[redacted]

Smlouva o poskytnutí programového vybavení

číslo smlouvy poskytovatele: **30 / 2021**
číslo smlouvy zákazníka: **2021/1044**
číslo zakázky poskytovatele: 439

Smluvní strany

Městská část Praha 1

se sídlem:	Vodičkova 681/18, 115 68 Praha 1 – Nové Město
IČ:	00063410
DIČ:	CZ00063410
Zastoupená:	Ing. Petrem Hejmou, starostou
Bankovní spojení:	Česká spořitelna, pobočka Praha 1
Číslo účtu:	27-2000727399/0800

(dále jen „zákazník")

a

DATACENTRUM systems & consulting, a. s.

se sídlem:	Praha 4, Písnická 30/13, PSČ 14200
IČ:	25631721
DIČ:	CZ25631721
Zastoupená:	Ing. Kamilem Ryšavým, předseda představenstva společnosti
Bankovní spojení:	KB Praha 4, expozitura Chodov
Číslo účtu:	19-8779880297/0100

(dále jen „poskytovatel")

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-Oracle server (dále jen „DC2") a DC3-Docházka

a jeho servisu (dále jen „smlouva")

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 součástí smlouvy jsou přílohy specifikované v čl. 10 bodě 10.6

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 a DC3 - Docházka specifikované v Příloze č. 1.

2.1.2. Poskytovatel poskytne zákazníkovi nevýlučné nepřenosné právo užití programového vybavení DC2 a DC3 -Docházka 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 a DC3 - Docházka s jinými částmi informačního systému zákaznika.

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 a DC3 - Docházka (podle této smlouvy) jsou stanoveny dohodou smluvních stran a podrobně 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. Veškeré ceny podle této smlouvy jsou uvedeny v českých korunách.

Celková cena v Kč bez DPH	576.600,--Kč
(zákonné DPH)	121.086,--Kč
Celková cena v Kč včetně DPH	697.686,--Kč

3.2. Cena uvedená v tabulce se skládá z paušální, tedy povinné, částky viz. bod 6.1. Přílohy č. 2 a volitelné, tedy nepovinné, částky viz. bod 6.2. Přílohy č. 2.

3.3. Cena může být překročena pouze v souvislosti se změnou DPH či daňových předpisů majících vliv na výši ceny, a to ve výši odpovídající změně těchto předpisů.

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

3.5. 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.

3.6. Fakturace servisních služeb specifikovaných v Příloze č. 2 bude prováděna měsíčně, vždy k poslednímu dni v měsíci za daný kalendářní měsíc. Na faktuře bude vždy uvedeno číslo smlouvy zákazníka (CES).

3.7. Při prodlení zákazníka s úhradou jakékoli dlužné částky je poskytovatel oprávněn účtovat zadavateli úrok z prodlení v zákonné výši, stanovené nařízením vlády č. 351/2013 Sb., ve znění pozdějších předpisů.

3.8. 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. Pojištění

4.1. Poskytovatel se zavazuje, že po celou dobu poskytování svých služeb podle této smlouvy bude pojištěn pro případy škody vyplývající z výkonu svojí podnikatelské činnosti na částku předmětného pojištění alespoň 3 miliony Kč s maximální spoluúčastí 10 %. Poskytovatel je povinen do 5 pracovních dnů od uzavření smlouvy předložit zákazníkovi pojistnou smlouvu (certifikát) a udržovat ho v platnosti po celou dobu platnosti této smlouvy. V případě, že pojistná smlouva (pojistný certifikát) pozbyde své platnosti během plnění dle této smlouvy, je poskytovatel povinen zákazníkovi předložit novou pojistnou smlouvu (pojistný certifikát) do 7 pracovních dnů od pozbytí platnosti původní pojistné smlouvy (certifikátu).

5. Náhrada škody

5.1. 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.

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

5.3. Poskytovatel neodpovídá za škodu způsobenou neoprávněnými zásahy do programového vybavení DC2 a DC3 - Docházka ze strany zákazníka nebo třetích osob, popř. jeho užíváním jinak než v souladu s touto smlouvou.

6. Ochrana informací, mlčenlivost

6.1. 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“).

6.2. 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.

6.3. Poskytovatel prohlašuje, že programové vybavení DC2 a DC3 - Docházka 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.

6.4. 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 a DC3 - Docházka, provádět jeho změny nebo úpravy ani jej užívat jinak než v souladu s touto smlouvou.

6.5. Povinnost mlčenlivosti a ochrany důvěrných informací podle smlouvy trvá po dobu účinnosti smlouvy a dále 3 (slovy: tři) roky po jejím ukončení. Vzhledem k veřejnoprávnímu charakteru zákazníka poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen, že žádné ustanovení této smlouvy nepodléhá z jeho strany obchodnímu tajemství a souhlasí se zveřejněním smluvních podmínek obsažených ve smlouvě, včetně jejích příloh a případných dodatků smlouvy za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění.

7. Sankce

7.1. Nebude-li poskytovatel udržovat v aktuálním stavu potřebnou dokumentaci spojenou s plněním podle této smlouvy (podrobná specifikace v Příloze č. 5) je povinen zákazníkovi zaplatit smluvní pokutu ve výši 500,--Kč bez DPH za každé porušení a den prodlení.
7.2. Neposkytne-li poskytovatel zákazníkovi nezbytnou součinnost při realizaci úprav daných platnou legislativou a legislativními změnami zavazuje se zákazníkovi uhradit smluvní pokutu ve výši 500,--Kč bez DPH za každý den prodlení.
7.3. V případě nedodržení termínů dle Přílohy č. 2 je poskytovatel povinen uhradit zákazníkovi smluvní pokutu ve výši 500,- Kč bez DPH za každou započatou provozní hodinu zákazníka (Příloha č. 2 bod 1), maximálně však do výše měsíčního poplatku.
7.4. Poruší-li poskytovatel kteroukoli povinnost ochrany informací a mlčenlivost uvedenou čl. 6 smlouvy, zavazuje se zákazníkovi uhradit smluvní pokutu ve výši 100.000,--Kč bez DPH za každý jednotlivý případ porušení povinnosti.
7.5. Uplatněné smluvní pokuty se nezapočítávají do náhrady škody, která zákazníkovi vznikla nedodržením ustanovení této smlouvy či platných zákonů ze strany poskytovatele.
7.6. Smluvní pokuty jsou splatné do 30 dnů ode dne obdržení příslušného vyúčtování.
7.7. Sankci (smluvní pokutu, úrok z prodlení) vyúčtuje oprávněná strana straně povinné písemnou formou. Ve vyúčtování musí být uvedeno to ustanovení smlouvy, které k vyúčtování sankce opravňuje a způsob výpočtu celkové výše sankce.
7.8. Strana povinná se musí k vyúčtování sankce vyjádřit nejpozději do deseti dnů ode dne jeho obdržení, jinak se má za to, že s vyúčtováním souhlasí. Vyjádřením se v tomto případě rozumí písemné stanovisko strany povinné. Nesouhlasí-li strana povinná s vyúčtováním sankce, je povinna písemně ve sjednané lhůtě sdělit oprávněné důvody, pro které vyúčtování sankce neuznává.

8. Trvání a ukončení smlouvy

8.1. Tato smlouva nabývá platnosti v den podpisu a účinnosti dnem jejího uveřejnění v registru smluv Ministerstva vnitra ČR, v souladu se zákonem č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), včetně důsledků porušení této povinnosti. Povinnost uveřejnit smlouvu v registru smluv MV ČR náleží městské části Praha 1.

8.2. Tato smlouva se uzavírá na dobu určitou do 30. 11. 2024.

8.3. K plnění této smlouvy se poskytovatel zavazuje dnem 1. 12. 2021.

8.4. Právo užití programového vybavení DC2 a DC3 - Docházka poskytuje poskytovatel zákazníkovi na dobu neurčitou.

8.5. Poskytování služeb údržby k programovému vybavení DC2 a DC3 - Docházka je sjednáno na dobu trvání této smlouvy.

8.6. Zákazník i poskytovatel může vypovědět tuto smlouvu kdykoliv po jejím podpisu bez udání důvodu, a to písemnou výpovědí s 3 (tříměsíční) výpovědní lhůtou. Výpovědní lhůta začíná běžet 1. kalendářní den měsíce následujícího po doručení výpovědi druhé smluvní straně.

8.7. Zákazník je oprávněn odstoupit od této smlouvy s okamžitou platností pokud:
- 8.7.1. práva třetích osob přes opatření učiněná poskytovatelem a přes součinnost zákazníka řádně poskytnutou k těmto opatřením znemožňují zákazníkovi užití programového vybavení DC2 a DC3 - Docházka.
- 8.7.2. je poskytovatel v prodlení s předáváním prací ve stanovených termínech nebo zapracováním změn předpisů déle než 30 dnů.

8.8. Poskytovatel je oprávněn odstoupit od smlouvy s okamžitou platností pokud:
- je zákazník v prodlení s úhradou ceny déle než 60 dní,
- zákazník poruší autorské právo ve vztahu k předmětu této smlouvy.

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

9. Jiná ujednání

9.1. 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, kontaktní adresy a telefonní čísla jsou uvedeny v Příloze č. 2.

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

9.3. 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.

9.4. Poskytovatel je povinen v průběhu poskytování služby zajistit bezpečnost informací zákazníka, s kterými přichází do styku nebo se seznámí při poskytování služby. Minimální požadavky zákazníka na úroveň bezpečnosti informací ze strany poskytovatele jsou stanoveny v Příloze č. 5 smlouvy – „Etalon minimální bezpečnosti pro smluvní partnery".

9.5. Zákazník je povinen na příslušném virtuálním serveru, na kterém je aplikace poskytovatele provozována, zajišťovat pravidelné aktualizace příslušného operačního systému a jeho součástí. O termínu plánované aktualizace OS bude zákazník informovat poskytovatele minimálně 3 pracovní dny předem na hotline@datacentrum.cz. Po aktualizaci operačního systému je poskytovatel povinen zkontrolovat funkčnost aplikace, a pokud vykazuje chyby, je poskytovatel povinen zajistit odstranění chyb a plnou funkčnost aplikace v součinnosti se zákazníkem.

9.6. Zákazník bude předem projednávat s poskytovatelem veškeré změny použité dB platformy včetně příslušných verzí dB, popř. změny v instalacích zařízení a prostředí, které mohou ovlivnit HW/SW funkci systému.

9.7. Zákazník je povinný poskytnout dostatečnou součinnost, a to především zajištěním přístupu k systémům za účelem profylaktických prohlídek a servisních zásahů, včetně účasti oprávněných osob zákazníka, dále pak včasným předáváním požadovaných informací a ověřováním instalací v provozu.

9.8. Zákazník je povinný zajistit, aby hlášení o poruchách systému bylo podáváno s co možná největší přesností poskytovaných informací, a to zejména:

- kde a kdy porucha nastala, jak se projevuje,
- jaká opatření již Zákazník sám učinil ve snaze závadu odstranit.

10. Závěrečná ustanovení

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

10.2. 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.

10.3. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, přičemž ke každému stejnopisu jsou pevně připojeny přílohy specifikované v bodě 9.6. Každá smluvní strana obdrží jeden originál této smlouvy.

10.4. 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 v platném znění.

10.5. Tímto se osvědčuje v souladu s ustanovením § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, v platném znění., že návrh na uzavření této smlouvy byl projednán a schválen Radou městské části Praha 1 dne 16. 11. 2021 usnesením č. UR21_1348.

10.6. Nedílnou součástí smlouvy jsou následující přílohy:

Číslo	Příloha
Příloha č. 1	Popis programového vybavení
Příloha č. 2	Specifikace servisu k programovému vybavení
Příloha č. 3	Technický popis, příručka uživatele, příručka administrátora
Příloha č. 4	Čestné prohlášení o výlučnosti
Příloha č. 5	Etalon minimální bezpečnosti pro smluvní partnery

Příloha č. 1 – Popis programového vybavení

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 DC3 – 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 1.200 OSČ**)
DATACENTRUM 2 - Personalistika (**do 1.200 OSČ**)
DC2 klient (**pro max. 5 současně pracujících klientů**)
Počet zpracovávaných organizací (**1 organizace**)
DC3 - Docházka (**do 800 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 (formát xml)
NEMPRI – Příloha k žádosti o dávku nemocenského pojištění (formát xml)
Export převodních příkazů do banky (Česká spořitelna, Bussines 24)
Účetní doklad a jeho přenos do účetnictví Gordic
Generátor sestav
Poštovní klient
Výplatní pásky emailem (formát xls)
Napojení na EOS
Obecný import
Import dat z docházky DC3 - Docházka
Zpětný přepočet
Exekuce
Insolvence
Organigram
Výběr zaměstnanců - uchazeči
Plánování absencí
Výplatní pásky – náhled v docházce
Modul GDPR
Modul eNeschopenka – komunikace s ePortálem ČSSZ
Modul eNeschopenka – zápis do mzdových složek mzdovou agendu

Příloha č. 2 - Specifikace servisu k programovému vybavení:

1. Stanovení časového rozsahu poskytovaných služeb - Provozní doba zadavatele

Pondělí	8:00 - 18:00 hod.
Úterý	8:00 - 16:00 hod.
Středa	8:00 - 18:00 hod.
Čtvrtek	8:00 - 16:00 hod.
Pátek	8:00 - 14:00 hod.

2. 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.

b) ***Zákaznickou podporu k programovému vybavení – DC2 a DC3 - Docházka:***

- poskytovatel bude provádět správu systémů včetně průběžných aktualizací nových verzí. Před započetím aktualizace nahlásí poskytovatel na email kontaktní osobě informaci o distribuci nové verze a sdělení termínu instalace aktualizace. Zákazník, resp. kontaktní osoba, před zahájením aktualizace odsouhlasí termín. Poskytovatel je povinný před aktualizací programového vybavení požádat zákazníka o zajištění zálohy programového vybavení DC2 a DC3 - Docházka pro případnou obnovu systému,
- poskytovatel bude, vždy s novou aktualizací programového vybavení, zasílat zákazníkovi informace ke změnám v nové verzi,
- poskytovatel bude zabezpečovat servis pomocí svého help-deskového systému, e-mailu či telefonicky prostřednictvím pracovníka DTC,
- poskytovatel bude před přihlášením na server a realizací plánovaných prací informovat zákazníka včetně vyžádání souhlasu s plánovanými pracemi v daném termínu, v případě přihlášení jen pro náhled poskytovatel upozorňovat zákazníka nemusí. Vzdálený přístup pracovníků poskytovatele je vždy vázán na jméno technika,
- doba poskytované podpory v pracovní dny od 8.00 do 16.30,
- reakční doba poskytovatele v období od 1. do 10. dne v měsíci je v případě nahlášení havárie programového vybavení DC2 a DC3 - Docházky do 2 pracovních hodin od nahlášení havárie. Nástup na opravu je do 8 pracovních hodin od potvrzení nahlášení havárie. Pracovní hodiny jsou definovány od pondělí do pátku v době od 8:00 – 16:30,
- v ostatní pracovní dny (tj. od 11. dne do konce měsíce) je reakční doba do 24 pracovních hodin a nástup na opravu do 48 hodin od nahlášení havárie,
- poskytovatel bude 1x ročně provádět po předchozí domluvě individuální školení dle potřeb zákazníka pro 4 osoby v rozsahu 6 hodin.

3. Definice typů chyb

Chyba typu „A" = Kritická chyba:
Data jsou nesprávně počítána či ukládána do databáze nebo uživatelské rozhraní aplikace neumožňuje dokončit některou operaci dle uživatelské dokumentace.

Reakční doba v případě výskytu chyby typu „A" je do 48 hodin od nahlášení v době od 8.00 do 16.30 v pracovní dny. V případě nahlášení havárie ve dnech pracovního klidu bude požadavek řešen hned následující pracovní den.

Chyba typu „B" = Středně závažná chyba:
Může jít o jakoukoli chybu odpovídající definici chyby typu „A", nicméně musí existovat alternativní způsob, jak chybovost aplikace obejít a dosáhnout základního účelu prováděné operace (např. dokončit výpočet nebo provést uzávěrku).
Reakční doba v případě výskytu chyby typu „B" je do 72 hodin od nahlášení v době od 8.00 do 16.30 v pracovní dny. V případě nahlášení havárie ve dnech pracovního klidu bude požadavek řešen hned následující pracovní den.

Chyba typu „C" = Nezávažná chyba:
Jde o jakoukoli chybu jinou než typu „A" resp. „B", která žádným závažným způsobem nebrání používání aplikace. Náleží sem zejména nedostatky ve vzhledu obrazovek nebo výstupů z aplikace, v komfortu ovládání aplikace apod.
V případě výskytu chyby typu „C" bude odstranění chyby vyřešeno s vydáním upgradu verze.

4. Proces hlášení chyby:

a) Objednavatel nahlásí problém: musí obsahovat jednoznačný popis, typ (závažnost) chyby (který musí být následně Poskytovatelem odsouhlasen) a požadovaný termín odstranění.

b) Poskytovatel odpoví: odsouhlasí / navrhne změnu typu chyby, navrhne způsob odstranění a odhadne termín odstranění.
U chyb typu A musí být alespoň snahou řešením chybu převést na typ B a podobně typ B na typ C až do vyřešení.

c) Objednavatel odsouhlasí postup řešení

V případě sporu se postupuje dle eskalačního schématu.

5. Kontaktní osoby:

a) Kontaktní osoby za stranu zákazníka pro oblast servisu programového vybavení jsou:

Jméno a Příjmení
Telefon
E-mail
Adresa instalace

Jméno a Příjmení
Telefon
E-mail
Adresa instalace
Doplnit D
Jméno a Příjmení
Telefon
E-mail
Adresa instalace

b) Spojení na poskytovatele pro účely konzultací:

Jméno a Příjmení	Hotline
Telefon	+420 267 906 280
E-mail	hotline@datacentrum.cz
Adresa	Písnická 30/13, 142 00 Praha 4

c) Spojení na poskytovatele ve věcech obchodních:

Jméno a Příjmení	[redacted]
Telefon	
E-mail	
Adresa	
Jméno a Příjmení	
Telefon	
E-mail	
Adresa	

6. Ceny:

6.1. Paušální cena za servis programového vybavení DC2 a DC3 - Docházky

a) Poskytování UPGRADE a UPDATE verzí s garancí legislativních změn	9.866,- Kč/ měsíčně
b) Zákaznická podpora – standardní	4.984,- Kč/ měsíčně
CELKEM bez DPH:	**14.850,- Kč/ měsíčně**
DPH:	**3.118,50,- Kč/ měsíčně**
CELKEM s DPH:	**17.968,50,- Kč/ měsíčně**

Celková paušální cena za 36 měsíců bez DPH	534.600,- Kč
DPH	112.266,- Kč
Celková paušální cena za 36 měsíců s DPH	646.866,- Kč

Cena stanovená dle bodu 6 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.

6.2. Celková cena plnění za služby nad rámec paušálních služeb podle bodu 6.1 za období plnění smlouvy je závislá na počtu objednaných podporových hodin nad rámec paušálu. Smluvní strany se dohodly na maximálním počtu 30 podporových hodin práce konzultanta v sazbě 1.400,- Kč za hodinu bez DPH nad rámec paušálu, které však Zákazník nemusí využít.

Celková cena za 30 podporových hodin bez DPH	42.000,- Kč
DPH	8.820,- Kč
Celková cena za 30 podporových hodin s DPH	50.820,- Kč

6.3. Fakturace dle bodu č. 6 Přílohy č. 2 bude zahájena po podpisu smlouvy a to vždy po akceptaci měsíčního výkazu poskytnutých služeb. Akceptace ze strany zákazníka proběhne max. do 5 pracovních dnů od zaslání výkazu.

7. Jiná ujednání

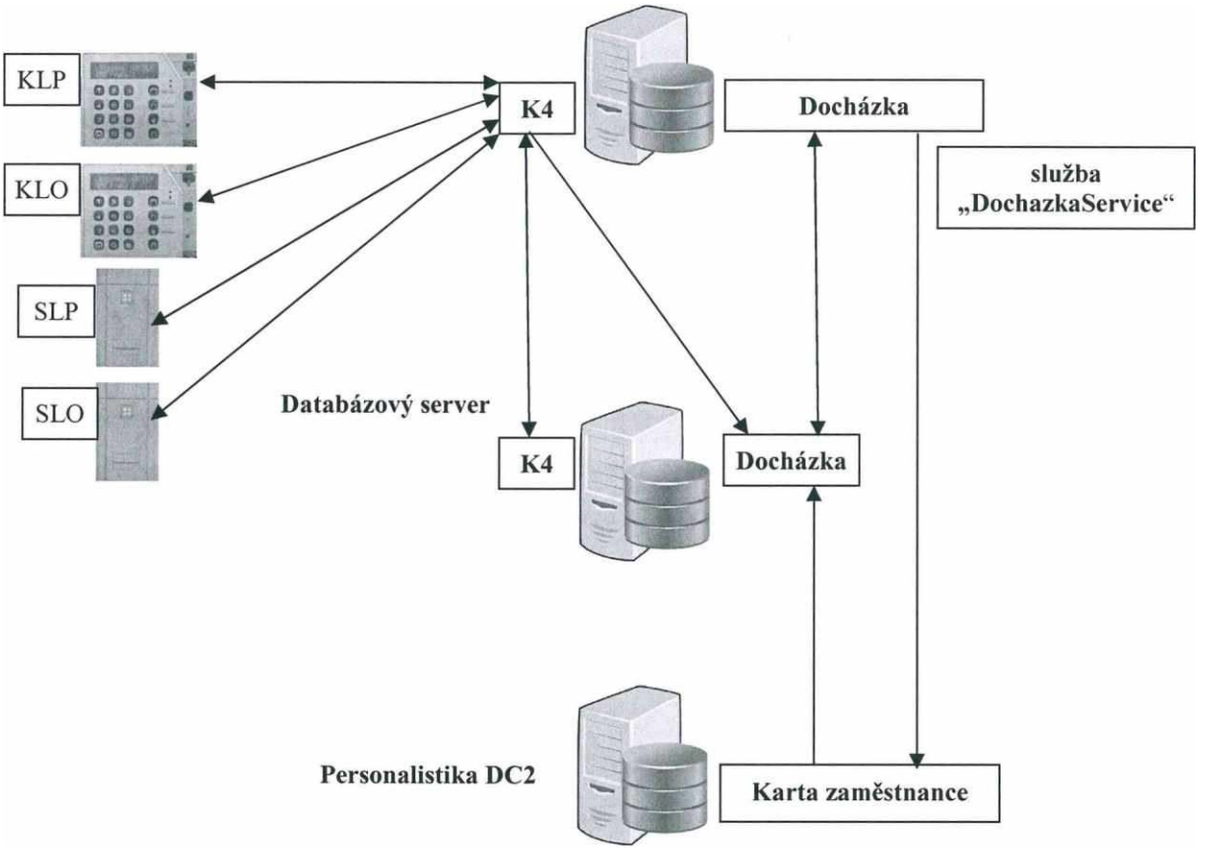
Zákazník souhlasí s tím, aby poskytovatel po dobu platnosti této smlouvy uváděl ve svých propagačních materiálech, výročních zprávách, přihláškách do tendrů a výběrových řízení a do dalších textů jméno zákazníka jako referenčního klienta, včetně jména kontaktní osoby zákazníka a jejího telefonního a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

Příloha č. 3 – Technický popis, příručka uživatele, příručka administrátora

Příručka uživatele a administrátora pro DC3 - Docházku bude zaslána zákazníkovi jako samostatný dokument mimo tuto přílohu smlouvy. Nápověda/příručka k programovému vybavení DC2 je pro uživatele dostupná přímo v aplikaci.

Technický popis



Databázový server

HW

Doporučená konfigurace pro databázový server je:

- 4 CPU
- RAM 6 GB a vyšší
- HDD min. 100 GB (DB + zálohy)

SW

Momentálně jsou podporovány následující databázové stroje:

- Microsoft SQL Server 2016+
- Microfost SQL Azure
- Oracle 12c+

V případě, že je použit databázový server Oracle, je nutné zajistit, aby uživatel **DC3** měl nagrantovaná následující oprávnění:

```
GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO "DC3";
GRANT CREATE VIEW TO "DC3";
```

Aplikační server

HW

Doporučená konfigurace pro aplikační server je

- 4 CPU
- RAM 6 GB a vyšší
- HDD min. 60 GB
- OS MS Windows Server 2016 (Programové vybavení DC2 není kompatibilní s vyšší verzí)

SW

Před vlastní instalací je nutné se ujistit, zda jsou na aplikačním serveru nainstalovány následující komponenty:

- .NET Core 5.0.7 Windows Hosting installer

Aplikační server dále musí být nakonfigurován v roli **Web server (IIS)**. V této roli je třeba zapnout minimálně následující balíčky:

- Web Server
  - Common HTTP Features
    - Default Document
    - Directory Browsing

- HTTP Errors
- Static Content
- HTTP Redirection

- Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - Request Monitor
- Performance
  - Static Content Compression
- Security
  - Request Filtering
  - Client Certificate Mapping Authentication
  - IIS Client Certificate Mapping Authentication
  - Windows Authentication
- Application Development
  - .NET Extensibility 4.5
  - Application Initialization
  - ASP.NET 4.5
  - ISAPI Extensions
  - ISAPI Filters
  - WebSocket Protocol

Management Tools

- IIS Management Console

Příloha č. 4 – Čestné prohlášení o výlučnosti

Poskytovatel DATACENTRUM systems & consulting, a. s., IČ: 25631721, [redacted] čestně prohlašuje, že je výlučným majitelem a jediným poskytovatelem programového vybavení, které je předmětem plnění této smlouvy.

Příloha č. 5 - Etalon bezpečnosti pro smluvní partnery (dokument Prahy 1)

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.
Etalon minimální bezpečnosti informací pro dodavatele MČ Praha 1 se na některých místech odkazuje na platné dokumenty o ICT a o bezpečnosti informací na MČ.
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 ze dne 6. 11. 2018.
Cílem etalonu minimální bezpečnosti 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 prostředí 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 souvisejících 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 v souladu s provozní a bezpečnostní dokumentací MČ Praha 1;
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 byly smluvnímu partnerovi 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, se kterými partnera vlastník informací prokazatelně seznámí;
g) Odpovědnost za dostatečné proškolení svých zaměstnanců a pracovníků svých subdodavatelů v oblasti zajištění bezpečnosti informací MČ Praha 1;
h) 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 Koncové pracovní stanice

Při práci na koncových stanicích nebo zařízeních smluvních partnerů, ze kterých se přistupuje do vnitřní sítě MČ Praha 1, musí být splněna nejméně následující bezpečnostní pravidla:

a) Použití koncového zařízení (počítače) musí být umožněno pouze oprávněné osobě; (Osoba oprávněná k použití koncového zařízení musí být vybavena přístupovými oprávněními.)
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 zapnutá a s přihlášeným uživatelem (k aplikaci, k IS); za minimální opatření se považuje „uzamčení" pracovní stanice (v každém případě je třeba minimalizovat možnost fyzického přístupu neoprávněným osobám);
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 virových definic (tento antivirový program by měl být v maximální míře aktualizován vůči všem známým virům). Dále je smluvní partner též zodpovědný za pravidelnou aktualizaci operačních systémů na těchto svých počítačích;
e) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému.

V případě, že smluvní partner vykonává svoji činnost též na ICT prostředcích nacházejících se na ÚMČ Praha 1, je povinen chránit vybavení ÚMČ Praha 1 a udržovat bezpečné pracovní prostředí. V blízkosti prostředků informačních technologií je zakázáno jíst, pít a kouřit.

4.2 Využívání prostředků a internetu

Systémy MČ Praha 1, vztahující se k počítačové síti, internetu, intranetu, počítačovému vybavení, k operačním systémům a médiím pro ukládání dat apod., jsou ve vlastnictví MČ Praha 1. Tyto systémy mohou být používány pouze pro pracovní účely tak, aby to sloužilo zájmům MČ Praha 1.

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 dohodnuty s Odborem informatiky ÚMČ Praha 1.

Obecně platí povinnost, že smluvní partner předem oznamuje datum a čas přihlášení k vnitřnímu prostředí a následné ukončení práce ve vnitřním prostředí systémů MČ Praha 1, ledaže se smluvní strany dohodnou jinak.

4.3 Bezpečnost IS / IT systémů

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

5 Řízení přístupu k informačním systémům a aplikacím

a) Informační systémy a aplikace by měly být vytvářeny tak, aby byl vždy vyžadován autorizovaný přístup uživatelů (identifikační a autentizační údaje) a měla by být zaznamenávána činnost uživatele v aplikaci/systému;
b) Uživatel informačního systému případně aplikace by měl být nucen si své přístupové heslo pravidelně měnit;
c) Informační systémy a aplikace, které nepřebírají přihlašovací údaje z Active Directory MČ Praha 1, by měly být vytvořeny tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po třech neúspěšných pokusech o přihlášení musí být další zadávání hesla dočasně omezeno nebo činnost ukončena.
d) Pokud je při přihlašování do aplikace či informačního systému 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 či informačního systému, který nepřebírá přihlašovací údaje z Active Directory MČ Praha 1, a v němž iniciační (vstupní) heslo určuje administrátor, měl by informační systém či aplikace vynutit změnu tohoto iniciačního hesla při prvním přihlášení uživatele;
f) Všichni uživatelé by měli při své činnosti používat jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti;
g) Každý pracovník na straně smluvního partnera, který pracuje s informačním systémem či aplikací, musí používat svůj vlastní přihlašovací identifikátor. (Smluvní partner tedy nemůže používat jeden přihlašovací identifikátor pro několik svých zaměstnanců.) Dále smluvní partner odpovídá za veškeré úkony provedené v aplikaci či informačním systému pracovníkem přihlášeným pod tímto identifikátorem;
h) Systém správy hesel by měl být podpořen efektivním a interaktivním vybavením, které prosazuje a vynucuje požadovanou kvalitu hesel;
i) U každého uživatele systému musí být možné identifikovat, jaká přístupová práva má přidělena;
j) 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, ...);
k) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo celé skupině uživatelů.

5.1 Monitorování používání systému a přístupu k systému

V informačním systému (případně v jeho jednotlivých součástech) musí být pořizovány auditní záznamy. Tyto záznamy by měly obsahovat údaje a informace, které jsou nezbytné k identifikaci aktivit sledovaného uživatele (jeho identifikační údaje, datum a čas přihlášení a odhlášení apod.)

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 by se měl evidovat identifikátor uživatele nebo procesu, který pořízení nebo změnu dat provedl.
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 informace zaslané emailem.
Dále se jedná o jakékoliv informace a data MČ Praha 1, se 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 následujícími ustanoveními 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 řízeným a bezpečným způsobem;
b) Uchovávání a případné zpracovávání dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana dle pravidel stanovených v bezpečnostní dokumentaci MČ Praha 1 (se kterými byl smluvní partner prokazatelně seznámen). Uchovávání a zpracování dat musí být ochráněno před neoprávněným přístupem a možným zneužitím – v souladu s bezpečnostními požadavky MČ Praha 1;
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 partner 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, případně s bezpečnostním správcem systému MČ Praha 1;
f) Smluvní partner si nesmí bez písemného souhlasu MČ Praha 1 sám „stahovat" (získávat) žádná data z informačních systémů MČ Praha 1. Data může uchovat pouze po nezbytně nutnou dobu.
g) Informace (data), která jsou součástí řešení, vytvářeného smluvním partnerem, nebo jsou předávána na základě realizace činností prováděných partnerem v rámci smluvního vztahu, se budou předávat pouze na vyžádání oprávněného pracovníka MČ Praha 1.

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 pracovníka informatiky MČ Prahy 1 přihlašovací jméno, certifikát a prostřednictvím SMS zprávy heslo, které je z důvodu bezpečnosti generované a pracovník dodavatele ho musí změnit za bezpečné heslo. Pracovník dodavatele musí heslo udržovat v tajnosti a nesmí jej zpřístupnit třetí osobě nebo jej 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 klienta SSL VPN.
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 svém počítači (stolní PC, notebook), ze kterého realizuje vzdálený přístup do informačního systému. Tento počítač musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databází (tento antivirový program by měl být v maximální míře aktualizován vůči všem známým virům). Dále musí tento počítač mít aktualizovaný operační systém a další obslužný SW.
e) Pracovník dodavatele se nesmí pokoušet přistupovat na jiné servery než ty, které mu byly přiděleny v rámci vykonávaných smluvních prací, aktivita na účtě může být monitorována.
f) Ukončení pracovního poměru pracovníka dodavatele s dodavatelem je dodavatel povinen písemně oznámit odpovědným pracovníkům Odboru informatiky ÚMČ Praha 1 nejpozději 5 pracovních dnů po ukončení tohoto pracovního poměru, přičemž Odbor informatiky ÚMČ Praha 1 je oprávněn vzdálený přístup do informačního systému pracovníkovi dodavatele bez dalšího s okamžitou platností zrušit, při neoznámení této skutečnosti nese dodavatel plnou zodpovědnost za činnost tohoto bývalého pracovníka.
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 Odbor informatiky ÚMČ Praha 1 oznámil toto zrušení, zajistit plnění smlouvy, potažmo této dohody, jiným zaměstnancem dodavatele, a o této výměně neprodleně písemně informovat Odbor informatiky ÚMČ Praha 1, přičemž tato výměna podléhá schválení Odborem informatiky ÚMČ Praha 1.

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

Lokální (přímý) přístup dodavatele do prostředí MČ Praha 1 (případně k aktivům MČ Praha 1) musí být v odůvodněných případech povolen manažerem bezpečnosti informací MČ Praha 1 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, informačních systémů a jejich modulů

Vývoj SW a informačních systémů musí probíhat:

a) s využitím legálního software;
b) na testovacím prostředí odděleném od prostředí produkčního. Za vytvoření softwarové složky testovacího prostředí v rozsahu své dodávky odpovídá smluvní partner, za vytvoření ostatních částí testovacího prostředí a jeho bezpečnost odpovídá MČ Praha 1;
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, přičemž za anonymizaci těchto dat odpovídá MČ Praha 1. Za bezpečnost testovacích dat v rozsahu smluvně dohodnutých pravidel odpovídá smluvní partner;
d) tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení těchto testů.

Před zahájením vývoje je smluvní partner povinen projednat se zástupci Odboru informatiky ÚMČ Praha 1 své navrhované řešení. Odbor informatiky musí předem odsouhlasit veškeré hardwarové, softwarové a síťové požadavky vytvářeného řešení a musí se předem ubezpečit, zda toto řešení bude respektovat veškeré bezpečnostní standardy MČ Praha 1.

8.2 Dodávky software a hardware

a) Dodávka software (SW) a hardware (HW) 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 jasná pravidla pro vydávání a používání licencí, včetně jejich evidence;
d) O každé dodávce musí existovat kromě účetních dokladů také předávací protokol o řádném dodání a instalaci; podepsaný dodavatelem a za odběratele oprávněným pracovníkem Odboru informatiky ÚMČ Praha 1;
e) Každý nový SW/nové HW zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí daného systému MČ Praha 1; za provedení testů je odpovědný dodavatel daného SW/HW, přičemž MČ Praha 1 je při provádění předmětných testů povinna poskytnout přiměřenou součinnost.
f) Správce HW (případně MČP1) je povinen na příslušném fyzickém či virtuálním serveru, na kterém je SW/aplikace Dodavatele (pro niž je správcem) provozována, zajišťovat pravidelné aktualizace příslušného operačního systému běžícího na tomto serveru. V případě, že po aktualizaci operačního systému je SW/aplikace nefunkční nebo vykazuje chyby, je Dodavatel SW/aplikace povinen zajistit odstranění chyb a plnou funkčnost SW/aplikace.

8.3 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.

8.4 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, včetně její aktualizace;
b) Dokumentace musí být předána formálním způsobem a podrobena akceptačnímu řízení ze strany zadavatele, tj. MČ Praha 1;
c) 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.

8.5 Akceptace dodávky

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

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 oprávněného 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 přístupu, narušení důvěrnosti a integrity aktiv MČ Praha 1.
Smluvní partner je odpovědný za veškeré aktivity svých pracovníků a pracovníků svých subdodavatelů provádějících činnosti na základě uzavřeného smluvního mezi smluvním partnerem a MČ Praha 1;

Smluvní partner zajistí, že veškeré činnosti dle smluvního vztahu budou prováděny jeho zaměstnanci nebo subdodavateli, budou prováděny kompetentními osobami, s příslušnou odbornou kvalifikací a bezpečnostními zárukami;

Smluvní partner provede a doložitelně zdokumentuje rozsah a obsah proškolení osob podílejících se na realizaci smluvního vztahu v oblasti zajištění bezpečnosti informací MČ Praha 1;

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. Obsah proškolení bude též vycházet z bezpečnostní dokumentace MČ Praha 1, kterou bude mít smluvní partner k dispozici.