřující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offload		
25	Filtrační funkce:		
26	Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly)		
27	Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv.		

Tabulka č.7 : K2 - Bezpečnostní infrastruktura - Firewall			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
	Grayware (rootkit, malware, spyware, keylogger, atd)		
28	Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty		
29	IPS (Intrusion Prevention System) ochrana stanic a uživatelů, možnost využít jako sondu pro odhalení nežádoucích aktivit v rámci vnitřní sítě, automatická aktualizace signatur a možnost definice vlastních IPS signatur		
30	Web Filter – založený na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne		
31	Application Control – detekce, monitoring, povolení či zakázání alespoň 2000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu		
32	Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...)		
33	DoS Policy prevence proti základním útokům typu DoS, syn proxy		
34	LDAP, Active Directory, Radius, TACACS+, Ověřování na základě certifikátu		
35	Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – Token pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů		
36	Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření		
	Dynamické routování:		
37	· RIP, BGP, OSPF, IS-IS		
38	· Policy-based routing		
39	· Traffic Shaping, QoS s podporou DSCP markování a ToS		
40	Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu		

Projektový záměr „Konsolidace IT a nové služby TC ORP Přelouč“**TECHNICKÁ SPECIFIKACE****Tabulka č.7 : K2 - Bezpečnostní infrastruktura - Firewall**

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
41	· WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní proxy, WCCP		
42	Integrované logování a reporting		
43	Záruka na HWs výměnou následující pracovní den v délce minimálně 60 měsíců a to včetně aktualizací SW a signatur		

Tabulka č.8 : K2 - Bezpečnostní infrastruktura - Network Behaviour Analyser

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	HW forma velikosti max 1U		
2	Min. 4x 10/100/1000 monitoring porty		
3	Plnohodnotné ovládání pomocí WWW rozhraní		
4	Schopnost pojmout agregovaná data (disková kapacita alespoň 500GB)		
5	Tvorba uživatelských statistik a grafů		
6	Analýza trendů v síti		
7	Automaticky generované a zasílané reporty		
8	Detekce anomálií včetně analýzy trendů		

Tabulka č.8 : K2 - Bezpečnostní infrastruktura - Network Behaviour Analyser

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
9	Detekce bezpečnostních hrozeb		
10	Schopnost exportu dat do nadřazeného kolektoru		
	Systém pro sledování datových toků by měl umožňovat následující:		
11	Detailně monitorovat síťový provoz v reálném čase i umožnit získat přehled o síťové aktivitě v rámci specifikovaného časového období v minulosti.		
12	Získat přesné informace o veškeré síťové aktivitě – např. kdo komunikoval s kým, kdy, kolik se přeneslo dat, pomocí které služby atd.		
13	Předcházet výpadkům a zahlcením sítě (upozorňovat na různé anomálie síťového provozu).		
14	Automatická detekce odchylek od normálního stavu (získaný samoučením a definicí administrátorem) a bude schopen emailem automaticky upozorňovat administrátory.		
15	Zvýšit bezpečnost síťového provozu odhalením vnějších i vnitřních útoků.		
16	Sledovat aktivity uživatelů i aplikací (služeb), dohlížet nad využitím linku do Internetu. Až do úrovně 7. vrstvy ISO/OSI		

Tabulka č.9 : K2 - Bezpečnostní infrastruktura - Monitorovací SW

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Proaktivní forma monitoringu zařízení a služeb		
2	Přehled o toku v síti – on-line		
3	Statistiky a reporty – periodické zasílání reportů		

Tabulka č.9 : K2 - Bezpečnostní infrastruktura - Monitorovací SW

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
4	Trendy		
5	Aplikace pro systém IOS nebo Android pro mobilní přístup		
6	Grafické mapy topologie sítě		
7	On-line monitoring dostupnosti sítě a kritických aplikací		
8	Sledování využití pásma a QoS v LAN i WAN prostředí		
9	IP SLA Monitor		
10	Identifikaci nechtěných zařízení a nechtěného provozu		
11	Identifikaci problémů na síťové vrstvě komunikace – ztráty paketů apod.		
12	VoIP monitoring		
13	Možnost nasazení v distribuovaném prostředí		
14	Minimálně 2500 monitorovaných veličin		

Tabulka č.10 : K2 - Bezpečnostní infrastruktura - Systém SIEM

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Podporované protokoly pro sběr dat: <ul style="list-style-type: none"> TCP Syslog UDP Syslog 		

Tabulka č.10 : K2 - Bezpečnostní infrastruktura - Systém SIEM			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
	<ul style="list-style-type: none"> • SMNP • SDEE • OPSEC • WMI • SQL 		
2	Lokální agent, komunikace s SIEM systémem musí být šifrování a komprimovaná		
3	Normalizace – systém musí umožňovat definici vlastního parseru pro jednotlivé zdroje logů		
4	Archivace logů – na úložiště CIFS, NFS, NAS a SAN. Logy. Archivy musí být komprimované a odolné proti neoprávněné manipulaci ochranou kontrolním součtem.		
5	Zobrazení a filtrování online dat		
6	Korelace – na základě času, uživatele, skupiny, aplikace, serveru a sítě		
7	Reporting – šablony odpovídající požadavkům odpovídající požadavkům PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX a možnost uživatelských reportů		
8	Delegace oprávnění – Grafické administrační rozhraní musí umět delegovat práva na různé části systému podle sítí, serverů apod.		
9	Systém musí být provozovatelný ve virtuálním prostředí VMWARE		
10	Systém musí pro aktuální infrastrukturu držet aktivní záznamy minimálně 90 dní, archivované 12 měsíců.		
11	Systém musí mít garantovanou propustnost alespoň 1100 EPS		
12	Systém musí umožňovat rozšíření o distribuovaný sběr událostí z různých zdrojů, bezpečnostních zón		
13	Systém by měl být umožňovat rozšíření o příjem auditních informací o databázových transakcích bez použití agentů		

Projektový záměr „Konsolidace IT a nové služby TC ORP Přelouč“**TECHNICKÁ SPECIFIKACE****Tabulka č.10 : K2 - Bezpečnostní infrastruktura - Systém SIEM**

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
14	Systém by měl být umožňovat rozšíření o korelaci archivních událostí		

Tabulka č.11 : K3 - Elektronizace procesů - Skenovací linka

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Systém umožní nastavení parametrů skenování bez zásahu uživatele: Formát, Barva/ČB, Orientace, Rozlišení, Simplex/Duplex		
2	Systém umožní nastavení parametrů skenování bez zásahu uživatele: Cílové složky, cílové E-mailové adresy, databáze, IS systém, DMS		
3	Zónové OCR = Text / čárový kód načtený z konkrétního místa v dokumentu		
4	OCR podporuje rozpoznání 34 jazyků vč. češtiny		
5	Převod dokumentů = Word, Excel, Searchable PDF, PDF/A, OpenOffice		
6	Využívá Metadata = data získaná skenováním / zadaná uživatele		
7	IČO, čárový kód, číslo: faktury, smlouvy, zboží, datum		
8	Metadata použije pro: název souboru, složky, údaje v IS, DB, DMS		
9	OCR – Převod – Zabezpečení – Třídění – Uložení skenovaných, nebo existujících dokumentů		
10	Skenovací linka musí být řešena jako součást integrovaného IS města (GORDIC GINIS).		

Tabulka č.12 : K3 - Elektronizace procesů - Propojení eZAK a spisové služby

Projektový záměr „Konsolidace IT a nové služby TC ORP Přelouč“

TECHNICKÁ SPECIFIKACE

Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Autentizace – jeden společný účet E-ZAK		
2	Výběr spisové značky před založením spisu v systému elektronické spisové služby GORDIC GINIS		
3	Založení (prázdného) spisu - Spisová služba přidělí spisový znak <ul style="list-style-type: none"> • Založení nové VZ • Založení nového DNS • Založení nového předběžného oznámení, při pokračování zadávacího řízení možnost použít již Založený spis 		
4	Smazání spisu – spis se stornuje, nebo uzavře <ul style="list-style-type: none"> • Smazání VZ • Smazání DNS • Smazání předběžného oznámení 		
5	Úprava spisu – jedná se o změnu názvu <ul style="list-style-type: none"> • Úprava VZ • Úprava DNS • Úprava předběžného oznámení 		
6	Uzavření spisu <ul style="list-style-type: none"> • Zadání, nebo zrušení VZ • Ukončení předběžného oznámení • Ukončení DNS 		
7	Vložení písemnosti do spisu – spisová služba přidělí číslo jednací <ul style="list-style-type: none"> • Vložení nového dokumentu • Vytvoření nového formuláře pro VVZ • Registrace nové odchozí komunikace do spisové služby • Registrace nově příchozí komunikace do spisové služby • Registrace zadavatelem odesílaných odpovědí do spisové služby • Registrace zadavatelem přijatých odpovědí do spisové služby 		

Tabulka č.12 : K3 - Elektronizace procesů - Propojení eŽAK a spisové služby			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
	<ul style="list-style-type: none"> Registrace šablony „Protokol o průběhu elektronické aukce“ 		
8	Úprava písemnosti – jedná se o změnu názvu <ul style="list-style-type: none"> Úprava dokumentu Editace formuláře do VVZ 		
9	Uzavření písemností ve spisové službě <ul style="list-style-type: none"> Uveřejnění formuláře 		
10	Smazání písemnosti – při smazání, nebo nahrazení <ul style="list-style-type: none"> Smazání dokumentu Smazání formuláře VVZ Storno formuláře VVZ 		
11	Příchozí listinné písemnosti <ul style="list-style-type: none"> Přijdou na podatelnu a jsou zaregistrovány do spisové služby Do E-ZAKu je možné vložit oskenované listinné písemnosti jako interní nebo veřejné dokumenty k zadávacímu řízení, DNS či rámcové smlouvě – v tomto případě uživatel nezvolí registraci příkládaného dokumentu do spisové služby; číslo jednací je možné k takovému dokumentu doplnit ručně 		
12	Odchozí listinné písemnosti <ul style="list-style-type: none"> Odcházejí přes podatelnu, jsou zaregistrovány do spisové služby Do E-ZAKu je možné vložit oskenované listinné písemnosti jako interní nebo veřejné dokumenty k zadávacímu řízení, DNS či rámcové smlouvě – v tomto případě uživatel nezvolí registraci příkládaného dokumentu do spisové služby; číslo jednací je možné k takovému dokumentu doplnit ručně 		

Tabulka č.13 : K3 - Elektronizace procesů - Rozklikávací rozpočet			
Parametr	Popis	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
1	Plán - zobrazení aktuálního stavu rozpočtu ve srovnání s rozpočtem schváleným		
2	Skutečnost - aktuální stav čerpání/plnění rozpočtu ve srovnání s aktuálním upraveným rozpočtem		
3	Průběh - vývoj upraveného rozpočtu a plnění/čerpání rozpočtu v průběhu roku		
4	Zobrazovat rozpočet ve formě stromu, včetně (vybraných) detailních informací o akcích, opět s možností zobrazení plánu a skutečnosti		
5	Fulltextové vyhledávání		
6	Export do formátu PDF a XLS		
7	Aplikace musí být integrována s modulem Rozpočet ekonomického informačního systému města Přelouč a začleněna do webové prezentace města.		

Součástí dodávky veškerých výše uvedených zařízení je proškolení odpovědných zaměstnanců a předání dokumentace.

4. Implementační služby

4.1. Obecné požadavky

(1) Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Uchazeč je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobcí a dle tzv. nejlepších praktik, i v případě pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

- (a) Zpracování předimplementační analýzy,
- (b) Zpracování prováděcí dokumentace,
- (c) Zajištění projektového vedení realizace předmětu plnění,
- (d) Dodávku nabízeného hardware a software,
- (e) Kompletní implementaci řešení splňující povinné a nabízené hodnocené parametry technického řešení,
- (f) Provedení školení, předání odpovídající dokumentace k HW i SW, uživatelských příruček
- (g) Zajištění zkušebního provozu,
- (h) Provedení akceptačních testů,
- (i) Předání do ostrého provozu,

(2) Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

(3) Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standardních formátech (např. MS Office) používaných zadavatelem na datovém nosiči a 1x kopii v papírové formě.

4.2. Požadavky na předimplementační analýzu

(1) Před implementací řešení zpracuje Uchazeč předimplementační analýzu, minimálně pro následující oblasti

- (a) Současný stav virtualizační platformy, bezpečnostní infrastruktury a LAN,
- (b) Způsob začlenění nabízených komodit do prostředí TC,
- (c) Konfigurace dodávaného ve vztahu k plánovanému využití,
- (d) Rekonfigurace stávajících systémů,
- (e) Dopady implementace na dostupnost stávajících služeb,
- (f) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon)
- (g) Požadované součinnosti Zadavatele.

(2) Výstupem předimplementační analýzy bude písemná zpráva, která podléhá schválení Zadavatelem.

4.3. Požadavky na zpracování prováděcí dokumentace

(1) Uchazeč před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity

potřebné pro řádné zajištění implementace předmětu plnění do stávajícího prostředí technologického centra.

- (2) Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem.
- (3) Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
 - (a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,
 - (b) Způsob zajištění potřebného HW a SW,
 - (c) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem
 - (d) Detailní návrh a popis postupu implementace předmětu plnění,
 - (e) Detailní harmonogram projektu včetně uvedení kritických milníků,
 - (f) Vazby na stávající systémy a jejich konfigurace,
 - (g) Návrh akceptačních kritérií a akceptačních testů,
 - (h) Detailní popis navrhovaných školení.

4.4. Požadavky na zajištění projektového vedení

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

Aktivita	Začátek	Termín
Podpis smlouvy	D	D
Zahájení projektu – úvodní projektová schůzka	D	D+7
Předimplementační analýza - zpracování	D+7	D+17
Předimplementační analýza – připomínkové řízení, schválení	D+17	D+20
Prováděcí dokumentace – zpracování	D+20	D+30
Prováděcí dokumentace – připomínkové řízení, schválení	D+30	D+32
Realizace předmětu plnění	D+32	D+102
Školení administrátorů	D+102	D+110
Zkušební provoz	D+110	D+125
Akceptační testy	D+125	D+132
Zahájení ostrého provozu	D+132	-

- (4) Uchazeč může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
- (5) Maximální lhůty trvání nesmí uchazeč při tvorbě detailního harmonogramu prodloužit.
- (6) Uchazeč uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy o dílo.

(7) Uchazeč uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.

(8) Nejpozdější termín pro zahájení ostrého provozu a ukončení projektu je **30.6.2015**.

4.5. Požadavky na školení

(1) Uchazeč zajistí školení pracovníků Zadavatele – administrátorů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

(2) Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.– školení bude zakončeno písemnou zkouškou potvrzující požadovanou úroveň znalostí pracovníků a úspěšným pracovníkům bude vystaveno osvědčení o školení.

(3) Minimální rozsah školení je 24 hodin.

(4) Školení bude probíhat v sídle Zadavatele.

(5) Předpokládá se účast max. 5 administrátorů.

(6) Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

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

(1) Uchazeč navrhne způsob a provedení akceptačních testů.

(2) O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol

(3) Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.

5. Záruky a servisní podmínky

(1) Zadavatel požaduje standardní záruku na veškeré dodané technologie v délce trvání minimálně 60 měsíců (není-li u konkrétní technologie uvedeno jinak) od okamžiku předání do provozu. Případné náklady na zajištění standardní záruky musí uchazeč zahrnout do pořizovací hodnoty položky, ke které se vztahují.

(2) Veškeré záruční opravy po dobu záruky budou bez dalších nákladů pro provozovatele.

(3) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(4) V případě že dodané zařízení/ software/ systém obsahuje software, budou záruky obsahovat i tzv. software maintenance, tzn. aktualizace software vydávané výrobcem zařízení/software/ systému. Náklady na maintenance uchazeč uvede v kalkulaci nabídkové ceny do položky "SW maintenance".

(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.

(6) Uchazeč ve své nabídce výslovně uvede všechny podmínky nabízených záruk.

(7) Uchazeč ve své nabídce výslovně uvede požadavky předmětu plnění na rozsah a frekvenci pozáručního servisu nutného pro udržení dodaného zařízení ve spolehlivém a provozuschopném stavu.

(8) Dále uchazeč ve své nabídce výslovně uvede **předpokládanou životnost zařízení** při běžném způsobu použití zařízení v obdobných podmínkách.

6. Podpora zajištění provozu

(1) Předmětem plnění této veřejné zakázky je také **podpora zajištění provozu** tzn. zajištění servisních služeb v režimu, který zajišťuje optimální poměr mezi náklady na zajištění provozu a pokrytím kritických komponent.

(2) Služby podpory zajištění provozu bude uchazeč zajišťovat po dobu udržitelnosti projektu, tj. 60 měsíců od předání díla jako celku do ostrého provozu.

(3) Pokud dojde k závadě na zařízení, na které se vztahuje záruka, pak je uchazeč povinen zajistit náhradní prvek nebo ekvivalentní funkční řešení a to do doby než vadné zařízení v rámci záruky nahradí funkčním zařízením a to v následujících termínech:

Zařízení	Termín
K1: Server pro virtualizaci	Oprava zařízení musí být provedena do příštího pracovního dne.
K1: Server pro zálohování	Oprava zařízení musí být provedena do příštího pracovního dne.
K1: Server pro disaster recovery	Oprava zařízení musí být provedena do příštího pracovního dne.

(4) Pro hlášení veškerých servisních požadavků zajistí Uchazeč Zhotoviteli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Provozní doba helpdeskového systému musí být minimálně 8-17 hod. v pracovních dnech.

(5) Kromě přístupu do helpdeskového systému uchazeč zajistí servisní telefonní číslo a e-mailovou adresu, včetně uvedení kontaktních osob se zpětnou vazbou zalogování požadavku zadavatele do 4 pracovních hodin s totožnou provozní dobou 8-17 v pracovních dnech.

(6) Detailní popis helpdeskového systému musí být součástí nabídky.

(7) Uchazeč zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

(8) Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejich provádění.

(9) Veškeré činnosti budou prováděny po dohodě se Zadavatelem takovým způsobem a v takových časech, aby neomezili provoz zadavatele.

(10) O veškerých činnostech bude prováděn písemný záznam, který bude předložen Zadavateli.

Veškeré náklady na zajištění požadovaných služeb podpory provozu zahrne uchazeč ve své nabídce a uvede v kalkulaci nabídkové ceny.