[redacted]

Smlouva o poskytnutí programového vybavení DATACENTRUM Klient-Aplikační server-SQL server (dále jen DC2) a jeho servisu

číslo smlouvy poskytovatele: 5 / 2016
číslo zakázky: 439

č. CES: 2017/0066

DATACENTRUM systems & consulting, a. s.
Se sídlem Písnická 30/13, 142 00 Praha 4 - Kamýk
Zastoupená Ing. Petrem Luckým, členem představenstva společnosti
IČ: 25631721 DIČ: CZ25631721
Bank. spojení: KB Praha 4, expozitura Chodov číslo účtu 19-8779880297/0100

(dále jen „poskytovatel")

- na straně jedné -

a

Městská část Praha 1
Se sídlem Vodičkova 18, 115 68 Praha 1
Zastoupená Ing.Miloslavem Urbanem, vedoucím odboru informatiky
IČ: 00063410 DIČ: CZ00063410
Bank. spojení: ČS a.s., číslo účtu 27-2000727399/0800

(dále jen „zákazník")

- na straně druhé -

(společně pak „smluvní strany")

Smluvní strany se níže uvedeného dne, měsíce a roku, v souladu s ustanoveními § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, s přihlédnutím k ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, dohodly na základě vzájemného konsenzu o všech dále uvedených ustanoveních tak, jak stanoví tato

Smlouva o poskytnutí programového vybavení DATACENTRUM Klient-Aplikační server-SQL server a jeho servisu

K

1. Úvodní ustanovení

1.1. Poskytovatel prohlašuje, že je právnickou osobou řádně založenou a zapsanou podle českého právního řádu v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, číslo vložky 5092.

1.2. Poskytovatel prohlašuje, že disponuje materiálními, technickými a personálními prostředky a vlastní všechny potřebné registrace k řádnému plnění této smlouvy. Zákazník bere na vědomí, že poskytovatel může poskytnout plnění podle této smlouvy i přímo prostřednictvím svých dceřiných společností.

1.3. Zákazník prohlašuje, že je oprávněn tuto smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.4. Nedílnou součást této smlouvy tvoří tyto přílohy:

1.4.1. Příloha č. 1, která obsahuje rozsah programového vybavení DC2.

1.4.2. Příloha č. 2, která specifikuje poskytování servisních služeb k programovému vybavení DC2 ze strany poskytovatele zákazníkovi a tomu odpovídající závazek zákazníka zaplatit poskytovateli dohodnutou cenu uvedenou v Příloze č. 2.

2. Předmět smlouvy

2.1. Zákazník tímto zadává u poskytovatele a poskytovatel souhlasí s tím, že poskytne zákazníkovi následující plnění:

2.1.1. Poskytovatel poskytne zákazníkovi programové vybavení DC2 specifikované v Příloze č. 1.

2.1.2. Poskytovatel poskytne zákazníkovi v souladu s § 46 a násl. autorského zákona nevýlučné nepřenosné právo užití programového vybavení DC2 v rozsahu specifikovaném v Příloze č. 1.

2.1.3. Poskytovatel poskytne zákazníkovi servisní služby k programovému vybavení v rozsahu specifikovaném v Příloze č. 2.

2.1.4. Poskytovatel poskytne potřebnou součinnost při propojování programového vybavení DC2 s jinými částmi informačního systému zákazníka (např. v případě spojení s docházkovým systémem apod.).

2.2. Zákazník se zavazuje zaplatit poskytovateli za plnění poskytnuté podle této smlouvy ceny uvedené v Příloze č. 2.

3. Cena a platební podmínky

3.1. Veškeré ceny za programové vybavení DC2 (podle této smlouvy) jsou stanoveny dohodou smluvních stran a uvedeny v Příloze č. 2 této smlouvy. Výše cen je stanovena ke dni uzavření smlouvy a jakákoliv změna je možná pouze písemnou dohodou smluvních stran, není-li výslovně stanoveno jinak. Veškerě ceny podle této smlouvy jsou uvedeny v českých korunách.

3.2. Ke všem cenám podle této smlouvy bude připočtena daň z přidané hodnoty v zákonné výši.

3.3. Ceny dle této smlouvy jsou splatné na základě faktur vystavených poskytovatelem – daňových dokladů, jejichž splatnost činí třicet (30) dnů ode dne jejich vystavení, není-li dohodnuto jinak. Fakturace servisních služeb specifikovaných v Příloze č. 2 bude prováděna měsíčně, vždy k poslednímu dni v měsíci. Na faktuře bude jako číslo objednávky uvedeno č. smlouvy CES.

3.4. V případě nedodržení termínů dle Přílohy č. 2 je poskytovatel povinen uhradit zákazníkovi smluvní pokutu ve výši 5% z ceny poplatků za čtvrtletí za servis k programovému vybavení dle Přílohy č. 2 za každý den prodlení, maximálně však do výše měsíčního poplatku.

3.5. Bude-li zákazník v prodlení s úhradou faktury, může poskytovatel účtovat úrok z prodlení ve výši 5% z fakturované částky dle této smlouvy za každý den prodlení, maximálně však do výše měsíčního poplatku.

3.6. Zaplacením smluvní pokuty a úroku z prodlení není dotčeno právo oprávněné strany na náhradu škody vzniklé v příčinné souvislosti s porušením smluvní povinnosti, za jejíž nedodržení jsou smluvní pokuta nebo úrok z prodlení vymáhány a účtovány.

4. Náhrada škody

4.1. Každá ze smluvních stran nese odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy. Obě strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

4.2. Žádná ze smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé strany.

4.3. Poskytovatel neodpovídá za škodu způsobenou neoprávněnými zásahy do programového vybavení DC2 ze strany zákazníka nebo třetích osob, popř. jeho užíváním jinak než v souladu s touto smlouvou.

5. Ochrana informací

5.1. Poskytovatel se zavazuje, že informace, které získá o zákazníkovi při provádění činností podle této smlouvy, a které nejsou veřejně dostupné, bude považovat za důvěrné (dále jen „důvěrné informace").

5.2. Poskytovatel se zavazuje, že bez předchozího písemného souhlasu zákazníka nezveřejní důvěrné informace, ani je neposkytne či jinak nezpřístupní osobám jiným, než jsou osoby zaměstnané nebo najaté poskytovatelem pro realizaci smlouvy. Poskytování důvěrných informací těmto osobám musí být provedeno pouze v míře potřebné pro realizaci této smlouvy a tyto osoby musí být poučeny o povinnosti ochrany důvěrných informací.

5.3. Poskytovatel prohlašuje, že programové vybavení DC2 má charakter zaměstnaneckého díla ve smyslu § 58, odst. 1 a 7 autorského zákona a bylo vytvořeno zaměstnanci společnosti v rámci plnění povinností vyplývajících z pracovního poměru, popř. bylo vytvořeno na objednávku. Poskytovatel je oprávněn svým jménem a na svůj účet vykovávat majetková autorská práva k dílu.

5.4. Zákazník se zavazuje zabezpečit předané programové vybavení před neoprávněným přístupem nebo manipulací, které mohou mít za následek jeho užití v jiné organizaci bez souhlasu poskytovatele, popřípadě jiný zásah do autorských práv poskytovatele. Bez souhlasu poskytovatele není zákazník oprávněn jakýmkoliv způsobem zasahovat do programového vybavení DC2, provádět jeho změny nebo úpravy ani jej užívat jinak než v souladu s touto smlouvou.

6. Trvání a ukončení smlouvy

6.1. Tato smlouva nabývá platnosti a účinnosti od 1. 1. 2017.

6.2. Právo užití programového vybavení DC2 poskytuje poskytovatel zákazníkovi na dobu neurčitou.

6.3. Poskytování služeb údržby k programovému vybavení DC2 je sjednáno na dobu do **31. 12. 2017**.

6.4. Zákazník může vypovědět tuto smlouvu z důvodu převodu na poskytovatele outsourcingu, a to písemnou výpovědí s měsíční výpovědní lhůtou. Výpovědní lhůta začíná běžet 1. kalendářní den měsíce následujícího po doručení výpovědi druhé smluvní straně.

6.5. Poskytovatel může vypovědět tuto smlouvu kdykoliv po jejím podpisu bez udání důvodu, a to písemnou výpovědí s šestiměsíční výpovědní lhůtou. Výpovědní lhůta začíná běžet 1. kalendářní den měsíce následujícího po doručení výpovědi druhé smluvní straně.

6.6. Zákazník je oprávněn odstoupit od této smlouvy s okamžitou platností pokud:

6.6.1. práva třetích osob přes opatření učiněná poskytovatelem a přes součinnost zákazníka řádně poskytnutou k těmto opatřením znemožňují zákazníkovi užití programového vybavení DC2,

6.6.2. je poskytovatel v prodlení s předáváním prací ve stanovených termínech nebo zapracováním změn předpisů déle než 30 dnů.

6.7. Poskytovatel je oprávněn odstoupit od smlouvy s okamžitou platností pokud:

6.7.1. je zákazník v prodlení s úhradou ceny déle než 90 dní,

6.7.2. zákazník poruší autorské právo ve vztahu k předmětu této smlouvy.

6.8. Odstoupení nabývá platnosti dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

7. Jiná ujednání

7.1. Každá ze smluvních stran jmenuje kontaktní osoby, které zastupují zájmy příslušné smluvní strany, přijímají požadovaná rozhodnutí nebo zajišťují bezodkladné přijetí příslušných opatření a starají se o dobrou spolupráci mezi smluvními stranami. Kontaktní osoby a kontaktní adresy a telefonní/faxová čísla jsou uvedeny v Příloze č. 2.

7.2. Každé oznámení poskytnuté jednou stranou druhé straně podle této smlouvy bude druhé straně zasláno písemně, popřípadě elektronickou poštou nebo faxem a následně písemně potvrzeno odesilatelem oznámení. Oznámení je účinné v případě jeho písemné formy jeho doručením, v případě elektronické či faxové formy doručením písemného potvrzení.

7.3. Smluvní strany se dohodly, že veškerá komunikace mezi kontaktními osobami poskytovatele a zákazníka bude vedena v českém jazyce. Rovněž veškeré projektové a zadávací dokumenty budou koncipovány v českém jazyce.

7.4. Poskytovatel je povinen v průběhu poskytování služby zajistit bezpečnost informací Zákazníka, s kterými přichází do styku a/nebo se seznámí při poskytování služby. Minimální požadavky Zákazníka na úroveň bezpečnosti informací ze strany Poskytovatele jsou stanoveny v příloze č. 1 této smlouvy – „Etalon minimální bezpečnosti pro smluvní partnery"

8. Závěrečná ustanovení

8.1. Veškeré změny a dodatky této smlouvy lze provést pouze písemnými číslovanými dodatky podepsanými oběma smluvními stranami, není-li ve smlouvě uvedeno jinak.

8.2. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla uvedena v centrální evidenci smluv vedené Městskou částí Praha 1, která může být veřejně přístupná, a která obsahuje údaje o smluvních stranách, předmětu smlouvy, číselné označení této smlouvy a datum jejího podpisu.

8.3. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, přičemž ke každému stejnopisu jsou pevně připojeny shora specifikované přílohy č. 1 a 2. Každá smluvní strana obdrží jeden originál této smlouvy.

8.4. Tato smlouva nahrazuje Smlouvu o poskytnutí programového vybavení DATACENTRUM 2 a jeho servisu č. 115/2005, uzavřenou dne 14. 12. 2005, a jejích dodatků.

8.5. Poskytovatel bere na vědomí, že informace obsažené v této smlouvě podléhají povinnosti zákazníka poskytnout je třetím osobám na žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

8.6. Podpisem této smlouvy zákazník v souladu s ustanovením § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, potvrzuje, že byly splněny všechny podmínky tohoto zákona k tomu, aby tato smlouva platně vznikla.

8.7. Tato smlouva obsahuje přílohu č.1 - „Etalon minimální bezpečnosti pro smluvní partnery".

V Praze dne: 25. 1. 2017

[redacted]

V Praze dne: 23. 1. 2017

[redacted]

Příloha č. 1

Programové vybavení DC2 – MZDY umožňuje evidenci všech údajů potřebných pro zpracování mzdové agendy a jejich zpracování v souladu s platnými mzdovými předpisy pro územní samosprávný celky včetně vytvoření potřebných výstupů (např. výplatní páska, potvrzení pro zaměstnance, výstupy pro orgány státní správy – Česká správa sociálního zabezpečení, Finanční úřad, Zdravotní pojišťovny).

Programové vybavení DC2 – PERSONALISTIKA umožňuje evidenci všech údajů potřebných pro zpracování personální agendy a jejich zpracování v souladu s platnými předpisy pro územní samosprávný celky včetně vytvoření potřebných výstupů (např. formuláře pro předstihové řízení, zápočtový list, přehled odchodů do důchodu, hlášení pro zdravotní pro zdravotní pojišťovny, podklady pro docházku, oznámení občanů se změněnou pracovní schopností, statistické šetření ISCP).

Programové vybavení DATACENTRUM IDESYS – Docházka je určen k evidenci a vyhodnocení pracovní doby pomocí identifikačních karet a výpočetní techniky. Zabraňuje falšování údajů, zjednodušuje a zpřesňuje zpracování docházky pracovníků. Systém slouží nejen ke zpracování informací o příchodech, odchodech, případně přerušení pracovní doby, ale na jejich základě i vytváří podklady pro mzdový systém. Výstupy systému umožňují provádět kvalifikovaná rozhodnutí podle přesných a obsáhlých informací.

Specifikace programového vybavení:

a) Uživatelská práva – Licence:

DATACENTRUM 2 - Mzdy (**do 500 OSČ**)
DATACENTRUM 2 - Personalistika (**do 500 OSČ**)
DC2 klient (**pro max. 6 současně pracujících klientů**)
Počet zpracovávaných organizací (**1 organizace**)
DOCH32 – Docházka (**do 600 OSČ**)

b) Uživatelská práva – Nadstavbové moduly:

ONZ – Přihlášky a odhlášky na ČSSZ (formát xml)
ELDP – Evidenční listy důchodového pojištění (formát xml)
PVPOJ – Přehled o výši pojistného a vyplacených dávkách
NEMPRI – Příloha k žádosti o dávku nemocenského pojištění
Export převodních příkazů do banky (1 banka)
Generátor sestav
Stravenky – Nárok na stravné
Účetní doklad a jeho přenos do účetnictví Gordic
EPO2 – II. pilíř důchodového spoření
Import dat z docházky IDESYS
Obecný import
Výpočet Exekuce
Insolvence
Organigram
Výběr zaměstnanců – uchazeči
Plánování absencí
Výplatní pásky – náhled v docházce
Poštovní klient
Napojení na EOS
Převodní příkazy do banky (ČS,Bussines)

Příloha č. 2

Specifikace servisu k programovému vybavení:

1. **Servis k programovému vybavení zahrnuje:**

a) ***UPGRADE*** *(základní verze pro běžný rok)* a ***UPDATE*** programového vybavení:
- v návaznosti na změny příslušných právních předpisů tyto neprodleně promítnout do programového vybavení; změny budou do programového vybavení zapracovány od okamžiku jejich účinnosti,
- zajišťovat další rozvoj programového vybavení.
- udržovat funkce datového propojení na systém MODIS

b) ***Zákaznickou podporu k programovému vybavení:***

- průběžná distribuce nových verzi (UPGRADE i UPDATE) nové verze jsou zasílány na kontaktní adresu zákazníka na CD nosičích nebo jsou stahovány zákazníkem z webových stránek poskytovatele; za správnou instalaci nové verze odpovídá zákazník

- zasílání dodatků k uživatelské dokumentaci
  průběžné zasílání vždy s novou verzí programového vybavení

- poskytování informačního servisu prostřednictvím uživatelského bulletinu

- poskytování servisu pomocí help-deskového systému, e-mailu či telefonicky prostřednictvím pracovníka DTC

- doba poskytované podpory v pracovní dny od 8.00 do 16.30

- reakce poskytovatele v případě havárie programového vybavení DC u zákazníka do 24hodin od nahlášení havárie. Nástup na opravu do 48hodin od nahlášení havárie.

2. **Kontaktní osoby:**

a) Kontaktní osobou za stranu zákazníka pro oblast servisu programového vybavení je/jsou:

Jméno a Příjmení	Daniela Kladívková
Telefon	[redacted] Fax
E-mail	
Adresa instalace	Vodičkova 18, 115 68 Praha 1

b) Spojení na poskytovatele pro účely konzultací:

Telefon	
E-mail	[redacted]
Adresa	Písnická 30/13, 142 00 Praha 4

3. **Ceny:**

Ceny za servis programového vybavení DC2

a) Poskytování UPGRADE a UPDATE verzí s garancí legislativních změn	6.976,- Kč/ měsíčně
b) Zákaznická podpora - standardní:	3.489,- Kč/ měsíčně
CELKEM bez DPH:	**10.465,- Kč/ měsíčně**
DPH:	**2.197,70,- Kč/ měsíčně**
CELKEM s DPH:	**12.662,70,- Kč/ měsíčně**

Cena stanovená dle bodu č. 3 Přílohy č. 2 může být po dohodě obou smluvních stran písemným dodatkem zvýšena (snížena) dle úpravy rozsahu poskytovaných služeb.
Cena stanovená dle bodu 3 a), b) Přílohy č. 2 může být po dohodě obou smluvních stran písemným dodatkem zvýšena na základě:

- rozšíření programového vybavení o další adresáře (např. o další právní subjekty),
- instalace atypické verze programového vybavení,
- rozšíření programového vybavení o další počítačové stanice, o návazné moduly a účelové programy,
- funkčního zhodnocení programového vybavení.

Fakturace dle bodu č. 3 Přílohy č. 2 bude zahájena po podpisu smlouvy.

4. Jiná ujednání

Zákazník souhlasí s tím, aby poskytovatel po dobu platnosti této smlouvy uváděl ve svých propagačních materiálech, výročních zprávách, přihláškách do tendrů a výběrových řízení a do dalších textů jméno zákazníka jako referenčního klienta, včetně jména kontaktní osoby zákazníka a jejího telefonního a e-mailového spojení. Bez předchozího písemného svolení zákazníka nesmí poskytovatel dle tohoto bodu použít další informace o zákaznícovi (když by byly veřejně dostupné) jako např:

- počet zpracovávaných osobních čísel
- které moduly zákazník využívá
- údaje o technickém vybavení zákazníka
- cenové informace
- informace o organizační struktuře zákazníka
- jména dalších osob zákazníka
- a další ...

1 Účel a cíle

Etalon minimální bezpečnosti informací pro dodavatele MČ Praha 1 tvoří soubor pravidel a postupů, které stanovují požadovanou minimální úroveň bezpečnosti informací.

Dodržování pravidel uvedených v dokumentu je povinné pro všechny partnery spolupracující na smluvní bázi s MČ Praha 1, pro všechny jejich zaměstnance či osoby spolupracující se smluvními partnery.

Používané i nově zaváděné informační systémy v rámci MČ Praha 1 musí být upraveny, vyvíjeny nebo vybírány tak, aby splňovaly zásady bezpečnosti informací v souladu s tímto dokumentem a se základním dokumentem pro bezpečnost informací MČ Praha 1, tj. Politikou bezpečnosti informací MČ Praha 1.

Cílem etalonu minimální bezpečnosti informací pro smluvní partnery obecně je:

a) Specifikovat základní pravidla a požadavky bezpečnosti informací MČ Praha 1 pro smluvní partnery;
b) Předcházet porušování platných právních předpisů ČR;
c) Zamezit, příp. minimalizovat možnost finanční, majetkové a nemajetkové újmy MČ Praha 1;
d) Zabránit neautorizovanému přístupu k informacím MČ Praha 1;
e) Umožnit řízení bezpečnosti informací MČ Praha 1 ve vztahu s dodavateli;
f) Zajistit dostupnost informací pro oprávněné uživatele a procesy;
g) Zabránit neautorizované modifikaci nebo zneužití dat a informací;
h) Definovat základní pravidla bezpečnosti v oblasti vývoje a dodávek prostřední IT;
i) Umožnit monitorování a vyhodnocování stavu bezpečnosti.

Výklad použitých zkratek:

BP	bezpečnostní politika informačního systému veřejné správy
ICT	informační a komunikační technologie (Information and Communication Technology)
IS	informační systém (obecně)
ISVS	informační systém veřejné správy (viz § 3 odst. 1 zák. č. 365/2000 Sb.)
MČ Praha1	Městská část Praha 1
ÚMČ Praha 1	Úřad městské části Praha 1
SŘBI / ISMS	systém řízení bezpečnosti informací, ustanovený na základě požadavků IEC 27001
MBI	Manažer bezpečnosti informací ÚMČ Praha 1
Zákon o ISVS	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění
HelpDesk	primární, centrální bod pro kontakt se všemi uživateli IS/ICT a informačních služeb za účelem hlášení chyb, nedostatků i námětů pro rozvoj řešení
NTB	notebook

2 Bezpečnost informací

Bezpečností informací se rozumí zajištění třech hlavních aspektů – důvěrnosti, dostupnosti a integrity informací v duchu požadavků a doporučení norem řady ISO/IEC 27000.
K zajištění výše uvedených aspektů bezpečnosti informací musí dodavatel použít a řídit vhodná bezpečnostní opatření, zahrnující jak technické, tak organizační opatření, zohledňující rozsah hrozeb související s předmětem dodávky.

3 Obecné povinnosti

Mezi odpovědnosti smluvních partnerů patří zejména:

a) Dodržování platných právních předpisů ČR k zajištění bezpečnosti informací;
b) Využívání informačních systémů MČ Praha 1 a jejich komponent tak, jak vyplývá z provozní a bezpečnostní dokumentace těchto systémů;
c) Používání informačních aktiv a ostatních aktiv MČ Praha 1 pouze v souladu s určeným rozsahem přístupových oprávnění a pouze ke schváleným účelům;
d) Zajištění ochrany autentizačních údajů (login, heslo, identifikační předmět) k informačním systémům a zařízením MČ Praha 1, které mu byly svěřené, příp. těch., ke kterým má přístup při naplňování smluvního vztahu;
e) Odpovědnost za každý přístup k informačním aktivům a dalším aktivům, provedený prostřednictvím jejich autentizačních údajů;
f) Respektování a dodržování všech bezpečnostních opatření, pravidel a procedur, stanovených vlastníkem informací, tj. MČ Praha 1;
g) Odpovědnost za dostatečné proškolení svých zaměstnanců a pracovníků svých subdodavatelů v oblasti zajištění bezpečnosti informací MČ Praha 1;
h) Vyhodnocování rizik vůči bezpečnosti informací MČ Praha 1 v rozsahu smluvního vztahu a samostatně přijímání potřebných opatření k jejich ošetření;
i) V případě vzniku bezpečnostního incidentu přijmutí nezbytných opatření k eliminaci dopadů tohoto incidentu a neprodlené informování MČ Praha 1.

3.1 Poskytování informací třetím stranám

a) Smluvní partneři jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při výkonu své činnosti na základě uzavřené smlouvy s MČ Praha 1.
b) Každé případné veřejné použití neveřejných informací MČ Praha 1 musí být schváleno vedoucím Odboru informatiky MČ Praha 1.

4 Bezpečnost HW, SW a komunikací

Smluvní partneři MČ Praha 1 musí chránit aktiva MČ Praha 1, která používají při své práci nebo naplňování smluvního vztahu a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití a/nebo odcizení.

4.1 HW (pracovní stanice, ...)

Při práci na koncových pracovištích musí být splněny nejméně následující bezpečnostní pravidla:

a) Použití koncového zařízení (počítače) musí být umožněno pouze oprávněné osobě;
b) Je zakázáno připojovat soukromé počítače do vnitřní sítě MČ Praha 1 bez vědomí oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;
c) Koncová zařízení (pracovní stanice, NTB) nesmí být ponechána bez dozoru zapnuté a s přihlášeným uživatelem (k aplikaci, IS); za minimální opatření se považuje „uzamčení" pracovní stanice;
d) Počítače smluvního partnera, které mají být připojeny do vnitřní sítě ÚMČ Praha 1, musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databází;
e) Smluvní partner je povinen chránit vybavení ÚMČ Praha 1, udržovat bezpečné pracovní prostředí; v blízkosti prostředků informačních technologií je zakázáno jíst, pít a kouřit;
f) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému.

4.2 Využívání prostředků a internetu

a) Systémy MČ Praha 1, vztahující se k počítačové síti, internetu, intranetu, počítačové vybavení, program, operačních systémů a médií pro ukládání dat, ..., jsou ve vlastnictví MČ Praha 1. Tyto systémy mohou být používány pouze pro pracovní účely tak, aby to sloužilo zájmům MČ Praha 1;
b) Smluvní partneři mají povoleno používání internetového připojení do a z vnitřní sítě MČ Praha 1 pouze za účelem plnění pracovních záležitostí v rozsahu smluvního vztahu. Způsob připojení a autentizace musí být předem dohodnuta s Odborem informatiky ÚMČ Praha 1;
c) Obecně platí povinnost, že smluvní partner předem oznamuje datum a čas přihlášení k vnitřnímu prostředí a následně ukončení práce ve vnitřním prostředí systémů MČ Praha 1.

5 Bezpečnost IS / IT systémů

U vyvíjených nebo dodávaných informačních systémů, jejich HW/SW komponent, musí být zajištěna níže uvedená pravidla:

5.1 Aplikace

a) Aplikace musí být vytvářeny tak, aby byl vždy vyžadován autorizovaný přístup uživatelů (identifikační a autentizační údaje); a musí být zaznamenávána činnost uživatele v aplikaci / systému;
b) Uživatel aplikace musí být nucen si své přístupové heslo pravidelně měnit;
c) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po několika neúspěšných pokusech o přihlášení musí být další zadávání hesla dočasně omezeno nebo činnost ukončena;
d) Pokud je při přihlašování do aplikace některá část přihlašovacích údajů chybná, nesmí být přihlašovateli poskytnuta informace, kde je chyba v přihlašovacích údajích;
e) V případě, že je povolen přístup do aplikace, v níž iniciační (vstupní) heslo určuje administrátor, musí aplikace vynutit změnu tohoto iniciačního hesla při prvním přihlášení uživatele;
f) Všichni uživatelé musí při své činnosti používat jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činností;

g) Smluvní partner může používat jeden přihlašovací identifikátor pro několik svých zaměstnanců, přičemž smluvní partner odpovídá za veškeré úkony provedené v aplikaci či informačním systému pracovníkem přihlášeným s tímto identifikátorem;
h) Systém správy hesel musí být podpořen efektivním a interaktivním vybavením, které prosazuje a vynucuje požadovanou kvalitu hesel.

5.2 Řízení přístupu k informačním systémům

a) Před umožněním přístupu musí proběhnout identifikace a autorizace každého uživatele;
b) Informační systém (příp. aplikace) by měl po určité době nečinnosti uživatele (doporučená doba <15> minut) daného uživatele odhlásit;
c) Po stanoveném počtu neúspěšných autentizačních pokusů (dle politiky řízení přístupů <3>) se musí ukončit přihlašovací procedura;
d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informace o tom, která část autentizace je chybná;
e) U každého uživatele systému musí být možné identifikovat, jaká přístupová práva má přidělena;
f) Pro každý prostředek systému musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, zápis, editace, ...);
g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo celé skupině uživatelů.

5.3 Monitorování používání systému a přístupu k systému

V informačním systému (případně v jeho jednotlivých součástech) musí být pořizovány auditní záznamy obsahující minimálně:

a) Identifikační údaje uživatele, resp. osoby provádějící úkony;
b) Datum a čas přihlášení a odhlášení;
c) Identifikaci místa, odkud se uživatel (resp. osoba) přihlašoval (dle možností);
d) Záznamy o přístupu k systému, a to jak úspěšném i neúspěšném.

6 Bezpečnost informací a dat

6.1 Kontrola správnosti dat

Data vstupující do systémů musí být kontrolována tak, aby byla zajištěna jejich maximální správnost. V aplikaci se musí evidovat identifikátor uživatele nebo procesu, který pořízení nebo změnu dat provedl.

Pro kontrolu dat je nezbytné aplikovat opatření:

a) Vstupní formální kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislosti, ...);
b) Kontrola vnitřního zpracování dat (dle problematiky);
c) Kontrola správnosti běhu programů;
d) Kontrola integrity dat;
e) Kontrola obsahu generovaných dat.

Opatření musí zahrnovat popis postupu při zjištění chyby v datech.

Pokud bude usouzeno, že vytvářený informační systém nebo aplikace by měla podporovat (využívat) kryptografické prostředky pro zajištění integrity dat, je nezbytné, aby aplikované prostředky byly podporovány mezinárodně uznávanými standardy a byly dodrženy právní předpisy České republiky.

6.2 Data / informace předávané smluvním partnerům

Jedná se o informace předávané MČ Praha 1 smluvnímu partnerovi na jakémkoliv nosiči a v jakékoliv formě, zejména listiny a dokumenty, CD ROM, Flash disky, pevné disky, nebo zaslané emailem.

Dále se jedná o jakékoliv informace a data MČ Praha 1, s kterými se smluvní partner seznámí nebo k nim má přístup na základě realizace činností prováděných v rámci smluvního vztahu.

Smluvní partner musí s informacemi nakládat v souladu s ustanovením tohoto dokumentu, pokud není smlouvou stanoveno jinak.

a) Předání, resp. poskytnutí nebo přístup k informacím (datům) musí být vymezeno ve smlouvě (struktura dat, způsob předání/ poskytování, způsoby ochrany, ...) a musí probíhat řízením a bezpečným způsobem;
b) Uchovávání a případné zpracovávání dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana dle pravidel stanovených MČ Praha 1 před neoprávněným přístupem a aby bylo znemožněno jejich zneužití;
c) Zodpovědnost za ochranu informací (dat) má smluvní partner;
d) Informace (data), která již nejsou potřeba pro účely vymezené smluvním vztahem, musí být smluvním partnerem bezpečně zlikvidována, včetně jejich nosičů. Pro likvidaci nosičů obsahující neveřejné informace MČ Praha 1 musí být zvolena metoda, zaručující, že takto zlikvidované informace (data) nelze běžně dostupnými prostředky obnovit (např. skartovače, SW skartovače dat, ...); provedení likvidace doloží protokolem o jejich zlikvidování;
e) Každé nové předání informací (dat) nebo zřízení dálkového přístupu k informačnímu systému nebo databázi na smluvním základě musí být konzultováno s manažerem bezpečnosti informací MČ Praha 1, příp. s bezpečnostním správcem systému MČ Praha 1;
f) Smluvní partner si nesmí sám „stahovat" (získávat) žádná data z informačních systémů MČ Praha 1, vytváření souborů dat musí provádět zaměstnanec ÚMČ, která následně vytvořená data smí poskytnout, resp. předat smluvnímu partnerovi.

7 Pravidla pro vzdálený přístup do informačního systému

Vzdálený přístup do informačního systému je poskytován výhradně smluvnímu partnerovi, resp. pracovníkům smluvního partnera a nelze ho dále převádět na jiné osoby, a to ani z části. Porušení této povinnosti je považováno za závažné porušení smlouvy.

Smluvní partner se zavazuje, že vzdálený přístup do informačního systému bude používat výhradně za účelem konání prací specifikovaných ve smlouvě. Porušení této povinnosti je považováno za závažné porušení smlouvy.

Smluvní partner, resp. pracovníci smluvního partnera, jsou povinni dodržovat Pravidla pro vzdálený přístup do informačního systému (bod 7.1). Porušení jakékoli povinnosti uvedené v těchto pravidlech se považuje za závažné porušení smlouvy.

7.1 Přístup smluvního partnera (dodavatele) do informačních systémů – podmínky:

a) Pracovník dodavatele za účelem zřízení vzdáleného přístupu do informačního systému a možnosti se do tohoto systému přihlásit a pohybovat se v něm obdrží e-mailem od zákazníka přihlašovací jméno a prostřednictvím SMS zprávy heslo, které je z důvodu bezpečnosti generované a pracovník dodavatele ho nemůže změnit, přičemž heslo musí pracovník dodavatele udržovat v tajnosti a nezpřístupnit ho třetí osobě nebo ho využít pro soukromé účely.
b) Vzdálený přístup k informačnímu systému MČ Praha 1 musí být chráněn kryptografickými prostředky, v současné době je přístup realizován pomocí FortiClienta SSLVPN.
c) Po ukončení konání prací ve vzdáleném přístupu do informačního systému za účelem plnění smlouvy je pracovník dodavatele vždy povinen se odhlásit.
d) Pracovník dodavatele musí dodržovat pravidla bezpečnosti práce na počítači (stolní PC, notebook), zejména mít aktualizovaný SW a především antivirový program.
e) Pracovník dodavatele se nesmí pokoušet přistupovat na jiné servery, než které mu byly přiděleny v rámci vykonávaných smluvních prací.
f) Ukončení pracovního poměru pracovníka dodavatele s dodavatelem je dodavatel povinen písemně oznámit zákazníkovi nejpozději 5 pracovních dnů před ukončením tohoto pracovního poměru, přičemž zákazník je oprávněn vzdálený přístup do informačního systému pracovníkovi dodavatele bez dalšího s okamžitou platností zrušit.
g) V případě, že pracovník dodavatele poruší kterékoli ujednání těchto pravidel, je Odbor informatiky UMČ Praha 1 oprávněn okamžitě po zjištění porušení těchto pravidel zrušit tomuto pracovníkovi dodavatele vzdálený přístup do informačního systému bez dalšího. Dodavatel se zavazuje nejpozději do 5 kalendářních dnů ode dne, kdy mu zákazník oznámil toto zrušení, zajistit plnění smlouvy, potažmo této dohody, jiným zaměstnancem dodavatele, a o této výměně neprodleně písemně informovat zákazníka, přičemž tato výměna podléhá schválení zákazníkem.

Vzdálený přístup dodavatele může být povolen pouze do vývojového a testovacího prostředí za podmínek stanovených Odborem informatiky ÚMČ Praha. Případné výjimky musí být projednány a schváleny manažerem bezpečnosti informací MČ Praha 1, příp. bezpečnostním správce systému.

Lokální přístup dodavatele do provozního prostředí (příp. k aktivům MČ Praha 1) musí být povolen manažerem bezpečnosti informací MČ Praha 1 v odůvodněných případech a musí probíhat v režimu dohledu ze strany Odboru informatiky ÚMČ Praha 1 nebo oprávněného (stanoveného) pracovníka ÚMČ Praha 1, ale vždy na základě žádosti dodavatele a po schválení Odborem informatiky UMČ Praha 1.

8 Bezpečnost dodávek a služeb

8.1 Vývoj software a informačních systémů

Vývoj SW a informačních systémů musí probíhat:

a) S využitím legálního software;
b) Na testovacím prostředí odděleném od prostředí produkčního; za vytvoření testovacího prostředí a jeho bezpečnost odpovídá smluvní partner;
c) Na testovacích datech, která nejsou převzata z provozní databáze; za testovací data je odpovědný smluvní partner. Pokud je nutné použít data z provozní databáze, je nutné je předem anonymizovat. Za bezpečnost testovacích dat odpovídá smluvní partner;
d) Tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení těchto testů.
a) Součástí dodávky informačního systému, příp. jeho částí, musí být mimo jiné:
   - definice a dokumentování postupů pro spuštění a ukončení chodu IS a jeho částí,
   - definice a dokumentování postupů pro obnovu činnosti IS po havárii,
   - definice a dokumentování postupů pro ošetření mimořádných stavů technických i programových částí IS,
   - definice a dokumentování záznamů o provozu IS (logy), včetně případného dálkového přístupu k těmto záznamům, jejich formy a způsobu ukládání,
   - zajištění a dokumentování způsobu ochrany záznamů o provozu IS,
   - zajištění podpory ze strany dodavatele při řešení bezpečnostních incidentů,
   - definice a dokumentování postupů pro zálohování dat IS a pro obnovu dat ze záloh, včetně postupů testování použitelnosti záloh, pokud je tato funkcionalita součástí systému.

8.2 Dodávky software

a) Dodávka software (SW) musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována;
b) U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený SW, nebo SW podléhající licenční nebo registrační politice;
c) Dodávka licenčního SW musí zahrnovat jasné pravidla pro vydávání a používání licencí, včetně jejich evidence.
d) Každý nový SW musí být otestován, než bude akceptován a zařazen do produkčního prostředí daného systému MČ Praha 1; za provedení testů je odpovědný dodavatel daného SW.

8.3 Dodávky hardware

a) Dodávky hardware (HW) musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována;
b) O každé dodávce musí existovat, kromě účetních dokladů, také předávací protokol o řádném dodání a instalaci HW; podepsaný dodavatelem a za odběratele oprávněným pracovníkem Odboru informatiky ÚMČ Praha 1;
c) Způsob předání dodávaného HW a jeho otestování závisí na konkrétním produktu a podmínkách smluvním vztahu s dodavatelem;
d) Každé nové HW zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí; za provedení testů je odpovědný dodavatel daného hardware.

8.4 Dodávky služeb a ostatní služby

a) Dodávka služeb musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována ze strany dodavatele i zadavatele;
b) Způsob předání výstupů služby závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve smlouvě; vždy musí existovat předávací a akceptační protokol o řádném poskytnutí služby;
c) Pracovníci smluvních partnerů, zajišťující servis IT technologií (HW / SW / IS), jsou na základě smlouvy oprávněni se pohybovat i na neveřejných místech ÚMČ Praha 1; a to vždy a pouze s vědomím oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;
d) Pracovníci smluvních partnerů, zajišťující ostatní služby (např. úklid, ostrahu, ...) jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech ÚMČ Praha 1. Při svém pohybu musí dbát příslušných bezpečnostních pravidel, nemají zpravidla přístup k informačním aktivům MČ Praha 1.

8.5 Dokumentace dodávky SW, HW a služeb

a) Nedílnou součástí každé dodávky SW, HW nebo služeb je příslušná projektová, provozní a bezpečnostní dokumentace vztahující se k předmětu dodávky;
b) Chybějící, neúplná a/nebo neaktuální dokumentace je důvodem k reklamaci dodávky a může být i důvodem k neakceptaci dodávky z důvodů nenaplnění požadavků ze strany dodavatele;
c) Dokumentace musí být předána formálním způsobem a podrobena akceptačnímu řízení ze strany zadavatele, tj. MČ Praha 1;
d) Dodavatel je povinen všechny změny v konfiguraci IS/IT v průběhu dodávky zadokumentovat a v případě již zpracované dokumentace musí provést její aktualizaci v potřebném rozsahu.

8.6 Akceptace dodávky

a) Každý dodaný SW, HW a služba musí být plně a v potřebné míře otestována, zda splňuje očekávané a smluvně definované parametry; a zda jeho používání nepředstavuje neočekávaná bezpečnostní nebo provozní rizika;
b) V případě informačního systému, před jeho uvedením do rutinního provozu, musí být formálně akceptován z hlediska provozního příslušným pracovníkem Odboru informatika a z hlediska bezpečnosti informací MBI ÚMČ Praha 1.

8.7 Outsourcing

a) Outsourcing musí být řádně smluvně zajištěn, průběžně monitorován a dokumentován;
b) Externí zpracovávání neveřejných informací MČ Praha 1 a přístup k aktivům MČ Praha 1 musí být smluvně ošetřeno tak, aby byla zajištěna úroveň ochrany informací MČ Praha 1 ve všech aspektech informační bezpečnosti dle požadavků MČ Praha 1 a platných právních předpisů ČR.

9 Fyzická bezpečnost

Cílem fyzické bezpečnosti v oblasti IT je chránit prostředí, ve kterém se nacházejí aktiva MČ Praha 1, zabránit náhodnému nebo cílenému neautorizovanému přístupu, poškození nebo narušení aktiv MČ Praha 1.

Prostory ÚMČ Praha 1 jsou rozčleněny na oblasti veřejnosti přístupné a oblasti neveřejné (např. serverovny, prostory s HW aktivy, ...).

a) V neveřejných prostorech není dovolen pohyb cizích osob, tzn. včetně pracovníků smluvních partnerů (= neautorizovaných osob) bez doprovodu opravněného pracovníka ÚMČ Praha 1;
b) Cizí osoby (= neautorizované osoby) nesmějí být ponechány v neveřejných prostorech ÚMČ Praha 1 bez dozoru, pokud tato skutečnost není ošetřena smlouvou.

10 Personální bezpečnost

Cílem personální bezpečnosti v oblasti IT je vytvoření potřebného bezpečnostního povědomí zaměstnanců dodavatele, příp. subdodavatelů, smluvních partnerů MČ Praha 1 v oblasti zajištění ochrany a bezpečnosti aktiv MČ Praha 1 s cílem předcházet, příp. zabránit neautorizovanému přístup, narušení důvěrnosti a integrity aktiv MČ Praha 1.

a) Smluvní partner je odpovědný za veškeré aktivity osob provádějící činnosti na základě uzavřeného smluvního mezi smluvním partnerem a MČ Praha 1;
b) Smluvní partner zajistí, že veškeré činnosti dle smluvního vztahu, budou prováděny kompetentními osobami, s příslušnou odbornou kvalifikací a bezpečnostními zárukami;
c) Smluvní partner provede a doložitelně dokumentuje rozsah a obsah proškolení osob podílející se na realizaci smluvního vztahu v oblasti zajištění bezpečnosti informací MČ Praha 1;
d) Rozsah a obsah proškolení vychází jednak z požadavků tohoto dokumentu, dále z platné Politiky bezpečnosti informací MČ Praha 1 a dalších upřesnění manažera bezpečnosti informací k danému smluvnímu vztahu.