[redacted]

Číslo smlouvy poskytovatele: 22/TP/5023 **Číslo smlouvy zákazníka, CES 2022/0899**

Smlouva o aktualizační službě a poskytování podpory při provozu informačního systému iDES

Účastníci smlouvy

Obchodní korporace	**TOM - computer, s. r. o.**
Sídlo	Praha 7 – Bubeneč, Sládkova 476/3, PSČ 17000
Jednající	Ing. Tomáš Huml, jednatel společnosti
IČO	60465832
DIČ	CZ60465832
Bankovní spojení	482684133/0300
Spisová značka	C 26737 vedená u Městského soudu v Praze

Dále „poskytovatel"

	Městská část Praha 1
Sídlo	Vodičkova 18, 11568 Praha 1
Zastoupená	Ing. Petrem Hejmou, starostou
IČO	00063410
DIČ	CZ00063410

Dále „zákazník"

I. Úvodní ustanovení

Smlouva upravuje vztahy mezi poskytovatelem programu iDES a zákazníkem. Smlouva zajišťuje zákazníkovi udržování software iDES neustále v aktuálním stavu, zejména dle platné legislativy (služba legislativního maintenance) a poskytování podpory při provozování IS iDES a jeho dalším rozvoji dle potřeby zákazníka (služby základní a rozšířené podpory).

II. Předmět smlouvy

Předmětem této Smlouvy je poskytování služeb specifikovaných níže v bodě II.1 a II.2 v oblasti správy a podpory k programu iDES poskytovatelem zákazníkovi a závazek zákazníka zaplatit za tyto služby poskytovateli odměnu uvedenou v čl. VI smlouvy.

Předmět smlouvy zahrnuje:

1. základní podporu – služby poskytované paušálně uvedené v bodě II.1 a v přílohách č.1 a č.4 za cenu ve výši 14.400,- Kč bez DPH za měsíc
2. rozšířenou podporu - služby poskytované na vyžádání nad rámec základní podpory uvedené v bodě II.2 v rozsahu maximálně do částky 292.600,- Kč bez DPH za dobu trvaní smlouvy, tj. 36 měsíců.

II.1. Základní podpora

- Průběžná aktualizační služba k programu iDES, licenční číslo 5023 - udržování legislativní, programové, systémové a metodické aktualizace programu iDES (maintenance). Průběžné dodávání nejnovějších verzí aplikace iDES v rozsahu dle zakoupené licence a poskytnutí užívacích práv.
- Instalace nejnovějších verzí iDES na infrastrukturu zákazníka, (zejména prostřednictvím vzdálené správy).
- Poskytnutí průběžné záruky na dodávané verze programu iDES.
- Poskytování služby telefonní konzultační linky a emailové podpory, zejména v souvislosti s ovládáním IS iDES.
- Pravidelná kontrola provozu aplikace iDES, kontrola místa na disku na infrastruktuře zákazníka (serveru), na které je provozování iDES, testovací i produkční prostředí. Kontrola se provádí 1x měsíčně v rozsahu 1 hodiny.
- Pravidelný monitoring provozu informačního systému, 1 x měsíčně v rozsahu 1 hodiny.
- Kontaktní údaje. Tel: 233371205, e-mail adresa: podpora@ides.cz.

II.2. Rozšířená podpora

- Zákazník může na základě písemné nabídky poskytovatele objednat služby, které souvisí s předmětem plnění této smlouvy a nejsou Základní podporou
- Objem těchto služeb je v rozsahu maximálně do částky 292.600,- Kč bez DPH za dobu platnosti této smlouvy.
- Realizace těchto služeb bude zákazníkem písemně objednána a stvrzena akceptačním protokolem, který bude činit povinnou přílohu faktury poskytovatele.
- Tato podpora se může týkat zejména služeb při dalším rozvoji programu iDES. Konzultace, školení, rozšiřování a úpravy funkcionality IS iDES, úpravy dat, analýzy, technická podpora na základě požadavků zákazníka.

III. Způsob a termíny plnění

III.1. Novější verze programu iDES je možno zákazníkovi dodat formou reinstalace prostřednictvím vzdálené správy. Termín dodání novějších verzí bude vždy dohodnut mezi zákazníkem a poskytovatelem.

III.2. Způsob a termíny plnění činností dle bodu II. 2 budou vždy dohodnuty mezi poskytovatelem a zákazníkem a na základě objednávky vystavené oprávněným zástupcem zákazníka.

III.3. Služby a práce dohodnuté v této smlouvě mohou být poskytovány i na pracovišti subjektu určeného zákazníkem (externí správce).

III.4. Poskytovatel poskytuje na provoz programu iDES průběžnou záruku po celou dobu platnosti této smlouvy.

III.5. Zákazník poskytne poskytovateli přístup do IS iDES za účelem plnění předmětu této smlouvy prostřednictví vzdálené správy a součinnost při realizaci služeb dle této smlouvy.

IV. Ochrana informací, mlčenlivost

IV.1. Poskytovatel se zavazuje, že informace, které získá o zákazníkovi při provádění činností podle této smlouvy, a které nejsou veřejně dostupné, bude považovat za důvěrné (dále jen „důvěrné informace").

IV.2. Poskytovatel se zavazuje, že bez předchozího písemného souhlasu zákazníka nezveřejní důvěrné informace, ani je neposkytne či jinak nezpřístupní osobám jiným, než jsou osoby zaměstnané nebo najaté poskytovatelem pro realizaci smlouvy. Poskytování důvěrných informací těmto osobám musí být provedeno pouze v míře potřebné pro realizaci této smlouvy a tyto osoby musí být poučeny o povinnosti ochrany důvěrných informací.

IV.3. Zákazník se zavazuje zabezpečit předané programové vybavení před neoprávněným přístupem nebo manipulací, které mohou mít za následek jeho užití v jiné organizaci bez souhlasu poskytovatele, popřípadě jiný zásah do autorských práv poskytovatele. Bez souhlasu poskytovatele není zákazník oprávněn jakýmkoliv způsobem zasahovat do programového vybavení, provádět jeho změny nebo úpravy ani jej užívat jinak než v souladu s touto smlouvou.

IV.4. Povinnost mlčenlivosti a ochrany důvěrných informací podle smlouvy trvá po dobu účinnosti smlouvy a dále 3 (slovy: tři) roky po jejím ukončení. Vzhledem k veřejnoprávnímu charakteru zákazníka poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen, že žádné ustanovení této smlouvy nepodléhá z jeho strany obchodnímu tajemství a souhlasí se zveřejněním smluvních podmínek obsažených ve smlouvě, včetně jejích příloh a případných dodatků smlouvy za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění.

IV.5. Zákazník se zavazuje, že informace, které získá o poskytovateli při provádění činností podle této smlouvy, a které nejsou veřejně dostupné, bude považovat za důvěrné (dále jen „důvěrné informace").

IV.6. Zákazník a poskytovatel jsou v rámci zpracování osobních údajů vázány Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

V. Sankce

V.1. Nebude-li poskytovatel udržovat v aktuálním stavu potřebnou dokumentaci spojenou s plněním podle této smlouvy je povinen zákazníkovi zaplatit smluvní pokutu ve výši 300,--Kč bez DPH za každé porušení a den prodlení.

V.2. V případě nedodržení termínů dle Přílohy č. 3, tabulka č. 1 je poskytovatel povinen uhradit zákazníkovi smluvní pokutu ve výši 300,- Kč bez DPH za každou započatou pracovní hodinu zákazníka, maximálně však do výše měsíčního poplatku.

V.3. Poruší-li poskytovatel, nebo zákazník kteroukoli povinnost ochrany informací a mlčenlivost uvedenou čl. IV smlouvy, zavazuje se druhé straně uhradit smluvní pokutu ve výši 50.000,--Kč bez DPH za každý jednotlivý případ porušení povinnosti.

V.4. Přístup poskytovatele do prostředí MČP1 je povolen pouze za podmínek stanovených Odborem informatiky ÚMČ Praha 1 a je monitorován. Případné výjimky musí být projednány a schváleny manažerem bezpečnosti informací MČ Praha 1, případně bezpečnostním správcem systému. V případě porušení těchto stanovených podmínek je poskytovatel povinen zákazníkovi zaplatit smluvní pokutu ve výši 2.000,--Kč za každé porušení.

V.5. Uplatněné smluvní pokuty se nezapočítávají do náhrady škody, která zákazníkovi vznikla nedodržením ustanovení této smlouvy či platných zákonů ze strany poskytovatele.

V.6. Smluvní pokuty jsou splatné do 30 dnů ode dne obdržení příslušného vyúčtování.

V.7. Sankci (smluvní pokutu, úrok z prodlení) vyúčtuje oprávněná strana straně povinné písemnou formou. Ve vyúčtování musí být uvedeno to ustanovení smlouvy, které k vyúčtování sankce opravňuje a způsob výpočtu celkové výše sankce.

V.8. Strana povinná se musí k vyúčtování sankce vyjádřit nejpozději do deseti dnů ode dne jeho obdržení, jinak se má za to, že s vyúčtováním souhlasí. Vyjádřením se v tomto případě rozumí písemné stanovisko strany povinné. Nesouhlasí-li strana povinná s vyúčtováním sankce, je povinna písemně ve sjednané lhůtě sdělit oprávněné důvody, pro které vyúčtování sankce neuznává.

VI. Cenová ujednání

VI.1. Cena za předmět smlouvy dle čl. II smlouvy je stanovena dohodou smluvních stran a podrobně uvedena v Příloze č. 1 této smlouvy. Výše ceny je stanovena ke dni uzavření smlouvy a jakákoliv změna je možná pouze písemnou dohodou smluvních stran, není-li výslovně stanoveno jinak. Veškeré ceny podle této smlouvy jsou uvedeny v českých korunách.

Celková cena v Kč bez DPH	811.000,-- Kč
(zákonné DPH)	170.310,-- Kč
Celková cena v Kč včetně DPH	981.310,-- Kč

VI.2. Cena uvedená v tabulce se skládá ze základní a rozšířené podpory dle čl. II. smlouvy a blíže specifikovaná v Příloze č. 1 této smlouvy.

VI.3. Fakturace za služby dle této smlouvy bude prováděna měsíčně, vždy k poslednímu dni v měsíci za daný kalendářní měsíc na základě zákazníkem odsouhlaseného a podepsaného výkazu o poskytnutých službách (tzv. akceptační protokol), který obsahuje zhodnocení kvalitativních parametrů poskytnuté služby za uplynulý měsíc. Akceptační protokol bude podepsán

oprávněnými osobami dle čl. VII této smlouvy, vždy nejpozději do 10. dne následujícího kalendářního měsíce. Akceptační protokol bude rovněž přílohou daňového dokladu. Faktury bude poskytovatel zasílat zákazníkovi elektronicky na jeho e-mailovou adresu posta@praha1.cz.

VI.4. Splatnost faktur je do 30 dnů od ode dne jejich vystavení, není-li dohodnuto jinak.

VI.5. V případě prodlení zákazníka s placením daňových dokladů, má poskytovatel nárok účtovat úrok z prodlení ve výši 0,05% z dlužné částky za každý den prodlení.

VI.6. Všechny ceny jsou uvedeny bez daně z přidané hodnoty. K uvedeným cenám bude připočtena daň z přidané hodnoty dle platných sazeb DPH na základě právních předpisů aktuálně platných v zúčtovacím období.

VI.7. Všechny faktury musí mít veškeré náležitosti daňového dokladu a na faktuře bude jako číslo objednávky uvedeno č. smlouvy CES zákazníka.

VI.8. Ceny za jednotlivá plnění jsou uvedeny v Příloze číslo 1, která je nedílnou součástí této smlouvy.

VI.9. V případě, že poskytovatel neplní smluvní ujednání řádným způsobem a v dohodnutém čase, může zákazník požadovat smluvní pokutu ve výši 0,05% z paušální měsíční částky za každý den prodlení.

VI.10. Vzhledem k možné inflaci je poskytovatel po celou dobu účinnosti smlouvy oprávněn každoročně, vždy nejdříve od 1. dne 3. měsíce zvýšit ceny služeb dle článku II. a přílohy č. 1 o hodnotu meziroční inflace, kterou pro daný rok stanoví Český statistický úřad na základě přírůstku indexu spotřebitelských cen předchozího kalendářního roku v České republice. Uvedená změna bude realizována uzavřením dodatku k této smlouvě.

VII. Oprávněné osoby a zásady komunikace

VII.1. Veškerá komunikace probíhá zásadně v českém jazyce.

VII.2. Oprávněný zástupce poskytovatele:

ve věcech smluvních: [redacted]

ve věcech technických:

VII.3. Oprávněný zástupce zákazníka:

ve věcech smluvních:

- [redacted]

ve věcech technických

- [redacted]
-
-

VIII. Pojištění

Poskytovatel se zavazuje, že po celou dobu poskytování svých služeb podle této smlouvy bude pojištěn pro případy škody vyplývající z výkonu svojí podnikatelské činnosti na částku předmětného pojištění alespoň 1 (jednoho) milionu Kč s maximální spoluúčastí 10 % a udržovat pojištění v platnosti po celou dobu platnosti této smlouvy.

IX. Platnost a účinnost smlouvy

IX.1. Smlouva se uzavírá na dobu určitou v trvání 36 měsíců od 1. 10. 2022.

IX.2. Tato smlouva nabývá platnosti v den podpisu této smlouvy poslední stranou 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.

X. Zánik smlouvy

X.1. Tato smlouva primárně zaniká uplynutím doby, na kterou je uzavřena. Před uvedeným datem smluvní strany dále mohou ukončit smluvní vztah písemnou dohodou obou smluvních stran. Konečně, tato smlouva může zaniknout i jednostrannou výpovědí či odstoupením od smlouvy.

X.2. Zákazník je oprávněn odstoupit od této smlouvy s okamžitou platností :

- v případě, že probíhá insolvenční řízení proti majetku poskytovatele, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek poskytovatele byl zcela nepostačující;
- v případě opakovaného překročení stanovených SLA (Příloha č. 3, tabulka č. 1) o 100 % poskytovatelem

X.3. Poskytovatel je oprávněn odstoupit od této smlouvy s okamžitou platností pokud:

- je zákazník v prodlení s úhradou ceny déle než 90 dní,
- zákazník poruší autorské právo ve vztahu k předmětu této smlouvy.

X.4. Odstoupení od smlouvy musí být učiněno písemným oznámením o odstoupení od této smlouvy druhé straně, účinky odstoupení nastávají dnem doručení oznámení druhé straně.

X.5. Zákazník i poskytovatel může vypovědět tuto smlouvu kdykoliv po jejím podpisu bez udání důvodu, a to písemnou výpovědí s 3 (tříměsíční) výpovědní lhůtou. Výpovědní lhůta začíná běžet 1. kalendářní den měsíce následujícího po doručení výpovědi druhé smluvní straně.

X.6. Smluvní strany jsou oprávněny od této smlouvy dále odstoupit za podmínek stanovených občanským zákoníkem nebo jinými právními předpisy.

X.7. Strany se dohodly, že po ukončení smlouvy trvají a zůstávají v platnosti ujednání stran týkající se odpovědnosti za vady, záruk za jakost a záruční lhůty, smluvních pokut, náhrady škody a cenová ujednání obsažená v této smlouvě.

XI. Další ujednání

XI.1. Veškeré programové vybavení poskytované dle této smlouvy podléhá autorskoprávní ochraně.

XI.2. Zákazník má právo na bezplatné odstranění vady způsobené chybným zásahem poskytovatele.

XI.3. Pokud není v této smlouvě stanoveno jinak, řídí se práva a povinnosti smluvních stran, jakož i právní poměry z ní vyplývající, nebo vznikající právními předpisy, zejména zákonem o obchodních korporacích a autorským zákonem.

XI.4. Poskytovatel je povinen při provádění závazků dle této smlouvy zajistit, aby k datům zákazníka neměly přístup neoprávněné třetí osoby a aby nedocházelo k neoprávněným zásahům do dat zákazníka či k jejich zneužití či změně. Poskytovatel bere na vědomí, že na data zákazníka se vztahují ustanovení zákona č. 110/2019 Sb. o zpracování osobních údajů. Poskytovatel se zavazuje zachovávat v tajnosti a nevyužívat ve svůj prospěch či ve prospěch třetích osob informace a data, které mají důvěrný charakter (důvěrná data).

XI.5. Veškeré informace a data obou smluvních stran, s nimiž přišly smluvní strany do styku při plnění této smlouvy, jsou považovány za důvěrné. Veškeré skutečnosti osobní, úřední, obchodní, ekonomické či technické povahy související se smluvními stranami, které nejsou běžně dostupné a se kterými při plnění smlouvy přijdou smluvní strany do styku, jsou podle své povahy obchodním tajemstvím podle § 504 občanského zákoníku nebo utajovanými skutečnostmi, osobními či citlivými údaji podle zákona č. 110/2019 Sb. o zpracování osobních údajů a znění některých zákonů případně údaji, které jsou předmětem povinnosti mlčenlivosti podle zvláštních zákonů.

XI.6. Poskytovatel je povinen v průběhu poskytování služby zajistit bezpečnost informací zákazníka, s kterými přichází do styku a/nebo se seznámí při poskytování služby. Minimální požadavky Zákazníka na úroveň bezpečnosti informací ze strany Poskytovatele jsou stanoveny v příloze č. 2 této smlouvy – „Etalon minimální bezpečnosti pro smluvní partnery"

XI.7. Smluvní strany se zavazují, že jiným subjektům tyto skutečnosti nesdělí, nezpřístupní a nepoužijí je ke svým vlastním účelům nebo účelům ostatních stran. Veškeré získané informace této povahy podrží smluvní strany v tajnosti a omezí jejich sdělení pouze na ty zaměstnance, kteří jsou oprávněni v souvislosti s obsahem a předmětem smlouvy tyto informace mít.

XI.8. V případě porušení obchodního tajemství ve smyslu ust. § 2985 občanského zákoníku, smluvní strany použijí prostředky právní ochrany proti nekalé soutěži. Smluvní strany se zavazují dodržet právo na ochranu obchodního tajemství po dobu platnosti této smlouvy a další 3 (slovy tři) roky po jejím ukončení

XI.9. Podmínky smlouvy lze měnit pouze dohodou, formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, vyjma příloh této smlouvy.

XI.10. Zákazník se zavazuje uzavřít s poskytovatelem dodatek ke smlouvě v případě nasazení/zprovoznění těchto modulů do provozu - modul IR iDES, vazba na insolvenční

rejstřík, modul Spis dlužníka, modul EDD, elektronická distribuce dokladů s tím, že základní podpora (paušální za 1 měsíc) bude navýšena o částku 5.300,- Kč bez DPH. Uvedené moduly jsou dodány a nainstalovány. Nasazením/zprovozněním uvedených modulů do provozu se rozumí zahájení využívání těchto modulů uživateli po předcházejícím proškolení uživatelů. O nasazení/zprovoznění bude sepsán akceptační protokol podepsaný smluvními stranami.

XI.11. Tímto se osvědčuje v souladu s ustanovením § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, v platném znění, že návrh na uzavření této smlouvy byl projednán a schválen Radou městské části Praha 1 dne 20. 9. 2022 usnesením č. UR22_1161

XI.12. Smlouva se vyhotovuje ve dvou stejnopisech, z nichž každý má platnost originálu, a každá ze smluvních stran obdrží po jednom paré.

XI.13. Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha 1 - Podrobná specifikace ceny
Příloha 2 - Etalon minimální bezpečnosti pro smluvní partnery
Příloha 3 - Stanovení SLA
Příloha 4 - Seznam licencí a modulů dotčených touto smlouvou
Příloha 5 - Technický popis prostředí informačního systému iDES
Příloha 6 - Prohlášení o výlučnosti

V Praze dne:
Za poskytovatele:

V Praze dne: 05 -10- 2022
Za zákazníka:

[redacted]

[redacted]

Příloha číslo 1 – Podrobná specifikace ceny:

Popis služby	Cena v Kč bez DPH	Cena v Kč včetně DPH
A. Základní podpora (paušální) za 1 měsíc	14.400,-Kč	17.424,-Kč
B. Rozšířená podpora, (nepovinná)		
Konzultace, školení, rozšiřování a úpravy funkcionality IS iDES, úpravy dat, analýzy, technická podpora - cena za 1 hodinu	1.625,- Kč	1966,25 Kč
Hromadné školení 3 a více osob – cena za 1 osobu za 1 blok (0,5 dne)	2200,- Kč	2662,- Kč

Celková cena za dobu trvání smlouvy v délce 36 měsíců je :

Základní podpora za 36 měsíců v Kč bez DPH	518.400,-- Kč
Rozšířená podpora za 36 měsíců v Kč bez DPH	292.600,-- Kč
Celková cena v Kč bez DPH	811.000,-- Kč
(zákonné DPH)	170.310,-- Kč
Celková cena v Kč včetně DPH	981.310,-- Kč

Příloha č. 2 - Etalon bezpečnosti pro smluvní partnery (dokument Prahy 1)

1 Účel a cíle

Etalon minimální bezpečnosti informací pro poskytovatele 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 poskytovatele MČ Praha 1 se na některých místech odkazuje na platné dokumenty o ICT a o bezpečnosti informací na MČ.
Používané i nově zaváděné informační systémy v rámci MČ Praha 1 musí být upraveny, vyvíjeny nebo vybírány tak, aby splňovaly zásady bezpečnosti informací v souladu s tímto dokumentem a se základním dokumentem pro bezpečnost informací MČ Praha 1, tj. Politikou bezpečnosti informací MČ Praha 1 ze dne 6. 11. 2018.

Cílem etalonu minimální bezpečnosti pro smluvní partnery obecně je:

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

Výklad použitých zkratek:

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

2 Bezpečnost informací

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

3 Obecné povinnosti

Mezi odpovědnosti smluvních partnerů patří zejména:

a) Dodržování platných právních předpisů ČR k zajištění bezpečnosti informací;
b) Využívání informačních systémů MČ Praha 1 a jejich komponent v souladu s provozní a bezpečnostní dokumentací MČ Praha 1;
c) Používání informačních aktiv a ostatních aktiv MČ Praha 1 pouze v souladu s určeným rozsahem přístupových oprávnění a pouze ke schváleným účelům;
d) Zajištění ochrany autentizačních údajů (login, heslo, identifikační předmět) k informačním systémům a zařízením MČ Praha 1, které byly smluvnímu partnerovi svěřené, příp. těch, ke kterým má přístup při naplňování smluvního vztahu;
e) Odpovědnost za každý přístup k informačním aktivům a dalším aktivům, provedený prostřednictvím jejich autentizačních údajů;
f) Respektování a dodržování všech bezpečnostních opatření, pravidel a procedur, stanovených vlastníkem informací, tj. MČ Praha 1, se kterými partnera vlastník informací prokazatelně seznámí;
g) Odpovědnost za dostatečné proškolení svých zaměstnanců a pracovníků svých subposkytovatelů v oblasti zajištění bezpečnosti informací MČ Praha 1;
h) V případě vzniku bezpečnostního incidentu přijmutí nezbytných opatření k eliminaci dopadů tohoto incidentu a neprodlené informování MČ Praha 1.

3.1 Poskytování informací třetím stranám

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

4 Bezpečnost HW, SW a komunikací

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

4.1 Koncové pracovní stanice

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

a) Použití koncového zařízení (počítače) musí být umožněno pouze oprávněné osobě; (Osoba oprávněná k použití koncového zařízení musí být vybavena přístupovými oprávněními.)
b) Je zakázáno připojovat soukromé počítače do vnitřní sítě MČ Praha 1 bez vědomí oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;

c) Koncová zařízení (pracovní stanice, NTB) nesmí být ponechána bez dozoru zapnutá a s přihlášeným uživatelem (k aplikaci, k IS); za minimální opatření se považuje „uzamčení" pracovní stanice (v každém případě je třeba minimalizovat možnost fyzického přístupu neoprávněným osobám);
d) Počítače smluvního partnera, které mají být připojeny do vnitřní sítě ÚMČ Praha 1, musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databází virových definic (tento antivirový program by měl být v maximální míře aktualizován vůči všem známým virům). Dále je smluvní partner též zodpovědný za pravidelnou aktualizaci operačních systémů na těchto svých počítačích;
e) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému.

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

4.2 Využívání prostředků a internetu

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

Smluvní partneři mají povoleno používání internetového připojení do a z vnitřní sítě MČ Praha 1 pouze za účelem plnění pracovních záležitostí v rozsahu smluvního vztahu. Způsob připojení a autentizace musí být předem dohodnuty s Odborem informatiky ÚMČ Praha 1.

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

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 přihlašovateli poskytnuta informace, kde je chyba v přihlašovacích údajích;
e) V případě, že je povolen přístup do aplikace či informačního systému, který nepřebírá přihlašovací údaje z Active Directory MČ Praha 1, a v němž iniciační (vstupní) heslo určuje administrátor, měl by informační systém či aplikace vynutit změnu tohoto iniciačního hesla při prvním přihlášení uživatele;
f) Všichni uživatelé by měli při své činnosti používat jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti;
g) Každý pracovník na straně smluvního partnera, který pracuje s informačním systémem či aplikací, musí používat svůj vlastní přihlašovací identifikátor. (Smluvní partner tedy nemůže používat jeden

přihlašovací identifikátor pro několik svých zaměstnanců.) Dále smluvní partner odpovídá za veškeré úkony provedené v aplikaci či informačním systému pracovníkem přihlášeným pod tímto identifikátorem;

h) Systém správy hesel by měl být podpořen efektivním a interaktivním vybavením, které prosazuje a vynucuje požadovanou kvalitu hesel;
i) U každého uživatele systému musí být možné identifikovat, jaká přístupová práva má přidělena;
j) Pro každý prostředek systému musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku, s rozlišením druhu přístupových práv (čtení, zápis, editace, ...);
k) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo celé skupině uživatelů.

5.2 Monitorování používání systému a přístupu k systému

Přístup poskytovatele do prostředí MČP1 je povolen pouze za podmínek stanovených Odborem informatiky ÚMČ Praha 1 a je monitorován. Případné výjimky musí být projednány a schváleny manažerem bezpečnosti informací MČ Praha 1, případně bezpečnostním správcem systému.
V informačním systému (případně v jeho jednotlivých součástech) musí být pořizovány auditní záznamy. Tyto záznamy by měly obsahovat údaje a informace, které jsou nezbytné k identifikaci aktivit sledovaného uživatele (jeho identifikační údaje, datum a čas přihlášení a odhlášení apod.)

6 Bezpečnost informací a dat

6.1 Kontrola správnosti dat

Data vstupující do systémů musí být kontrolována tak, aby byla zajištěna jejich maximální správnost. V aplikaci by se měl evidovat identifikátor uživatele nebo procesu, který pořízení nebo změnu dat provedl.
Pokud bude usouzeno, že vytvářený informační systém nebo aplikace by měla podporovat (využívat) kryptografické prostředky pro zajištění integrity dat, je nezbytné, aby aplikované prostředky byly podporovány mezinárodně uznávanými standardy a byly dodrženy právní předpisy České republiky.

6.2 Data / informace předávané smluvním partnerům

Jedná se o informace předávané MČ Praha 1 smluvnímu partnerovi na jakémkoliv nosiči a v jakékoliv formě, zejména listiny a dokumenty, CD ROM, Flash disky, pevné disky, nebo informace zaslané emailem.
Dále se jedná o jakékoliv informace a data MČ Praha 1, se kterými se smluvní partner seznámí nebo k nim má přístup na základě realizace činností prováděných v rámci smluvního vztahu.
Smluvní partner musí s informacemi nakládat v souladu s následujícími ustanoveními tohoto dokumentu, pokud není smlouvou stanoveno jinak:

a) Předání, resp. poskytnutí nebo přístup k informacím (datům) musí být vymezeno ve smlouvě (struktura dat, způsob předání/ poskytování, způsoby ochrany, ...) a musí probíhat řízeným a bezpečným způsobem;
b) Uchovávání a případné zpracovávání dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana dle pravidel stanovených v bezpečnostní dokumentaci MČ Praha 1 (se kterými byl smluvní partner prokazatelně seznámen). Uchovávání a zpracování dat musí být ochráněno před neoprávněným přístupem a možným zneužitím – v souladu s bezpečnostními požadavky MČ Praha 1;
c) Zodpovědnost za ochranu informací (dat) má smluvní partner;
d) Informace (data), která již nejsou potřeba pro účely vymezené smluvním vztahem, musí být smluvním partnerem bezpečně zlikvidována, včetně jejich nosičů. Pro likvidaci nosičů obsahující neveřejné informace MČ Praha 1 musí být zvolena metoda, zaručující, že takto zlikvidované informace (data) nelze běžně dostupnými prostředky obnovit (např. skartovače, SW skartovače dat, ...); provedení likvidace doloží partner protokolem o jejich zlikvidování;

e) Každé nové předání informací (dat) nebo zřízení dálkového přístupu k informačnímu systému nebo databázi na smluvním základě musí být konzultováno s manažerem bezpečnosti informací MČ Praha 1, případně s bezpečnostním správcem systému MČ Praha 1;
f) Smluvní partner si nesmí bez písemného souhlasu MČ Praha 1 sám „stahovat" (získávat) žádná data z informačních systémů MČ Praha 1. Data může uchovat pouze po nezbytně nutnou dobu.
g) Informace (data), která jsou součástí řešení, vytvářeného smluvním partnerem, nebo jsou předávána na základě realizace činností prováděných partnerem v rámci smluvního vztahu, se budou předávat pouze na vyžádání oprávněného pracovníka MČ Praha 1.

7 Pravidla pro vzdálený přístup do informačního systému

Vzdálený přístup do informačního systému je poskytován výhradně smluvnímu partnerovi, resp. pracovníkům smluvního partnera a nelze ho dále převádět na jiné osoby, a to ani z části. Porušení této povinnosti je považováno za závažné porušení smlouvy.
Smluvní partner se zavazuje, že vzdálený přístup do informačního systému bude používat výhradně za účelem konání prací specifikovaných ve smlouvě. Porušení této povinnosti je považováno za závažné porušení smlouvy.
Smluvní partner, resp. pracovníci smluvního partnera, jsou povinni dodržovat pravidla pro vzdálený přístup do informačního systému (bod 7.1). Porušení jakékoli povinnosti uvedené v těchto pravidlech se považuje za závažné porušení smlouvy.

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

a) Pracovník poskytovatele, za účelem zřízení vzdáleného přístupu do informačního systému a možnosti se do tohoto systému přihlásit a pohybovat se v něm, obdrží e-mailem od pracovníka informatiky MČ Prahy 1 přihlašovací jméno, certifikát a prostřednictvím SMS zprávy heslo, které je z důvodu bezpečnosti generované a pracovník poskytovatele ho musí změnit za bezpečné heslo. Pracovník poskytovatele 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 poskytovatele vždy povinen se odhlásit.
d) Pracovník poskytovatele musí dodržovat pravidla bezpečnosti práce na svém počítači (stolní PC, notebook), ze kterého realizuje vzdálený přístup do informačního systému. Tento počítač musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databází (tento antivirový program by měl být v maximální míře aktualizován vůči všem známým virům). Dále musí tento počítač mít aktualizovaný operační systém a další obslužný SW.
e) Pracovník poskytovatele se nesmí pokoušet přistupovat na jiné servery než ty, které mu byly přiděleny v rámci vykonávaných smluvních prací, aktivita na účtě může být monitorována.
f) Ukončení pracovního poměru pracovníka poskytovatele s poskytovatelem je poskytovatel povinen písemně oznámit odpovědným pracovníkům Odboru informatiky ÚMČ Praha 1 nejpozději 5 pracovních dnů po ukončení tohoto pracovního poměru, přičemž Odbor informatiky ÚMČ Praha 1 je oprávněn vzdálený přístup do informačního systému pracovníkovi poskytovatele bez dalšího s okamžitou platností zrušit, při neoznámení této skutečnosti nese poskytovatel plnou zodpovědnost za činnost tohoto bývalého pracovníka.
g) V případě, že pracovník poskytovatele poruší kterékoli ujednání těchto pravidel, je Odbor informatiky UMČ Praha 1 oprávněn okamžitě po zjištění porušení těchto pravidel zrušit tomuto pracovníkovi poskytovatele vzdálený přístup do informačního systému bez dalšího. Poskytovatel 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 poskytovatele, a o této výměně neprodleně písemně informovat Odbor informatiky ÚMČ Praha 1, přičemž tato výměna podléhá schválení Odborem informatiky ÚMČ Praha 1.

Vzdálený přístup poskytovatele 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 poskytovatele 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 poskytovatele a po schválení Odborem informatiky UMČ Praha 1.

8 Bezpečnost dodávek a služeb

8.1 Vývoj software, informačních systémů a jejich modulů

Vývoj SW a informačních systémů musí probíhat:

a) s využitím legálního software;
b) na testovacím prostředí odděleném od prostředí produkčního. Za vytvoření softwarové složky testovacího prostředí v rozsahu své dodávky odpovídá smluvní partner, za vytvoření ostatních částí testovacího prostředí a jeho bezpečnost odpovídá MČ Praha 1;
c) na testovacích datech, která nejsou převzata z provozní databáze; za testovací data je odpovědný smluvní partner. Pokud je nutné použít data z provozní databáze, je nutné je předem anonymizovat, přičemž za anonymizaci těchto dat odpovídá MČ Praha 1. Za bezpečnost testovacích dat v rozsahu smluvně dohodnutých pravidel odpovídá smluvní partner;
d) tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení těchto testů.

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

8.2 Dodávky software a hardware

a) Dodávka software (SW) a hardware (HW) musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována;
b) U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený SW, nebo SW podléhající licenční nebo registrační politice;
c) Dodávka licenčního SW musí zahrnovat jasná pravidla pro vydávání a používání licencí, včetně jejich evidence;
d) O každé dodávce musí existovat kromě účetních dokladů také předávací protokol o řádném dodání a instalaci; podepsaný poskytovatelem 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 poskytovatel daného SW/HW, přičemž MČ Praha 1 je při provádění předmětných testů povinna poskytnout přiměřenou součinnost.
f) Správce HW (případně MČP1) je povinen na příslušném fyzickém či virtuálním serveru, na kterém je SW/aplikace Poskytovatele (pro niž je správcem) provozována, zajišťovat pravidelné aktualizace příslušného operačního systému běžícího na tomto serveru. V případě, že po aktualizaci operačního systému je SW/aplikace nefunkční nebo vykazuje chyby, je Poskytovatel SW/aplikace povinen zajistit odstranění chyb a plnou funkčnost SW/aplikace.

8.3 Dodávky služeb a ostatní služby

a) Dodávka služeb musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována ze strany poskytovatele i zákazníka;
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 zákazníka, tj. MČ Praha 1;
c) Poskytovatel 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 poskytovatele, příp. subposkytovatelů, 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 subposkytovatelů 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 subposkytovateli, 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.

Příloha číslo 3- Stanovení SLA:

1. **Poskytování nových verzí Informačního systému a opravných patchů dle článku II. 1.1. Smlouvy zahrnuje následující činnosti:**

   - poskytování aktualizací a nových verzí Informačního systému včetně dokumentací k těmto aktualizacím a novým verzím;
   - poskytování opravných patchů nutných pro bezchybný chod Informačního systému.

   Zákazník má nárok na veškerá zlepšení a dodatky k Informačnímu systému (update nebo upgrade Informačního systému) vydané během účinnosti této Smlouvy. Součástí poskytnutí těchto upgrade a update není jejich implementace u zákazníka (vyjma poskytnutí nezbytné součinnosti), ani rozdílové školení, pokud bude potřeba s ohledem na rozsah upgrade či update.

   Update se rozumí aktualizace Informačního systému formou opravných patchů, zohledňující většinou chyby nebo bezpečnostní mezery, které u předcházející verze nebyly známé) včetně dokumentace zahrnující popis změn.

   Upgrade se rozumí vylepšení (optimalizace) dosavadního Informačního systému na vyšší výkonnost a nové funkce v rámci poskytnuté licence včetně dokumentace zahrnující popis změn.

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

   Poskytovatel bude provádět správu systémů včetně průběžných aktualizací nových verzí. Před započetím aktualizace nahlásí poskytovatel na e-mail kontaktní osobě informaci o distribuci nové verze a sdělení termínu instalace aktualizace. Zákazník, resp. kontaktní osoba, před zahájením aktualizace odsouhlasí termín. Poskytovatel je povinný před aktualizací programového vybavení požádat zákazníka o zajištění zálohy programového vybavení.

2. **Služby dle článku II. 1.2.**

   Pro účely této Smlouvy je pro vyžádání Služeb poskytovaných poskytovatelem a podchycení komunikace oprávněných osob poskytovatele a zákazníka zřízeno komunikační centrum Hotline s garantovanou reakcí ze strany poskytovatele. Služba HotLine zahrnuje zejména přijímání dotazů či požadavků ze strany zákazníka týkající se aplikační části Informačního systému a prostředí, ve kterém je provozován, jejich vyhodnocení a zajištění jejich vyřešení v souladu s touto Smlouvou. Komunikační centrum HotLine je realizováno pomocí určené telefonní linky, 233371205 a e-mailové adresy poskytovatele - podpora@ides.cz.

   Dostupnost služby HotLine

Poskytovatel je povinen reagovat na požadavky zákazníka pouze v pracovní dny v době od 8.30 do 16.30 hodin (dále jen „Pracovní doba"). Pracovním dnem se rozumí pondělí až pátek (dále jen „Pracovní den"), Pracovními dny nejsou soboty, neděle, státní svátky a ostatní svátky dle zákona č. 245/2000 Sb., o státních svátcích, o ostatních svátcích, o významných dnech a o dnech pracovního klidu, ve znění pozdějších předpisů.
Komunikační centrum HotLine je pro zákazníka telefonicky dostupná v Pracovní době, elektronicky lze předkládat požadavky 7 dní v týdnu, 24 hodin denně.

Reakce poskytovatele
Poskytovatel je povinen potvrdit přijetí požadavku zákazníka ve lhůtě 1 hodin. V případě vady Informačního systému je součástí přijetí požadavku ze strany Poskytovatele předběžná klasifikace vady a stanovení požadavků na součinnost zákazníka.

Kategorie vad:

Pro účely této Smlouvy jsou vady kategorizovány takto:

(i) **Vady kategorie A:**
Jedná se o stav, kdy jsou více než jednomu uživateli nedostupné funkce Informačního systému nebo jeho částí, nebo hrozí poškození dat, nebo je znemožněno provádění hromadných operací, nebo je znemožněno provést operaci, nebo nebude možné z důvodu vady zpracovat v požadované lhůtě výstup stanovený zákonem.

(ii) **Vady kategorie B:**
Jedná se o vadu, jejíž povaha neodpovídá podmínkám kategorie A nebo C.

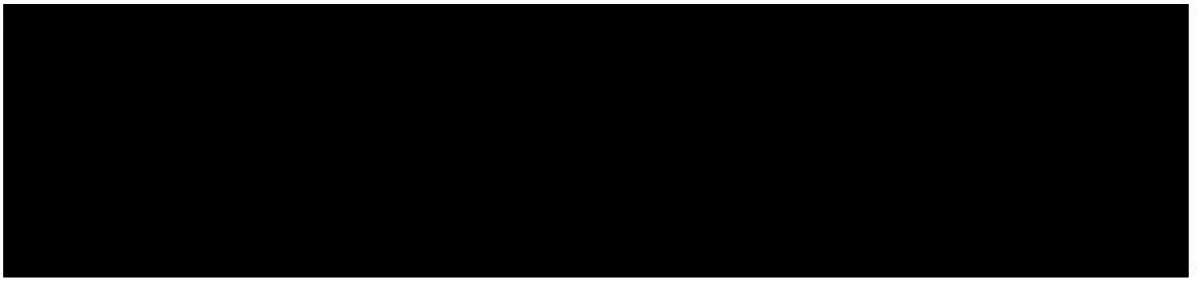
(iii) **Vady kategorie C:**

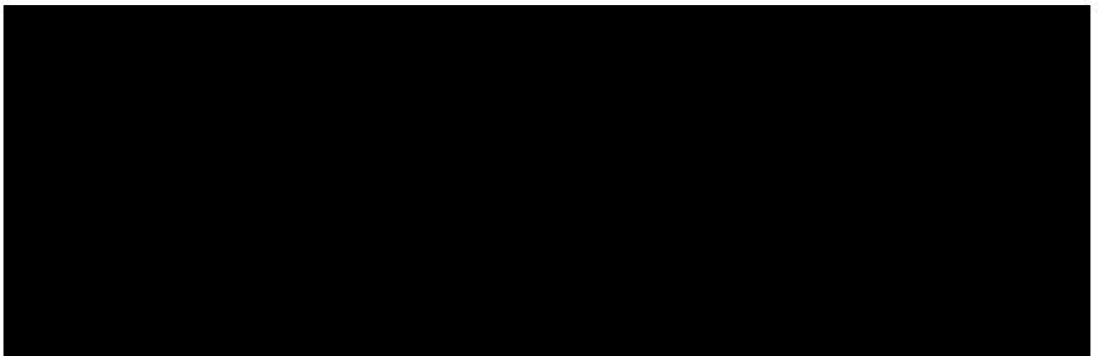
Informační systém vykazuje drobnější vady nebo je podezření na vadu, ale základní funkčnost Informačního systému nebo jeho dílčí části je zachována.

Zákazník oznámí (ohlásí) vadu poskytovateli prostřednictvím služby HotLine s označením kategorie vady. Jestliže zákazník neoznačí kategorii vady, má se za to, že se jedná o vadu kategorie C.

Příloha č.4 – Seznam licencí a modulů dotčených touto smlouvou

IS iDES je dodán v rozsahu s omezením do 4000 nájemních jednotek a bez omezení počtu uživatelů.
IS iDES se skládá z následujících modulů:
Modul Pasport iDES
Modul Nájemné iDES
Modul Vlastníci iDES
Modul Vyúčtování služeb iDES
Modul Účetnictví iDES
Modul Export do SAP
Modul Export do Ginis
Modul VNO, převod nákladů
Modul vazba na ENO (PROXIO)
Modul vazba na CES (PROXIO)
Modul Speciálních funkcionalit P1





Příloha č. 6 - Prohlášení o výlučnosti

Poskytovatel **TOM - computer, s. r. o.**, IČO: 60465832, zastoupený Ing. Tomášem Humlem, jednatelem společnosti, čestně prohlašuje, že je výlučným majitelem a jediným poskytovatelem programového vybavení, které je předmětem plnění této smlouvy.

V Praze dne: