DODATEK č. 3
ke smlouvě o dílo
na poskytování služeb technické podpory
k agendě Spisová služba
pro příspěvkové organizace kraje Vysočina ze dne 31. 7. 2009

I. Smluvní strany

1. Kraj Vysočina

se sídlem:	Žižkova 1882/57, 586 01 Jihlava
IČ:	70890749
DIČ:	CZ70890749
bankovní spojení:	Sberbank CZ, a.s., pobočka Jihlava
č.ú.:	4050005000/6800
zastoupena:	Mgr. Vítězslavem Schrekem, MBA, hejtmanem kraje
k podpisu pověřen:	RNDr. Jan Břížďala, radní pro oblast školství, mládež a sport, informatiku a komunikační technologie

(dále jen „***objednatel***“)

a

2. GEOVAP, spol. s r. o.

se sídlem:	Čechovo nábřeží 1790, 530 03 Pardubice
IČ:	15049248
DIČ:	CZ15049248
bankovní spojení:	Česká spořitelna, a.s.
č.ú.:	500069362/0800
zastoupena:	Ing. Robert Matulík, jednatel společnosti

(dále jen „***poskytovatel***“)

(společně dále jen „***smluvní strany***“)

II. Změna smlouvy

Smluvní strany se shodli na následujících změnách:

A) V čl. II (Účel smlouvy, předmět smlouvy a vymezení) se odstavec 2 ruší a nahrazuje novým odstavcem 2, který zní:

2. Předmětem této smlouvy je závazek poskytovatele poskytovat služby technické podpory k typovému aplikačnímu programovému vybavení (TAPV) CityWare - modulu Spisová služba a modulu PDF Server pro hostované organizace Objednatele prostřednictvím centrální hostované spisové služby pro příspěvkové organizace kraje Vysočina, tj. jedné centrální instalace hostované spisové služby s jednou instancí databáze, ke které by měly přístup všechny příspěvkové organizace kraje Vysočina a (oba moduly dále jen souhrnně „SSL") včetně poskytnutí licence k užití SSL a závazek objednatele za poskytnuté služby zaplatit poskytovateli cenu stanovenou v Čl. III této smlouvy.

B) V čl. III. (Cena) se odstavec 1 ruší a nahrazuje novým odstavcem 1, který zní:

„1. Cena služby paušální technické podpory na jeden rok činí:

Cena bez DPH .... 145 200,00 Kč
DPH .... 30 492,00 Kč
Cena včetně DPH .... 175 692,00 Kč“

C) V čl. IV. (Platební podmínky a sankce) se odstavec 1 ruší a nahrazuje novým odstavcem 1, který zní:

„1. Služby paušální technické podpory bude poskytovatel na základě této smlouvy fakturovat objednateli 1 x za kalendářní čtvrtletí zpětně ve výši 1/4 roční částky sjednané dle čl. III. odst. 1. této smlouvy, a to vždy k pátému dni prvního měsíce následujícího kalendářního čtvrtletí se zdanitelným plněním k poslednímu dni posledního měsíce kalendářního čtvrtletí, ke kterému se platba vztahuje. V roce 2022 bude první platba fakturována k 31.3.2022 v poměrné části za měsíce únor a březen 2022 ve výši 24.200,- Kč bez DPH, tj. 29.282,- Kč s DPH.

D) V čl. VIII. (Licence) se odstavec 1 ruší a nahrazuje novým odstavcem 1, který zní:

„1. Poskytovatel poskytuje touto smlouvou objednateli a objednatel touto smlouvou přijímá nevýhradní licenci k užití SSL včetně jejích aktualizací zejména podle vývoje právní úpravy, a to na jakékoliv v současnosti známé využití. Licence je poskytnuta na dobu trváni majetkových práv k nehmotnému statku."

E) Do smlouvy se doplňuje nová Příloha č. 5 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele, jejíž úplné znění je přílohou tohoto dodatku.

III. Závěrečná ustanovení

1. Ustanovení smlouvy tímto dodatkem nedotčená zůstávají nadále v platnosti.
2. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá smluvní strana obdrží jedno vyhotovení. V případě, že bude smlouva podepisována elektronicky, každá smluvní strana obdrží elektronický dokument s kvalifikovanými elektronickými podpisy obou smluvních stran v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.
3. Smluvní strany prohlašují, že si tento dodatek přečetly, že byl sepsán podle jejich pravé a svobodné vůle, nikoliv v tísni a za nápadně nevýhodných podmínek, a na důkaz toho připojují své podpisy.
4. Smluvní strany souhlasí se zveřejněním tohoto dodatku v jeho plném znění včetně podpisů dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
5. Poskytovatel výslovně souhlasí se zveřejněním celého textu tohoto dodatku včetně podpisů v informačním systému veřejné správy – Registru smluv. Smluvní strany se dohodly, že dodatek smlouvy v Registru smluv zveřejní objednatel.
6. Tento dodatek nabývá platnosti dnem podpisu poslední smluvní strany a účinnosti dnem uveřejnění v Registru smluv.

7. Nedílnou součástí tohoto dodatku jsou tyto přílohy:
   Příloha č. 5 smlouvy – Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele.

Za poskytovatele:	Za objednatele:
V Pardubicích dne	V Jihlavě dne
Ing. Robert Matulík Digitálně podepsal Ing. Robert Matulík Datum: 2021.12.20 07:53:50 +01'00'	RNDr. Jan Břížďala Digitálně podepsal RNDr. Jan Břížďala Datum: 2021.12.22 09:22:45 +01'00'
Ing. Robert Matulík jednatel	RNDr. Jan Břížďala radní kraje

Příloha č. 5 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele

- Bezpečnost přístupových oprávnění
  - Zhotovitel je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům Zhotovitele, které umožňují přístup k informačním aktivům objednatele či umožnují jejich správu.
  - Zhotovitel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 17 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      - malá písmena
      - velká písmena
      - číslice
      - speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1,5 roku.
  - Zhotovitel je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  - Pokud by Zhotovitel zřizoval přístupová oprávnění třetí straně, je Zhotovitel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.

- Řízení rizik
  - Objednatel si vyhrazuje právo na informace o tom, jakým způsobem Zhotovitel řídí rizika, tedy o tom, jakou metodiku pro řízení rizik používá, jakým způsobem jsou rizika hodnocena a klasifikována, jakým způsobem jsou rizika ošetřována a kdo je za řízení rizik za Zhotovitele zodpovědný.
  - Zhotovitel se zavazuje řídit rizika informační bezpečnosti minimálně v následujícím rozsahu:
    - Identifikace a ohodnocení aktiv souvisejících s plněním této smlouvy,
    - Identifikace, analýza a ohodnocení rizik souvisejících s plněním této smlouvy,
    - Zvládání a monitoring rizik souvisejících s plněním této smlouvy.
- Řízení kybernetických bezpečnostních incidentů:
  - Zhotovitel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které by mohli mít nějakou souvislost s:
    - informačními aktivy objednatele,
    - přístupovými údaji k informačním aktivům objednatele,
    - informacím objednatele.
  - Zhotovitel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Objednatele.

- Kryptografie:

Pokud budou v souvislosti s plněním této smlouvy použity kryptografické funkce, algoritmy či metody, je Zhotovitel povinen řídit se těmito požadavky:

Obecně

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá a popsaná.

Hashovací funkce

Ukládání otisků hesel

- pro ukládání hesel uživatelů mohou být použity pouze tyto hashovací funkce:
  - Argon2i
  - bcrypt
  - scrypt

        - PBKDF2
        - SHA2

Elektronické podepisování e-mailů a dokumentů

- SHA-2 a vyšší
- délka otisku 256 bitů a vyšší

Ověřování integrity souborů

- SHA-2 a vyšší
- délka otisku 224 bitů a vyšší

Asymetrická kryptografie

SSL/TLS

- verze protokolu minimálně TLSv1.2 a vyšší
- konfigurace
    - cipher suite musí být vybrána na základě serverem preferovaného pořadí
    - vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
        - ECDHE musí mít vyšší prioritu než DHE
        - ECDSA musí mít vyšší prioritu než DSA
    - všechny EXPORT cipher suites musí být zakázány
    - algoritmy a funkce pro výměnu klíčů
        - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
            - tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
            - a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn., že pro každou session je generován nový set Diffie-Hellman klíčů
        - délky klíčů:
            - pro Diffie-Hellman (DH) - 2048 bitů a více (postupně přecházet na 3072 bitů, tam kde to bude možné)
            - pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
        - nesmí být použita anonymní výměna klíčů
    - algoritmy a funkce pro autentizaci
        - minimální délky klíčů:
            - RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
            - ECDSA - 256 bitů
    - algoritmy a funkce pro symetrické šifrování
        - nesmí být použita hodnota NULL v cipher suites
        - nesmí být použity tyto šifry:
            - DES, 3DES, RC4
        - minimální délka šifrovacího klíče - 128 bitů
        - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
    - MAC (Message Authentication Code)
        - použití SHA funkce s minimální délkou hashe 256 bitů
        - vyšší délky otisků musí mít vyšší prioritu v cipher suites
- Certifikáty dodá zadavatel

TLS cipher suites

- Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
- TLS1.3:
  TLS_AES_256_GCM_SHA384
  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_128_GCM_SHA256
  TLS_AES_128_CCM_SHA256

- TLS1.2:
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
    - algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
    - délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to bude možné)
    - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

Symetrická kryptografie

- nesmí být použity tyto šifry:
    - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 128 bitů
    - pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
- nesmí být použity tyto módy pro ochranu integrity:
- HMAC-SHA1, CBC-MAC-X9.19