Dodatek č. 1
Ke Smlouvě o poskytování služeb outsourcingu informačních technologií v režimu vertikální spolupráce

uzavřené v souladu s ustanovením § 1746 odst. 2 občanského zákoníku č. 89/2012 Sb. (dále jen „smlouva"), mezi těmito smluvními stranami:

(dále jen „dodatek")

Smluvní strany

Město Žďár nad Sázavou
Žižkova 227/1, 591 01 Žďár nad Sázavou
IČ: 00295841
DIČ: CZ00295841
[redacted]
Zastoupené: Ing. Martin Mrkos, ACCA, starosta města
(dále jen „zadavatel")

a

SATT a.s.
Okružní 1889/11, 591 01 Žďár nad Sázavou
Spisová značka B 1592 vedená u Krajského soudu v Brně
IČ: 60749105
DIČ: CZ60749105
[redacted]
Zastoupená: Ing. Petr Scheib, MBA, prokura
(dále jen „poskytovatel")

Obsah dodatku
Čl. 1.

1.1. Smluvní strany se dohodly na změně smlouvy o poskytování outsourcingu informačních technologií v režimu vertikální spolupráce uzavřené dne 30. 12. 2021 na základě schválení radou města na své schůzi dne 20. 12. 2021 usnesením č.j. 842/2021//RM.
1.2. V čl. 4., odstavci 4.1 se doplňuje bod I. Zajištění role Architekta KB a Správce ICT
1.3. V čl. 4., odstavci 4.1 se doplňuje bod J. Zajištění pohotovostní služby
1.4. V čl. 4., odstavci 4.1 se doplňuje bok K. Poradenská činnost, která zahrnuje zejména:
a) osobní účast na pravidelných poradách IT,
b) osobní účast na jednáních v souvislosti s rozvojem IS/IT zadavatele
1.5. V čl. 7., odstavci 7.3 písm. a) zní: „Odměna za poskytování služeb dle čl. 4. odstavce 4.1, mimo skupiny a podskupiny (C10., H., I., J.), je tvořena odměnou ve výši 324000,- Kč bez DPH za měsíc."
1.6. V čl. 7., odstavci 7.3 písm. b) zní: „Odměna za poskytování služeb správy mobilních zařízení dle článku 4., odstavce 4.1, podskupiny C10., bude po celou dobu účinnosti smlouvy hrazena na základě skutečně poskytnutých služeb v hodinové sazbě ve výši

820,- Kč bez DPH/hod., přičemž minimální účtovaná jednotka spotřeby času činí ¼ hodiny. Celkové plnění těchto služeb nepřesáhne částku 70000,- Kč bez DPH za období jednoho roku."

1.7. V čl. 7., odstavci 7.3 písm. c) zní: „Odměna za služby poskytované nad běžný rámec služeb dle článku 4. odst. 4.3 bude po celou dobu účinnosti smlouvy hrazena na základě skutečně poskytnutých služeb v hodinové sazbě ve výši 820,- Kč bez DPH/hod., přičemž minimální účtovaná jednotka spotřeby činí ¼ hodiny. Celkové plnění těchto služeb nepřesáhne částku 200000, - Kč bez DPH za období jednoho roku."

1.8. V čl. 7., odstavci 7.3 se doplňuje písm. d), které zní: „Odměna za poskytování služeb dle čl. 4 odstavce 4.1, podskupiny I., bude po celou dobu účinnosti smlouvy hrazena na základě skutečně poskytnutých služeb v sazbě ve výši 14000,- Kč bez DPH/člověkoden za roli Architekt KB. Za roli správce ICT v sazbě ve výši 9000,- Kč bez DPH/člověkoden, přičemž pojmem člověkoden se rozumí 8 člověkohodin práce. Minimální účtovaná jednotka spotřeby činí ½ člověkohodiny." Přílohou faktury bude časový výkaz odvedené práce.

1.9. V čl. 7., odstavci 7.3 se doplňuje písm. e), které zní: „Odměna za poskytování služeb dle čl. 4 odstavce 4.1, podskupiny J., bude po celou dobu účinnosti smlouvy hrazena paušální částkou ve výši 30000,- Kč bez DPH/měsíc."

1.10. V čl. 9., odstavci 9.2.4 se mění oprávněná osoba v odrážce „za zadavatele" na [redacted]

1.11. V čl.10., odstavci 10.2 písm. a) zní: „svolávat operativní schůzky smluvních stran a vyžadovat zprávy a stanoviska k předmětu plnění v ústní i písemné formě"

1.12. V čl. 10., odstavci 10.3 písm. g) zní: „bez prodlení zadavateli hlásit každý výskyt bezpečnostního incidentu souvisejícího s provozem svěřeného ICT a poskytnout o tom písemnou zprávu v minimálním rozsahu popisu příčiny, rozsahu škod, přijatých opatřeních",

1.13. V čl. 10., odstavci 10.3 písm. j) zní: „udržovat provozní, uživatelskou a administrativní dokumentaci svěřených IS a technologií nezbytnou pro zajištění řádného provozu v souladu s platnou legislativou evropskou, národní a zadavatele",

1.14. V čl. 10., odstavci 10.3 písm. n) zní: „na písemnou výzvu zadavatele sjednat nápravu ve věci plnění předmětu smlouvy do 10 dnů od doručení výzvy, pokud nebude dohodnuto jinak."

1.15. V příloze č. 1, Specifikace předmětu plnění, písm. A. Služby v oblasti plánování a rozvoje IS/ICT, bod A1. Tvorba koncepce rozvoje IS/ICT zadavatele zní: „Poskytovatel se v úzké součinnosti se zadavatelem podílí na přípravě strategických a koncepčních dokumentů v oblasti rozvoje oblasti ICT města Žďár nad Sázavou – Strategie rozvoje ICT města Žďár nad Sázavou a informační koncepce, včetně zajištění systému řízení bezpečnosti informací, zajištění návrhů a implementaci bezpečnostních opatření IS/ICT zadavatele.

Strategické cíle definované výše uvedenými dokumenty a aktuální potřeby rozvoje ICT zadavatele jsou podkladem pro zpracování návrhu kapitálového a běžného rozpočtu zadavatele na další období.

Cílem je zajistit koncepční rozvoj vybraných prioritních oblastí a možnost je v postupných krocích systematicky rozvíjet v závislosti na rozpočtových možnostech zadavatele."

1.16. V příloze č. 1, Specifikace předmětu plnění se doplňuje, písm. I. Zajištění role Architekta KB a Správce ICT ve znění: „Poskytovatel se zavazuje zajistit pro zadavatele role Architekt KB (kybernetické bezpečnosti) a Správce ICT jejichž odpovědnosti jsou stanoveny v příloze č.4 – Odpovědnosti Architekta KB a Správce ICT."

1.17. V příloze č. 1, Specifikace předmětu plnění se doplňuje, písm. J. Zajištění pohotovostní služby ve znění: „Poskytovatel se zavazuje zajistit nepřetržitou pohotovostní službu v době mimo Provozní dobu městského úřadu, která je vždy aktuálně zveřejněna na adrese: https://www.zdarns.cz/kontakty. Služba je dostupná prostřednictvím jednotného bodu kontaktu. Pohotovost se poskytuje pro požadavky priority Havárie, Vysoká a Střední dle

přílohy č. 2. včetně povinností vyplývajících z přílohy č.4 smlouvy. Součástí služby je poskytnut objem 4 člověkohodin/měsíc pro fyzickou přítomnost v místě zásahu. Výkon nad rámec služby bude hrazen na základě vzájemné dohody odpovědných osob dle čl. 9. odst. 9.2.4. o této dohodě bude veden záznam elektronickou formou v systému ServiceDesk."

1.18. V příloze č. 3 Seznam kritických služeb se doplňují další body: „IS stavebního úřadu", „Elektronická spisová služba", „VSS – kamerový systém úřadu", „ACS – elektronický přístupový systém" a nahrazují se slova: „EZS docházkový systém" za slova: „EZS - elektronický zabezpečovací systém". Dále se nahrazuje slova „IS Marbes" za slova „IS Vera Radnice"

1.19. Doplňuje se příloha č.4 - Odpovědnosti Architekta KB a Správce ICT

Čl. 2 Platnost a účinnost smlouvy

2.1. Platnosti nabývá tento dodatek podpisem obou smluvních stran a účinnosti uveřejněním dodatku v informačním systému veřejné správy – Registru smluv.

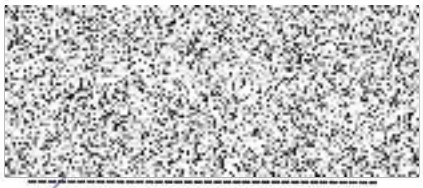
2.2. 2.2. Tento dodatek byl vyhotoven ve čtyřech (4) stejnopisech, z nichž každá smluvní strana obdrží po dvou (2) stejnopisech. Smluvními stranami podepsané stejnopisy mají právní účinky originálu.

2.3. 2.3. Uzavření tohoto dodatku schválila rada města na své 92. schůzi dne 22.12.2025.

Poskytovatel

Datum: 23. 12. 2025

Místo: Žďár nad Sázavou



Zadavatel

Datum: 23. 12. 2025

Místo: Žďár nad Sázavou

Příloha č.4 - Odpovědnosti Architekta KB a Správce ICT

Zajišťování kybernetické bezpečnosti

Architekt KB

- Návrh a zajištění implementace technických bezpečnostních opatření zajišťujících bezpečnou architekturu informačního systému
- Návrh bezpečné architektury informačního systému města
- Monitoring a analýza možných dopadů aktuálních hrozeb a zranitelností, zveřejňovaných NÚKIB
- Definice bezpečnostních požadavků na návrh, akvizici, vývoj, testování a implementaci nových technických aktiv a změnu stávajících
- Předkládání návrhů implementace technických opatření
- Řešení kybernetických bezpečnostních událostí a incidentů

V rámci řízení dodavatelů:

- Návrh vhodných bezpečnostních opatření ke snížení rizika „vendor lock – in"

Správce ICT

- V rámci vývoje zajistit bezpečnost vývojového, zálohovacího a testovacího prostředí a ochranu informací a dat v nich zpracovávaných
- Zajistí oddělení provozního, vývojového, zálohovacího a testovacího prostředí.
- Stanovuje postupy a pravidla pro údržbu a podporu nového aktiva
- Vyřazení aktiva z provozu
- Zpracování exit strategie aktiva
- Provedení opatření ke zvýšení fyzické bezpečnosti

Aplikační bezpečnost

Architekt KB

- Zajištění pravidelné identifikace zranitelností aktiv prováděnou sledováním informací od výrobců a NÚKIB
- Navrhuje nástroj pro automatizované skenování zranitelností
- V případě potřeby nařizuje provedení manuálního skenování zranitelností u určeného technického aktiva
- Určení rozsahu a postup implementace nápravných zařízení
- Návrh bezpečnostních opatření pro nepodporované typy aktiv

Správce ICT

- Vede evidenci všech technických aktiv souvisejících s poskytováním dodávané služby
- Zajištění zálohování a konfigurací u bezpečnostních a technických aktiv
- Vede evidenci nepodporovaných technických aktiv
- Zajištění podpory technických aktiv, evidence jejich zajištěné podpory a jejich bezodkladnou aktualizaci
- Zajišťuje automatizované skenování zranitelností

- Zaznamenává, eviduje a vyhodnocuje skenování zranitelností z pohledu rizik
- Přiděluje zranitelnostem kategorie
- Řešení kritické zranitelnosti do 48 hodin od zjištění a pokud je to technicky možné
- Informuje dotčené uživatele o provedení aktualizace

Bezpečnost komunikačních sítí

Architekt KB

- V rámci ochrany sítě odpovídá za výběr komunikačních protokolů, které jsou odolné vůči známým útokům a jsou bezpečné dle aktuálních standardů a doporučení NÚKIB
- Vede seznam zakázaných protokolů
- Odpovídá za návrh rozdělení sítě
- Doporučení nástroje a stanovení rozsahu monitorovaných technických aktiv
- Sledování zranitelnosti nasazených síťových zařízení
- Aktualizace a revize pravidel bezpečnosti technických aktiv
- Stanovuje pravidla obměny kryptografických klíčů

Správce ICT

- Odpovídá za zdokumentování sítě a realizaci bezpečnostních pravidel a opatření
- Odpovídá za provoz nástrojů pro zaznamenávání bezpečnostních a provozních událostí a za zajištění důvěrnosti a integrity zaznamenávaných událostí
- Vyhodnocuje statistiky provozu nástrojů pro zaznamenávání bezpečnostních a provozních událostí
- Zajištění nepřetržité synchronizace jednotného času technických aktiv
- Nastavení bezpečnostních pravidel u spravovaných technických aktiv.
- Povoluje vzdálenou správu technických aktiv
- Odpovídá za instalace, změny konfigurací nebo zásahy do systému
- Odpovídá za nastavení pravidel vzdáleného přístupu, vedení evidence a její aktualizace
- Zajištění technických prostředků pro šifrování dat
- Vedení centrální správy kryptografických klíčů

Bezpečnost lidských zdrojů

Správce ICT

- Poučení administrátorů informačních systémů o pravidlech zajišťování kybernetické bezpečnosti a o pravidlech výkonu funkce administrátora

Detekce a zvládání KBU a KBI

Architekt KB

- Trvale monitoruje zveřejněné hrozby a zranitelnosti v oblasti kybernetické bezpečnosti, provádí jejich analýzu a navrhuje potřebná protiopatření

- Podílí se na vyšetřování kybernetického bezpečnostního incidentu a návrhu technických nápravných opatření
- Prověří oznámené zdroje a příčiny možné hrozby v podmínkách provozovaných informačních a komunikačních systémů regulované služby
- Návrh rozsahu monitorovaných technických aktiv

Správce ICT

- Shromažďuje a vyhodnocuje informace o ohlášených kybernetických bezpečnostních událostech u města a dodavatelů a třetích stran.
- Rozhoduje, zda je ohlášená nebo detekovaná událost provozní událostí, kybernetickou bezpečnostní událostí nebo kybernetickým bezpečnostním incidentem
- Vede evidenci a záznamy o kybernetických bezpečnostních událostech a incidentech
- Odpovídá za detekci, zaznamenávání a vyhodnocování detekovaných kybernetických bezpečnostních událostí a incidentů
- Odpovídá za zvládání kybernetických bezpečnostních incidentů
- Při hlášení kybernetické bezpečnostní události/incidentu povinen zajistit, pro příjem a posouzení detekovaných a ohlášených událostí, trvalou dostupnost určeného zaměstnance
- Vede záznam o kybernetickém bezpečnostním incidentu v ServiceDesku
- Odpovídá za ochranu integrity, důvěrnosti a dostupnosti záznamů a důkazních materiálů o incidentu
- Zajištění realizace bezpečnostního opatření a jeho ohlášení MKB
- Zajišťuje v rámci interní komunikační sítě města provoz automatizovaných nástrojů zajišťujících detekci kybernetických bezpečnostních událostí
- Zajistí pravidelnou aktualizaci software pro detekci a odstranění škodlivých kódů
- Stanoví rozsah detekovaných provozních událostí technických aktiv ve své provozní dokumentaci
- Zajišťuje řízení automatického spouštění obsahu u zařízení města, zejména v případě připojování vyměnitelných zařízení a datových nosičů
- Zajišťuje nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech prostřednictvím notifikací na určenou e-mailovou adresu ServiceDesku
- Zaznamenává detekované kybernetické bezpečnostní události
- Uchovává záznamy o detekovaných kybernetických bezpečnostních událostech po dobu nejméně 6 měsíců
- Provádí pravidelnou kontrolu účinnosti nástrojů pro detekci kybernetických bezpečnostních událostí
- Provádí aktualizaci a optimalizaci nástrojů pro detekci kybernetických bezpečnostních událostí

Řízení kontinuity činností

Správce ICT

- Vede evidenci RTO a RPO pro jednotlivá aktiva a odpovídá za zpracování a realizaci plánů zálohování a plánů obnovy záloh
- Navrhuje starostovi města vyhlášení mimořádné situace a na základě jejího vyhlášení zahajuje aktivaci plánů kontinuity a plánů obnovy
- Odpovídá za řízení procesů kontinuity činností ICT a realizaci plánů obnovy

- Určení rozsahu garantů obnovy dle charakteru mimořádné události nebo kybernetického útoku.
- Řízení kapacit pro zálohování, včetně provádění zálohování a testování obnovy záloh
- Realizace pravidel pro nakládání se zálohovacími médii

Řízení přístupu

Architekt KB

- Nastavení pravidel pro použitá softwarová řešení

Správce ICT

- Přidělení privilegovaných oprávnění administrátorů
- Přidělení a odebrání přístupových oprávnění a zrušení registrace uživatele na základě schválených žádostí, zajištění pravidelného přezkoumání přidělených oprávnění uživatelů
- Vede evidenci zaměstnanců, kteří disponují privilegovaným oprávněním, která přezkoumává
- Řízení přístupu dodavatele v souladu s pravidly uvedenými ve smlouvě.
- Zrušení všech přístupů dodavatele v případě ukončení smlouvy
- Vedení evidence přístupových oprávnění dodavatelů
- Vedení evidence uživatelů, kteří mají povolen vzdálený přístup, kterou přezkoumává v součinnosti s tajemníkem úřadu z hlediska aktuálnosti a potřebnosti minimálně 1x 6 měsíců
- Revize identit a jejich změn
- Zřizování identit dodavatelům
- Zřízení identity každého uživatele v nástroji pro centrální správu uživatelů, technických prostředků a řízení oprávnění v síti
- Obnovení účtu po jeho zablokování
- Nastavení pravidel pro hesla v nástroji pro centrální správu uživatelů, technických prostředků a řízení oprávnění v síti
- Zajištění bezodkladnou změnu přístupového hesla v případě oznámení jeho kompromitace nebo podezření na možnou kompromitaci
- Zabezpečení záložních administrátorských účty pro případ obnovy po havárii, mimořádné události nebo kybernetickém bezpečnostním incidentu.