

KUPNÍ SMLOUVA

Č. smlouvy kupujícího: CES 2018 / 1616

Č. smlouvy prodávajícího: 1110/2018

uzavřená dle ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku,
v platném znění

Níže uvedeného dne, měsíce a roku uzavřeli:

1. Městská část Praha 1

se sídlem: Vodičkova 681/18, 115 68 Praha 1
IČO: 00063410
DIČ: CZ00063410
bankovní spojení: Česká spořitelna, pobočka Praha 1
číslo účtu: 27-2000727399/0800
zastoupená: Ing. Oldřichem Lomeckým, starostou městské části Praha 1
(dále jen „**kupující**“ na straně jedné)

a

2. BSS Praha s.r.o.

se sídlem: V Holešovičkách 20, 180 00, Praha 8
IČO: 28207611
DIČ: CZ28207611
bankovní spojení: KB
číslo účtu: 43-1001620257/0100
zastoupená: Petrem Šilovským

zapsaný v obchodním rejstříku u Městského soudu v Praze

(dále jen „**prodávající**“ na straně druhé)

(prodávající a kupující dále též označování jako „**smluvní strany**“)

Kupní smlouvu na dodávku a instalaci elektronické úřední desky

(dále jen „smlouva“)

I. Předmět smlouvy

1. Prodávající se zavazuje dodat kupujícímu nové, plně funkční zboží, dle Přílohy č. 1- Technická specifikace
2. Kupující se zavazuje převzít řádně a včas dodaný předmět koupě za podmínek dále stanovených v této smlouvě a uhradit za něj sjednanou kupní cenu dle čl. II. této smlouvy.

II. Kupní cena a platební podmínky

Celková kupní cena za předmět koupě:

celková kupní cena za předmět bez DPH: 847.000,- Kč

sazba DPH 21% a její celková výše 177.870,- Kč

celková kupní cena za předmět koupě včetně DPH: 1.024.870,- Kč

2. Cena za předmět koupě uvedená v odst. 1 tohoto článku je konečná a maximální a může být měněna pouze v souvislosti se změnou sazeb DPH či jiných daňových předpisů majících vliv na cenu předmětu kupní smlouvy. Rozhodným dnem pro změnu kupní ceny z důvodu zákonné změny sazby DPH je den účinnosti takové změny.
3. Kupní cena bude kupujícím uhrazena v českých korunách na základě řádně a oprávněně vystaveného účetního a daňového dokladu (faktury). Kupní cena bude uhrazena na základě faktury, a to postupem dle čl. III. této smlouvy. Lhůta splatnosti faktury se sjednává na 30 dnů od dne jejího prokazatelného doručení kupujícím. V případě prodlení kupujícího s úhradou faktury se kupující zavazuje uhradit prodávajícímu úrok z prodlení ve výši 0,01 % z příslušné dlužné částky za každý den prodlení.
4. V případě, že faktura nebude vystavena oprávněně, není kupující povinen ji proplatit.
5. Přílohou faktury musí být předávací protokol. Na faktuře budou uvedeny ceny za jednotlivé položky dodaného systému dle požadavku Objednatele
6. Kupní cena bude hrazena bez poskytování záloh.

III. Předání a převzetí předmětu koupě a jeho instalace

1. Předmět koupě bude prodávajícím řádně dodán do 4 týdnů od podpisu smlouvy.
2. Místem předání a převzetí je adresa kupujícího.
3. Při řádném a včasném dodání předmětu koupě bude smluvními stranami sepsán předávací protokol. Teprve podpisem písemného předávacího protokolu oběma smluvními stranami se považuje předmět koupě za řádně dodaný a prodávajícímu vzniká právo na zaplacení celkové kupní ceny dle čl. II. odst. 1 této smlouvy.
4. Kupující není povinen převzít předmět koupě s vadami.
5. Osobou oprávněnou jednat v záležitostech předání a převzetí předmětu koupě a jeho instalace je vedoucí Odboru informatiky [REDAKCE]

IV. Účinnost smlouvy. Odstoupení

1. Tato smlouva nabývá platnosti okamžikem jejího podpisu posledním účastníkem této smlouvy a účinnosti jejím následným zveřejněním v registru smluv
2. Odstoupit od smlouvy lze pouze z důvodů stanovených v této smlouvě nebo zákonem.
3. Kupující má právo odstoupit od této smlouvy:
 - i) neodstraní-li prodávající vadu předmětu koupě ve lhůtě do 30 dnů ode dne reklamace – oznámení vzniku vady kupujícím prodávajícímu nebo oznámí-li prodávající před jejím uplynutím, že vadu neodstraní;
 - ii) jestliže bylo proti prodávajícímu zahájeno insolvenční řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), v platném znění;
 - iii) v případě, že by předmět koupě neměl požadované vlastnosti stanovené dle čl. I. odst. 1 této smlouvy;
4. Odstoupením od smlouvy zanikají všechna práva a povinnosti smluvních stran z této smlouvy. Odstoupení od smlouvy se nedotýká nároku na náhradu škody, nároků na smluvní pokuty, a ty závazky smluvních stran, které dle smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví zákon.

V. Ustanovení o doručování, kontaktní osoby

Smluvní strany se dohodly a prodávající určil, že osobou oprávněnou zastupovat prodávajícího ve všech věcech, které se týkají realizace této smlouvy, je:

jméno: [REDAKCE]
doručovací adresa: BSS Praha s.r.o., V Holešovičkách 1451/20, 180 00 Praha 8
tel: [REDAKCE]
e-mail: [REDAKCE]

Smluvní strany se dohodly a kupující určil, že osobou oprávněnou zastupovat kupujícího ve všech věcech, které se týkají realizace této smlouvy, je:

jméno: [REDAKCE]
doručovací adresa: Městská část Praha 1, Vodičkova 681/18, 115 68 Praha 1
tel: [REDAKCE]
e-mail: [REDAKCE]

2. Veškerá korespondence, pokyny, oznámení, odstoupení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém nebo anglickém jazyce a doručují se buď osobně, nebo doporučenou poštou, k rukám a na doručovací adresy oprávněných osob dle této smlouvy.
3. Má se za to, že došla zásilka odeslaná s využitím provozovatele poštovních služeb došla třetí pracovní den po odeslání, byla-li však odeslána na adresu v jiném státu, pak patnáctý pracovní den po odeslání.
4. Smluvní strany se dohodly, že pro vzájemnou komunikaci může být používána také elektronická pošta; ve věcech týkajících se změny či ukončení účinnosti této kupní smlouvy je však nutné použít doručení prostřednictvím pošty, příp. osobně.
5. Pokud v době účinnosti této smlouvy dojde ke změně adresy některé ze smluvních stran, resp. jejich zástupců dle odst. 1 nebo 2 tohoto článku, je dotčená smluvní strana povinna neprodleně písemně oznámit druhé smluvní straně tuto změnu, a to způsobem uvedeným v tomto článku.

VI. Ustanovení o nabytí vlastnického práva

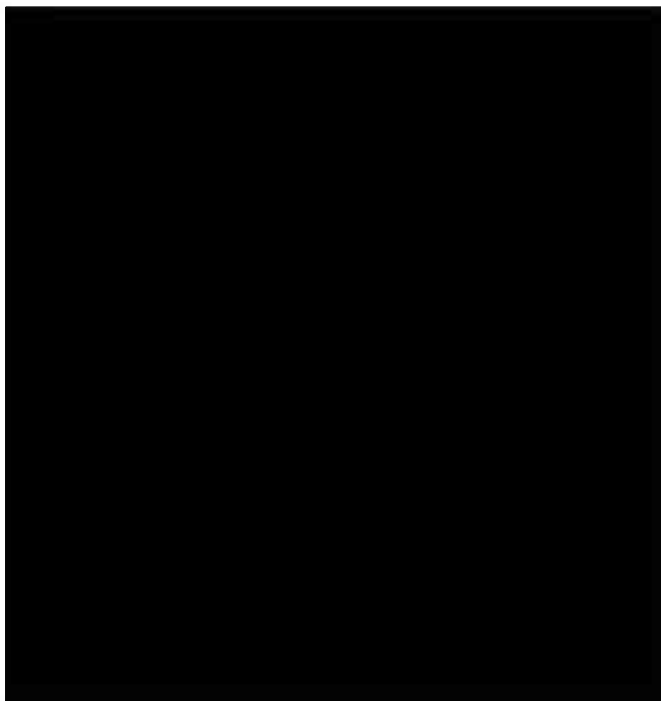
1. Vlastnické právo k předmětu koupě nabývá kupující podpisem předávacího protokolu oběma smluvními stranami dle čl. III. odst. 3 této smlouvy.

VII. Závěrečná ustanovení

- 1 Vztahy mezi smluvními stranami se řídí platným právním řádem České republiky. Ve věcech touto smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, v platném znění a ostatními obecně závaznými právními předpisy.
- 2 Tato Smlouva nabývá platnosti v den podpisu této Smlouvy a účinnosti dnem 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.
- 3 Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla uvedena v Centrální evidenci smluv (CES) vedené zadavatelem, která je veřejně přístupná a obsahuje údaje o smluvních stranách, předmětu Smlouvy, číselné označení této Smlouvy a datum jejího podpisu i v případné evidenci smluv zadavatele.
- 4 Veškeré změny či doplnění této smlouvy lze učinit pouze na základě písemné dohody smluvních stran, přičemž za písemnou formu nebude pro tento účel považována výměna e-mailových či jiných elektronických zpráv. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků smlouvy.
- 5 Prodávající je povinen v průběhu poskytování služby zajistit bezpečnost informací Objednavatele, s kterými přichází do styku anebo se seznámí při poskytování služby. Minimální požadavky Objednavatele na úroveň bezpečnosti informací ze strany Prodávajícího jsou stanoveny v **Příloze č. 2 této smlouvy - v Etalonu minimální bezpečnosti pro smluvní partnery.**
- 6 Smluvní strany budou vždy usilovat o smírné urovnání případných sporů vzniklých ze smlouvy. Pokud nebylo dosaženo smírného urovnání sporu ani do 30 pracovních dnů po jeho prvním oznámení sporné skutečnosti druhé smluvní straně, je kterákoliv ze smluvních stran oprávněna obrátit se se svým nárokem k příslušnému soudu. Smluvní strany si sjednaly, že místně příslušným soudem pro všechny spory vzniklé z této smlouvy je obecný soud kupujícího. Rozhodčí řízení je vyloučeno.
- 7 Kupující prohlašuje, že nemůže nastat změna skutečností, která by plnění předmětu plnění dle této smlouvy podstatně ztěžovala.

Prodávající není oprávněn postoupit jakákoliv práva anebo povinnosti z této smlouvy na třetí osoby bez předchozího písemného souhlasu kupujícího.

- 9 Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s jejím obsahem bez výhrad souhlasí. Smlouva je vyjádřením jejich pravé, skutečné, svobodné a vážné vůle. Na důkaz pravosti a pravdivosti těchto prohlášení připojují oprávnění zástupci smluvních stran své vlastnoruční podpisy.
- 10 Smlouva se vyhotovuje ve dvou stejnopisech, z nichž každý má platnost originálu a každý z účastníků této smlouvy obdrží po jednom stejnopise.
- 11 Smluvní strany prohlašují, že před uzavřením této smlouvy řádně splnily všechny hmotněprávní podmínky pro platné uzavření této smlouvy vyplývající z platných právních předpisů, jakož i z jejich platných vnitřních předpisů, a dále prohlašují, že uzavřením této smlouvy nedojde k porušení jakýchkoliv jejich zákonných či smluvních povinností.
- 12 Podpisem kupujícího na této smlouvě se osvědčuje v souladu s § 43 zák. 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 09.10.2018 usnesením UR18_1159.
- 13 Vzhledem k veřejnoprávnímu charakteru Zadavatele prodávající 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, ve znění pozdějších předpisů a zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).



příloha č. 1 – Technická specifikace

Předmětem realizace této fáze je komplexní dodávka interaktivní úřední desky (dále jen „IUD“), včetně instalace, implementace a integrace. Úpravy dokumentů, zveřejňování a distribuce musí probíhat z jednoho funkčního místa. Preferovaným řešením je integrovat IUD se stávajícím redakčním systémem, aby nedocházelo k duplicitnímu zadávání dat do systému. Systém by měl umožňovat budoucí integraci řešení s dalšími informačními systémy (spisová služba). Umístění IUD je navrhováno tak, aby byly technologie umístěny v budově MČ Praha 1. Řešení IUD musí obsahovat dodávku všech komponent HW a SW pro zajištění komplexní dodávky IUD. Řešení počítá s dodávkou 2 ks IUD včetně SW a 1 ks serverové aplikace pro IUD instalované ve virtuálním serveru umístěném v datovém centru úřadu. Zadavatel požaduje umístění IUD v prosklené výloze u vstupu do úřadu – Vodičkova 681/18, Praha 1. Omezujícím faktorem je šířka výlohy 250 cm. Sklo je zde dvojitě, dtermické, pokovené. Zadavatel nepovoluje jakékoliv průrazy rámu, skel, zdí. IUD musí obsahovat vnitřní designový kryt technologie IUD v souladu s prostředím místnosti, ve které budou umístěny. Zadavatel preferuje systém, který nenárokují nákup nových serverových licencí. Zadavatel dále požaduje, aby pro vnitřní potřeby úřadu generovala IUD knihu úřední desky s kompletními evidenčními šablonami obsahujícími veškeré atributy pro zákonnou evidenci vyvěšených dokumentů a pro jejich snadné zpětné vyhledání.

PLÁNOVANÉ UMÍSTĚNÍ IUD MČ PRAHA 1



Internetovou konektivitu pro připojení IUD k interní síti úřadu zajistí zadavatel. Typ konektivity bude zajištěn na základě konkrétního rozmístění jednotlivých úředních desek. Podle lokality bude zvolen nejdostupnější způsob spojení prostřednictvím počítačové sítě úřadu. Zadavatel dále zajistí ve spolupráci s dodavatelem přístup k webovému serveru a k databázi redakčního systému pro integraci se systémem IUD, a to prostřednictvím interního rozpočtu organizace. Zadavatel požaduje ovládání obrazovky pomocí dotykového panelu pod obrazovkou umístěného ve výšce vhodné pro pohodlné ovládání pro tělesně hendikepované - vozíčkáře. Dotykový panel nesmí zasahovat do obrazovky.

1) Výstup

Zadavatel požaduje vytvoření podrobného návrhu integrace systému, návrh instalace a implementace včetně dodávky celého systému IUD (HW a SW) a grafického návrhu okolí IUD.

2) Požadované výstupy

- návrh řešení,
- dodávka HW a SW pro komplexní řešení IUD,
- vyčítání dokumentů z webové služby,
- automatické zveřejňování el. dokumentu na IUD a internetové úřední desce,

- evidence a archiv zobrazovaných dokumentů,
- obsluha IUD - bezdotyková obrazovka + dotykový panel pod obrazovkou,
- automatické zobrazení dokumentů v požadovaných termínech zveřejnění a expirace,
- funkčnost zobrazování již zveřejněných dokumentů na IUD musí být zajištěna i po výpadku internetu/datové sítě,
- jednoduchá obsluha,
- listování v seznamu vyvěšených dokumentů, tříděných do kategorií a odborů
- výběr dokumentu a jeho zobrazení na displeji,
- možnost zvětšení, případně zmenšení velikosti zobrazení dokumentů,
- výběr dokumentu v úrovních až na detail ve formátu PDF,
- zajištění funkčnosti IUD v případě přerušení datové konektivity,
- v případě nečinnosti obsluhy návrat po stanovené době na úvodní stranu,
- dohled a vzdálená správa,
- zajištění bezpečnosti (fyzické zajištění),
- kompletní hardwarová (fyzická) a softwarová instalace do prostředí zadavatele včetně technické podpory.

3) Specifikace dodávky

- HW + SW IUD,
- 2 ks interaktivních úředních desek,
- instalace, implementace, integrace IUD.

4) Technické parametry

V rámci technických parametrů IUD zadavatel požaduje:

- panel (obrazovka) každé IUD musí mít rozlišení alespoň 1920 x 1080 bodů, jas min. 700 cd/m²,
- Velikost obrazovky na šířku maximálně 110 cm a tomuto rozměru se bude co nejvíce blížit, nejméně však 46 palců.
- ovládání IUD – bezdotyková obrazovka + dotykový panel
- síťové rozhraní – Ethernet 1 Gb,
- HDD s kapacitou min. 750 GB,
- odolnost vůči vnějšímu poškození (tzv. „antivandal“ řešení),
- požadavek nepřetržitého provozu

5) Popis prostředí pro implementaci projektu

Spisová služba - E-Spis, modul E-deska

6) Požadavky na služby:

- záruční a pozáruční servis
- garantovaná servisní dojezdová doba
- dálková diagnostika provozu zařízení

Příloha č. 2 - Etalon minimální bezpečnosti pro smluvní partnery.

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 1. 12. 2014, která byla aktualizována v květnu 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 zkratk:

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 Praha 1	Městská část Praha 1
ÚMČ Praha 1	Úřad městské části Praha 1
SRBI / 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 tak, jak vyplývá z provozní a bezpečnostní dokumentace 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 partneri 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 partneri 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 databázi (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 partneri 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 následně ukončení práce ve vnitřním prostředí systémů MČ Praha 1, ledaže se smluvní strany dohodnou jinak.

5 Bezpečnost IS / IT systémů

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

5.1 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 přihlašovatel 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.

5.2 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 sám „stahovat“ (získávat) žádná data z informačních systémů MČ Praha 1, vytváření souborů dat musí provádět zaměstnanec ÚMČ Praha 1, který následně vytvořená data smí poskytnout, resp. předat smluvnímu partnerovi.
- 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 přes uložisko MČ Praha 1, ke kterému bude smluvnímu partnerovi zřízen přístup.

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

pecifikovaných 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. 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 databázi (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.
- f) Ukončení pracovního poměru pracovníka dodavatele s dodavatelem je dodavatel povinen písemně oznámit odpovědným pracovníkům Odboru informatiky ÚMČ Praha 1 nejpozději 5 pracovních dnů před ukončením tohoto pracovního poměru, přičemž Odbor informatiky ÚMČ Praha 1 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 ÚMČ 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 ÚMČ 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 předemných testů povinna poskytnout přiměřenou součinnost.

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.