[redacted]

SMLOUVA
O TECHNICKÉ PODPOŘE

číslo TP07/17

CES č. 2017/0067.....

Poskytovatel: VITA software, s.r.o., Na Beránce 57/2, 160 00 Praha 6, IČ 61060631
zapsaná u Městského soudu v Praze, značka C/42951
zastoupená jednatelem RNDr. Ivanou Havlíkovou

Uživatel: Městská část Praha 1, Vodičkova 18, 115 68 Praha 1, IČ 00063410
zastoupená Ing. Miloslavem Urbanem vedoucím odboru informatiky

Poskytovatel a Uživatel 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 TECHNICKÉ PODPOŘE

I.
Úvodní ustanovení

1. Práva a závazky z této smlouvy se řídí právním řádem České republiky. Pokud tato smlouva nestanoví odchylnou úpravu, použijí se ustanovení obecně platných předpisů, zejména zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a zákona č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů.

II.
Předmět smlouvy

1. Předmětem smlouvy je poskytování technické podpory a dalších služeb k software poskytovatele, který má uživatel právo užívat. Software a další služby jsou specifikovány v příloze č. 1 SPECIFIKACE.

III.
Práva a povinnosti poskytovatele

1. Poskytovatel se zavazuje poskytovat uživateli technickou podporu v souladu s LICENČNÍMI PODMÍNKAMI, které jsou přílohou č. 2 této smlouvy, a další služby specifikované v příloze č. 1 SPECIFIKACE.
2. Poskytovatel je povinen provést změny software před termínem účinnosti změn právních předpisů. Pokud právní předpis nabude účinnosti dříve než 30 dnů po uveřejnění ve Sbírce zákonů, je poskytovatel povinen provést změny software nejpozději do 30 dnů ode dne uveřejnění ve Sbírce zákonů.
3. Poskytovatel je povinen změněný software neprodleně zpřístupnit uživateli na svých webových stránkách pro instalaci. Spolu s tím je povinen zpřístupnit seznam změn.
4. Poskytovatel odpovídá za zajištění konzistence dat při změně software.
5. Poskytovatel službu HotLine poskytuje prostřednictvím e-mail na hotline@vitasw.cz a na telefonní lince uvedené na www.vitasw.cz, a to v pracovních dnech v době 8 - 15 hod, v pondělí a středu do 17 hodin.
6. Poskytovatel poskytuje uživateli službu HelpDesk http://www.vitasw.cz/helpdesk.

7. Poskytovatel je povinen v průběhu poskytování dalších služeb zajistit bezpečnost informací uživatele, s kterými přichází do styku a/nebo se seznámí při poskytování dalších služeb Minimální požadavky uživatele na úroveň bezpečnosti informací ze strany poskytovatele jsou stanoveny v příloze č. 3 této smlouvy – „Etalon minimální bezpečnosti pro smluvní partnery"

IV.
Práva a povinnosti uživatele

1. Uživatel má právo užívat změněný software po úhradě ceny za technickou podporu.
2. Uživatel je povinen užívat software v souladu s Licenčními podmínkami.
3. Uživatel uveřejní smlouvu prostřednictvím registru smluv podle zákona o registru smluv.

V.
Mlčenlivost

1. Smluvní strany se zavazují zachovávat mlčenlivost o důvěrných informacích. Pro účely této smlouvy se za důvěrné informace považují veškeré informace a údaje, které se smluvní strany dozví v přímé i nepřímé souvislosti s plněním předmětu smlouvy, především všechny údaje uložené v informačním systému uživatele, informace o právech a povinnostech, cenách a průběhu plnění podle této smlouvy a informace týkající se obchodního tajemství, činnosti, struktury, hospodářských výsledků a know-how smluvních stran.
2. Při plnění předmětu smlouvy budou smluvní strany vzájemně spolupracovat v oblasti přípravy, realizace a rozvíjení informačního systému uživatele, který uchovává a zpracovává osobní údaje podle zákona o ochraně osobních údajů. Za tímto účelem bude mít poskytovatel přístup k údajům uloženým v informačním systému uživatele. Smluvní strany se řídí zákonem č. 101/2000 Sb., o ochraně osobních údajů.
3. Smluvní strana:
   a) je povinna nakládat s důvěrnými informacemi druhé strany tak, že omezí přístup k nim pouze na pověřené osoby, a to pouze v rozsahu nutném pro plnění předmětu smlouvy,
   b) nepoužije důvěrné informace jí poskytnuté v souladu s touto smlouvou k jinému účelu než vymezenému touto smlouvou, nepředá je, ani nezpřístupní třetím osobám,
   c) nebude pořizovat jakékoliv kopie důvěrných informací poskytnutých jí druhou stranou v souladu s touto smlouvou.
4. Smlouva není obchodním tajemstvím a kterákoli ze smluvních stran ji může zveřejnit.

VI.
Cena

1. Cena technické podpory na jedno čtvrtletí činí **21.196,-** Kč bez DPH. Specifikována je v příloze č. 1 SPECIFIKACE.
2. Platba technické podpory za software dle Specifikace se sjednává od 2.1.2017.
3. Poskytovatel bude účtovat technickou podporu vždy na počátku daného období. Faktura je splatná do 30 dnů ode dne doručení uživateli. Ke všem cenám podle této smlouvy bude připočtena daň z přidané hodnoty v zákonné výši.
4. Na faktuře bude jako číslo objednávky uvedeno č. smlouvy CES.
5. Pro případ prodlení uživatele s úhradou ceny za předmět smlouvy je poskytovatel oprávněn vyúčtovat mu úrok ve výši 0,05% z dlužné ceny za každý den prodlení, nejvýše však 30% z této ceny.
6. Pokud poskytovatel nedodrží termín dodání předmětu smlouvy, vzniká uživateli právo na zaplacení smluvní pokuty ve výši 0,05% z ceny nedodaného předmětu smlouvy za každý den prodlení, nejvýše však 30% z této ceny.

VII.
Závěrečná ujednání

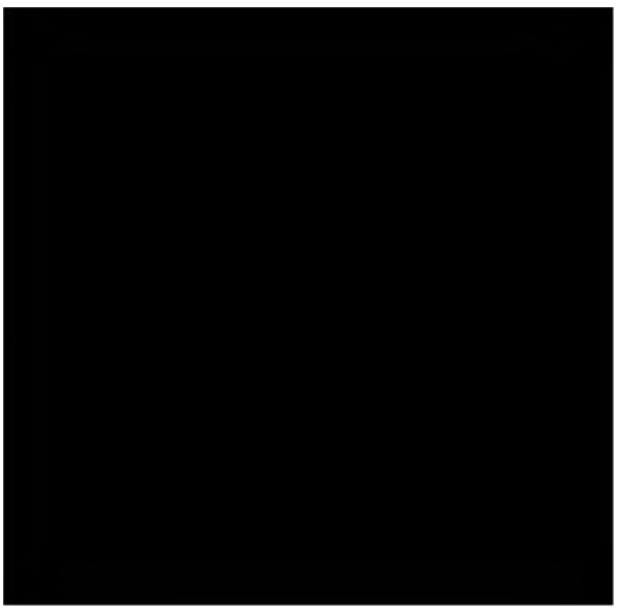
1. Tato smlouva nabývá platnosti dnem podpisu smlouvy a účinnosti od 2.1.2017. Uzavírá se na dobu určitou do 31.12.2017.
2. Smluvní strany mohou smlouvu vypovědět kdykoli bez udání důvodu, výpovědní lhůta je 30 dnů ode dne doručení výpovědi druhé straně.

3. Neplnění kteréhokoli ze smluvních závazků poskytovatele se považuje za hrubé porušení smlouvy a uživatel je oprávněn od smlouvy odstoupit bez výpovědní lhůty.
4. Prodlení uživatele s úhradou ceny za technickou podporu delší než tři měsíce se považuje za podstatné porušení smlouvy. Poskytovatel je v tomto případě oprávněn od smlouvy odstoupit.
5. Odstoupením jedné ze smluvních stran smlouva zaniká. Odstoupení od smlouvy musí mít písemnou formu s tím, že je účinné ode dne jeho doručení druhé smluvní straně.
6. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla vedena v evidenci smluv vedené uživatelem, která bude přístupná podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, a která obsahuje údaje o smluvních stranách, předmětu smlouvy, číselné označení této smlouvy a datum jejího podpisu. Smluvní strany rovněž výslovně souhlasí s tím, že tato smlouva podléhá uveřejnění podle zákona č. 137/2006 Sb., o veřejných zakázkách, v platném a účinném znění.
7. Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství, ve smyslu § 504 zákona č. 89/2012 Sb., občanský zákoník, v platném znění a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoli dalších podmínek.
8. 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.
9. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoli v tísni za nápadně nevýhodných podmínek. Autentičnost této smlouvy potvrzují svým podpisem.
10. Tato smlouva je provedena ve třech vyhotoveních, poskytovatel obdrží dvě vyhotovení a uživatel jedno vyhotovení.
11. Nedílnou součástí této Smlouvy jsou následující přílohy:

    Příloha č. 2 – LICENČNÍ PODMÍNKY

    Příloha č. 1 – SPECIFIKACE

    Příloha č. 3 – Etalon bezpečnosti pro smluvní partnery



PŘÍLOHA č. 1 - SPECIFIKACE

I.
Specifikace a cena software

1. Název software, počet licencí a cena technické podpory:

Název	Počet licencí
Stavební úřad	16
Vodoprávní úřad	1
Propojení do GIS	16
Propojení SSL e-Spis	16

Cena technické podpory za jedno čtvrtletí činí 21.196,- Kč.

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

II.
Specifikace a cena dalších služeb

1. Další služby nejsou specifikovány.

PŘÍLOHA č. 2 - LICENČNÍ PODMÍNKY

LICENČNÍ PODMÍNKY

2015-01-15

I. Úvodní ustanovení

1. Počítačové programy (dále jen "software") firmy VITA software s.r.o. (dále jen "poskytovatel") jsou chráněny autorským právem a know-how v nich obsažený tvoří součást obchodního tajemství.
2. Licenční podmínky stanoví, za jakých podmínek může oprávněný uživatel software užívat.

II. Práva a povinnosti uživatele

1. Uživatel je oprávněn užívat software po zaplacení ceny licence.
2. Uživatel není oprávněn software pronajímat, půjčovat nebo jiným způsobem umožnit třetím osobám jeho využití, provádět změny v software, upravovat ho nebo z něj odstranit ochrannou známku autorských práv (copyright).
3. Uživatel je povinen užívat software v souladu s platnými právními předpisy a licenčními podmínkami.
4. Uživatel je povinen při komunikaci s poskytovatelem ohledně implementace a reklamací používat systém HelpDesk.
5. Uživatel má právo na poskytování technické podpory k software na základě samostatně uzavřené smlouvy.

III. Práva a povinnosti poskytovatele

1. Poskytovatel odpovídá za to, že software odpovídá svojí jakostí a provedením účelům, jež jsou uvedeny v dokumentaci, která je součástí dodávky software. Funkčnost software je zaručena v prostředí doporučeném v dokumentaci k software.
2. Poskytovatel neodpovídá za poškození, ztrátu nebo zničení dat, software a hardware způsobené nesprávným užitím nebo nedbalostí uživatele.
3. Zjistí-li poskytovatel vadu software, která může způsobit poškození nebo zničení dat, software nebo hardware nebo může chybnou interpretací dat uvést uživatele v omyl, je povinen neprodleně s tím seznámit uživatele. Pokud tak neučiní, nese odpovědnost za škody, které uživateli v důsledku takové vady vznikly.
4. Poskytovatel nepřejímá odpovědnost za vady propojení software s počítačovými programy jiných poskytovatelů způsobené nesouladem verzí a nesprávnou konfigurací.
5. Poskytovatel je oprávněn po dohodě s uživatelem využívat vzdáleného připojení pro instalaci a řešení nestandardních situací.
6. Poskytovatel se zavazuje poskytovat technickou podporu k software na základě uzavřené smlouvy.

   Technická podpora zahrnuje:

   a. Provádění změn software vyplývajících ze změn obecně platných právních předpisů České republiky a z vývojových změn softwarového prostředí, včetně distribuce upraveného software.
   b. Právo uživatele účasti na schůzkách uživatelů.
   c. Poradenskou službu HotLine pro vyškolené uživatele.
   d. Právo na nákup vyšších verzí software (UPGRADE) za zvýhodněnou cenu (při nepřetržitém odběru technické podpory).
7. Poskytovatel doporučuje uživateli průběžně aktualizovat software. Reklamovat je možné pouze aktuálně distribuovanou verzi software.

IV. Doba trvání licence, porušení licenčních podmínek

1. Licence k software je uživateli poskytována na dobu neurčitou, není-li smluvně domluveno jinak.
2. Instalací aktuální verze software jsou původní licenční podmínky nahrazeny aktuálně platnými licenčními podmínkami poskytovatele.
3. Poskytovatel je oprávněn odstoupit od licenční smlouvy v případě, že uživatel:
   a. neoprávněně pořídí rozmnoženinu software v jakékoli formě, trvalou nebo dočasnou,
   b. provede neoprávněný překlad, zpracování, úpravu či jinou změnu software,
   c. umožní užití software další osobě, včetně pronájmu a půjčování,
   d. neoprávněně využije jakoukoli znalost o myšlenkách a postupech, struktuře, algoritmu nebo použitých metodách, na nichž je software založen nebo které obsahuje, nebo je sdělí jiné osobě,
   e. poruší ustanovení autorského zákona jiným způsobem.
4. V případě zániku smluvního vztahu nemá uživatel nárok na vrácení ceny licence ani její části.

V. Závěrečná ustanovení

1. Licenční podmínky se řídí autorským zákonem a občanským zákoníkem.
2. Licenční podmínky platí přiměřeně i pro dokumentaci k software.

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;
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.