DODATEK Č. 3
SMLOUVY O TECHNICKÉ PODPOŘE

Městská část Praha 1

Sídlo:	Vodičkova 18, Praha 1, PSČ 115 68
Zastoupená:	Ing. Oldřichem Lomeckým, starostou MČ Praha 1
IČO:	00063410
DIČ:	CZ00063410
Bankovní spojení:	Česká spořitelna a.s.
Číslo účtu:	27-2000727399/0800

(dále jen „Objednatel")

a

AiP Safe s.r.o.

Sídlo:	Talichova 807, Beroun 2, PSČ 266 01
Jednající:	Ing. Jan Mottl, jednatel
IČO:	26128012
DIČ:	CZ26128012
Bankovní spojení:	ČSOB a.s.
Číslo účtu:	161790816/0300

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 72599
(dále jen „Poskytovatel")

(dále označovány společně jako „strany této Smlouvy" nebo „smluvní strany")

uzavřely níže uvedeného dne, měsíce a roku tento

Dodatek č. 3
ke smlouvě o technické podpoře ze dne 28. 3. 2014
číslo smlouvy Objednatele 2014/0445, číslo smlouvy Poskytovatele S090027
(dále jen „Dodatek").

I.
Předmět Dodatku

1. Smluvní strany spolu uzavřely dne 28. 3. 2014 smlouvu o technické podpoře (dále jen „Smlouva") provozovaného Software dříve dodaného Poskytovatelem. Nedílnou součástí Smlouvy jsou její přílohy č. 1 až č. 4.
2. V souladu s článkem 12. odstavcem 12.1 byla tato Smlouva uzavřena s účinností na období od 1. 4. 2014 do 31. 12. 2014 s tím, že její platnost a účinnost může být po dohodě smluvních stran písemným dodatkem prodloužena, což se již stalo Dodatkem č. 1 Smlouvy podepsaným dne 30. 12. 2014, kterým byla platnost a účinnost Smlouvy prodloužena na období od 1. 1. 2015 do 31. 12. 2015, a Dodatkem č. 2 Smlouvy

podepsaným 14. 1. 2016, kterým byla platnost a účinnost Smlouvy prodloužena na období od 1. 1. 2016 do 31. 12. 2016.

3. Rozsah Objednatelem provozovaného aplikačního vybavení se v období od uzavření Dodatku č. 2 Smlouvy rozšířil na základě objednávky č. 4500060154 ze dne 22. 4. 2016 o rozšíření systému DMS 2 SAFE o automatické mazání dokumentů pro Úřední desku a Objednatel se rozhodl k zajištění technické podpory i pro dříve dodaný systém DMS 2 SAFE a Replikační aplikaci systému DMS 2 SAFE, a proto se Objednatel a Poskytovatel dohodli na novém znění Přílohy č. 4 Smlouvy a Přílohy č. 2 Smlouvy, které v tomto pořadí specifikují komponenty servisované Poskytovatelem a výši jeho odměny za poskytování základních služeb technické podpory Objednateli.
4. Objednatel a Poskytovatel se dále dohodli na prodloužení platnosti a účinnosti Smlouvy o dalších 8 kalendářních měsíců.
5. Předmětem tohoto Dodatku je proto prodloužení platnosti a účinnosti Smlouvy na období od 1. 1. 2017 do 31. 8. 2017, změna výše odměny Poskytovatele za poskytování základních služeb technické podpory Objednateli a rozšíření seznamu komponent servisovaných Poskytovatelem.
6. Poskytovatel je povinen v průběhu poskytování služby zajistit bezpečnost informací Objednavatele, s kterými přichází do styku a/nebo se seznámí při poskytování služby. Minimální požadavky Objednavatele na úroveň bezpečnosti informací ze strany Poskytovatele jsou stanoveny v příloze č. 1 tohoto dodatku – „Etalon minimální bezpečnosti pro smluvní partnery".

II.
Dodatkem provedené změny ve Smlouvě

1. Smluvní strany se dohodly na následující změně Smlouvy:

V článku 12 „Platnost a účinnost Smlouvy" se za odstavec 12.1.2 vkládá nový odstavec 12.1.3, který zní:

> „Platnost a účinnost této Smlouvy se po dohodě smluvních stran prodlužuje písemným Dodatkem č. 3 k této Smlouvě na období od 1. 1. 2017 do 31. 8. 2017."

2. Smluvní strany se dále dohodly na následující změně Smlouvy:

V Příloze číslo 2 Smlouvy „Podrobná specifikace poskytovaných služeb" se v její části 3 „Cena a rozsah technické podpory" ruší v článku 3.1 stávající tabulka

Služba	**Cena bez DPH za 1 kalendářní měsíc (i započatý)**
Odstraňování ZKZ a telefonická podpora a Inovace Software	**11 776,- Kč**

a nahrazuje se tabulkou

Služba	**Cena bez DPH za 1 kalendářní měsíc (i započatý)**
Odstraňování ZKZ a telefonická podpora a Inovace Software	**17 429,- Kč**

3. Smluvní strany se dále dohodly na následující změně Smlouvy:

V Příloze číslo 4 Smlouvy „Specifikace podporovaného programového vybavení" se v její části 3 „Přehled podporovaných řešení" doplňují do stávající tabulky „Popis agendy/rozšíření" doplňují následující řádky:

DMS 2 SAFE jako úložiště souborů aplikací v demilitarizované zóně ÚMČ Praha 1 (zdrojová data pro Úřední desku a pro časové řezy daty Úřední desky)
Replikační aplikace mezi DMS 1 SAFE a DMS 2 SAFE pro: - Usnesení rady a zastupitelstva (vybrané části ke zveřejnění) - Dokumenty e-Spis pro Úřední desku
Dokumenty e-spis pro Úřední desku v DMS 2 SAFE
Usnesení rady a zastupitelstva v DMS 2 SAFE
Automatické mazání dokumentů Úřední desky od exekutorů a finančních úřadů v DMS 2 SAFE

4. Ostatní ujednání Smlouvy ve znění všech jejích dodatků zůstávají v platnosti beze změn.

III.
Závěrečná ustanovení

1. Tento Dodatek nabývá platnosti i účinnosti dnem jeho podpisu oběma Smluvními stranami.
2. Tento Dodatek byl sepsán po vzájemné dohodě Smluvních stran na základě jejich pravé a svobodné vůle, nikoli v tísni za nápadně nevýhodných podmínek.
3. Tento Dodatek je vyhotoven ve dvou stejnopisech s platností originálu, z nichž každá ze Smluvních stran obdrží po jednom.
4. Tento Dodatek obsahuje přílohu č.1 - „Etalon minimální bezpečnosti pro smluvní partnery".

[redacted]

[redacted]

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 ze dne 19.11.2014.

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, se kterými ho vlastník informací prokazatelně seznámí;
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 smluvních partnerů, ze kterých se přistupuje do vnitřní sítě MČ Praha 1, 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 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 aplikace, která nepřebírá přihlašovací údaje z Active Directory MČ Praha 1, 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, která nepřebírá přihlašovací údaje z Active Directory MČ Praha 1, a 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 se kterými ho MČ Praha 1 prokazatelně seznámí, 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 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.
e) 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.

Pokud výše uvedená dokumentace nebo některá z jejích částí nebyla součástí dodávky dříve dodaného software nebo informačního systému, uzavře MČ Praha 1 se smluvním partnerem smlouvu o jejím doplnění.

Pokud některou z výše uvedených služeb smluvní partner MČ Praha 1 ke dni nabytí účinnosti dodatku smlouvy mezi MČ Praha 1 a smluvním partnerem zavádějícího do smluvního vztahu etalon minimální bezpečnosti neposkytuje, zavazují se smluvní partneři řešit poskytování této služby samostatným dodatkem ke smlouvě.

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 SW, přičemž MČ Praha 1 je při provádění předmětných testů povinna poskytnout přiměřenou součinnost.

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 ode dne nabytí účinnosti dodatku smlouvy mezi MČ Praha 1 a smluvním partnerem zavádějícího do smluvního vztahu „Etalon minimální bezpečnosti pro smluvní partnery" 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 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 přístup, narušení důvěrnosti a integrity aktiv MČ Praha 1.

a) 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;
b) 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;
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.