SERVISNÍ SMLOUVA

podle zákona č. 89/2012 Sb., občanského zákoníku (dále jen „NOZ“),

(tato servisní smlouva dále též jen „**smlouva**“)

1. SMLUVNÍ STRANY

Objednatel:

Kraj Vysočina,

Se sídlem: Žižkova 1882/57, 586 01 Jihlava

IČO: 70890749,

DIČ: CZ70890749 (není plátcem DPH)

jehož jménem jedná RNDr. Jan Bříždala, radní

Bankovní spojení: Komerční banka a.s.

Č. účtu: 123-6403810267/0100

(dále jen „**objednatel**“)

a

Poskytovatel:

Spolek pro budování a implementaci sdílených open source nástrojů, z. s.,

IČO: 05730732

se sídlem: Žižkova 1872/89, 586 01 Jihlava,

spisová značka: L 22325 vedený u Krajského soudu v Brně

zastoupený Ing. Evou Janouškovou, ředitelkou spolku

Bankovní spojení: Fio Banka, a. s.

Č. účtu: 2401243360/2010

E-mail: info@spolek-bison.cz

Kontaktní osoba zhotovitele ve věcech technických dle této smlouvy je:

Martin Hadrava, e-mail: hadrava.martin@spolek-bison.cz, tel.: 724 650 289

(dále jen „**poskytovatel**“)

2. ÚVODNÍ USTANOVENÍ

1. Poskytovatel prohlašuje, že je způsobilý k řádnému a včasnému poskytování servisních služeb dle této smlouvy a že disponuje takovými kapacitami a odbornými znalostmi, které jsou třeba k řádnému a včasnému poskytování servisních služeb.
2. Smluvní strany prohlašují, že identifikační údaje uvedené v čl. I této smlouvy odpovídají aktuálnímu stavu a že osobami jednajícími při uzavření této smlouvy jsou osoby oprávněné k jednání za nebo jménem smluvních stran. Jakékoliv změny údajů uvedených v čl. I této smlouvy, jež nastanou v době po uzavření této smlouvy, jsou smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé smluvní straně.

3. V případě, že se kterékoliv prohlášení některé ze smluvních stran podle tohoto článku ukáže býti nepravdivým, odpovídá tato smluvní strana za škodu a nemajetkovou újmu, která nepravdivostí prohlášení nebo v souvislosti s ní druhé smluvní straně vznikla.
4. Tato smlouva navazuje na smlouvu o dílo ze dne 20. 5. 2024, uzavřenou mezi Objednatelem a Poskytovatelem jako zhotovitelem (dále jen „smlouva o dílo“).
5. Je-li v této smlouvě pojednáváno o díle, je tím míněn předmět plnění dle smlouvy o dílo (dále jen „dílo“).

3. PŘEDMĚT SMLOUVY

1. Poskytovatel se zavazuje poskytovat na svůj náklad a nebezpečí řádně a včas dále specifikované servisní služby a Objednatel se zavazuje zaplatit za řádně a včasně poskytnuté servisní služby sjednanou cenu.
2. Poskytovatel se zavazuje za podmínek uvedených v této smlouvě poskytovat Objednateli servisní služby vztahující se k dílu provedenému dle smlouvy o dílo. Servisní služby jsou dále specifikovány v příloze č. 1 této smlouvy. Kategorizace a úroveň servisních služeb dle této servisní smlouvy ve vztahu k dílu je uvedena v příloze č. 1 této smlouvy. Veškeré servisní služby poskytované na základě této smlouvy jsou dále označovány také jen jako „**servisní služby**“.
3. Servisní služby budou prováděny v následujících kategoriích:
    a. Maintenance;
    b. Technická podpora;
    c. Řešení incidentů.

    Specifikace jednotlivých kategorií a rozsah jednotlivých servisních služeb v nich poskytovaných jsou uvedeny v příloze č. 1 této smlouvy.
4. Servisními službami v kategorii řešení incidentů je i odstraňování záručních vad, avšak pouze těch částí díla, které jsou stanoveny v příloze č. 1 této smlouvy. Jestliže se vyskytne záruční vada části díla, která není stanovena v příloze č. 1 této smlouvy, budou smluvní strany postupovat dle smlouvy o dílo.
5. Poskytovatel je povinen poskytovat servisní služby dle této smlouvy tak, aby dostupnost Evidence náhradní rodinné péče byla alespoň 99% ročně po celou dobu účinnosti této smlouvy. Výpočet skutečně dosažené dostupnosti se řídí metodikou dle přílohy č. 1 této smlouvy.

4. POSKYTOVÁNÍ SERVISNÍCH SLUŽEB

1. Servisní služby mohou být prováděny vzdálenou správou nebo přímo příjezdem pracovníka Poskytovatele na místo plnění.
2. Poskytovatel je povinen udržovat servisní pohotovost tak, aby byl schopný garantovat časové lhůty stanovené v příloze č. 1 této smlouvy.
3. Poskytovatel je povinen při poskytování servisních služeb dodržovat reakční dobu (dále jen „**reakční doba**“ nebo „**reakce**“) a dobu vyřešení incidentu nebo požadavku (dále jen „**doba vyřešení**“). Specifikace reakční doby a doby vyřešení je uvedena v příloze č. 1 této smlouvy.

4. Kategorizace incidentů, reakční doby na jednotlivé kategorie incidentů a doby vyřešení jednotlivých kategorií incidentů a reakční doby a doby vyřešení požadavků jsou uvedeny v příloze č. 1 této smlouvy a jsou pro Poskytovatele závazné.
5. Objednatel nahlásí incident nebo požadavek Poskytovateli prostřednictvím helpdesku dostupném na adrese http://spolek-bison.cz/helpdesk. Objednatel stanoví kategorii incidentu a úroveň požadovaných servisních služeb dle přílohy č. 1 této smlouvy.
6. Poskytovatel má právo si na základě nahlášení incidentu nebo požadavku vyžádat po Objednateli bližší specifikaci incidentu nebo požadavku. Tato činnost je již považována za zahájení činnosti Poskytovatele ve smyslu přílohy č. 1 této smlouvy.
7. V případě, že Objednatel informuje e-mailem Poskytovatele ve výše uvedené lhůtě 24hod, že s vyřešením incidentu nebo požadavku nesouhlasí, je Poskytovatel povinen pokračovat v řešení požadavku nebo incidentu v jeho původní kategorii a je povinen dodržet dobu vyřešení dle přílohy č. 1 této smlouvy. Do doby vyřešení dle přílohy č. 1 této smlouvy není počítána doba od okamžiku doručení e-mailu Objednateli o vyřešení incidentu či požadavku do okamžiku doručení e-mailu obsahujícího informaci o souhlasu či nesouhlasu Objednatele s vyřešením incidentu nebo požadavku Poskytovateli.
8. Dílo – SW Coby, obsahuje osobní údaje ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Zhotovitel při plnění této smlouvy neprovádí zpracování osobních údajů a ani k nim nemá přístup (osobní údaje jsou šifrované a čitelné pouze pro subjekty, které k tomu mají právní důvod).

5. CENA SERVISNÍCH SLUŽEB

1. Objednatel se zavazuje zaplatit Poskytovateli za poskytování servisních služeb dle této smlouvy smluvní cenu. Cena plnění je tvořena následujícími částmi:

	Cena v Kč bez DPH za 1 měsíc
Paušální cena za poskytování servisních služeb v kategorii Maintenance	5 000,- Kč

	Cena v Kč bez DPH za 1 hodinu
Cena za poskytování servisních služeb v kategorii Technická podpora a vývoj	1 200,- Kč
Cena za poskytování servisních služeb v kategorii Řešení incidentů nad rámec paušálu v kategorii Maintenance	1 200,- Kč

2. Cena servisních služeb v kategorii Maintenance zahrnuje veškeré náklady, jež mohou Poskytovateli v souvislosti s poskytováním této kategorie služeb vzniknout, zejm. cestovní výdaje a náklady na softwarové a hardwarové vybavení. Za poskytování služeb v kategorii Maintenance tak Poskytovatel kromě shora uvedené ceny nemá nárok na žádné další finanční plnění.
3. Cena servisních služeb v kategorii Maintenance zahrnuje:

- veškeré náklady, jež mohou Poskytovateli v souvislosti s poskytováním této kategorie služeb vzniknout, zejm. cestovní výdaje a náklady na softwarové a hardwarové vybavení;
- cenu dodaného software a licencí nutných pro vyřešení jednotlivých požadavků objednatele. Licence musí odpovídat podmínkám stanoveným ve smlouvě o dílo.

Za poskytování služeb v kategorii Technická podpora a vývoj kromě shora uvedené ceny nemá Poskytovatel nárok na žádné další finanční plnění.

4. Cena servisních služeb v kategorii Řešení incidentů zahrnuje:
   - veškeré náklady, jež mohou Poskytovateli v souvislosti s poskytováním této kategorie služeb vzniknout, zejm. cestovní výdaje a náklady na softwarové a hardwarové vybavení;
5. K cenám uvedeným v tomto článku bude při fakturaci dopočítáno DPH dne zákonné sazby.

6. FAKTURACE A PLATEBNÍ PODMÍNKY

1. Cenu za poskytování servisních služeb se Objednatel zavazuje platit na základě faktur (dále jen „**faktura**“) vystavených Poskytovatelem po uplynutí kalendářního měsíce trvání této smlouvy. Fakturou bude vyúčtována:
   - cena servisních služeb v kategoriích Maintenance a Řešení incidentů poskytnutých v příslušném kalendářním měsíci trvání této smlouvy;
   - cena servisních služeb v kategorii Technická podpora a vývoj dle času skutečně a účelně stráveného Poskytovatelem při poskytování této kategorie servisních služeb;
2. O poskytování servisních služeb v jednotlivých kalendářních měsících je Poskytovatel povinen Objednateli zasílat výkazy k potvrzení.
3. Cena za poskytování servisních služeb je splatná do 30 kalendářních dnů od doručení faktury Objednateli.

7. OSTATNÍ PODMÍNKY PLNĚNÍ PŘEDMĚTU SMLOUVY

1. Poskytovatel je povinen při poskytování servisních služeb postupovat v souladu s platnými právními předpisy.
2. Objednatel je povinen spolupracovat s Poskytovatelem a poskytovat mu veškerou nutnou součinnost potřebnou pro řádné poskytování servisních služeb podle této smlouvy. Objednatel je povinen informovat Poskytovatele o veškerých skutečnostech, které jsou nebo mohou být důležité pro poskytování servisních služeb dle této smlouvy.
3. Pokud Objednatel neposkytne součinnost dle tohoto článku, má Poskytovatel právo požadovat od Objednatele posunutí stanovených termínů o dobu, po kterou nemohl Poskytovatel poskytovat servisní služby dle této smlouvy z důvodu neposkytnutí součinnosti. Objednatel je povinen takovému požadavku vyhovět.
4. Objednatel je povinen poskytnout Poskytovateli součinnost k zajištění vzdáleného přístupu Poskytovateli k serverům, na kterých je umístěno dílo výhradně pro účely poskytování servisních služeb podle této smlouvy.

5. Smluvní strany spolu budou komunikovat způsobem stanoveným v příloze č. 1 této smlouvy.
6. Písemné oznámení o změnách výše uvedených kontaktních údajů Poskytovatele nebo webové adresy Helpdesk předá Poskytovatel Objednateli alespoň pět dní před očekávanou změnou.
7. Poskytovatel je povinen dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.
8. Poskytovatel se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina uvedené v příloze č. 2 této smlouvy
9. Poskytovatel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných poddodavatelů či jiných osob, které mají přístup k informačním aktivům Kraje Vysočina prostřednictvím poskytovatele.
10. Poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi poskytovatel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění poskytovatele veřejně přístupnými stanou (dále jen „důvěrné informace“). Poskytovatel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch objednatele. Povinnosti dle tohoto odstavce je poskytovatel povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění poskytovatele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je poskytovatel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené poskytovateli právním předpisem nebo rozhodnutím orgánu veřejné moci.
11. Za nesplnění kterékoliv povinnosti obsažené v tomto článku v odstavci 7 až 10 a v příloze č. 2 této smlouvy, je objednatel oprávněn účtovat poskytovateli smluvní pokutu ve výši 10 000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku a příloze.
12. Poskytovateli na základě této smlouvy nevzniká žádné právo na užití dat zpracovávaných prostřednictvím díla.

8. TRVÁNÍ A UKONČENÍ SMLOUVY

1. Tato smlouva je uzavřena na dobu neurčitou a její plnění začíná běžet od převzetí díla objednatelem dle smlouvy o dílo. Výpovědní doba jsou 3 měsíce a počíná běžet prvním den měsíce následujícím po měsíci, ve kterém byla výpověď doručena.
2. Jestliže Objednatel nebo Poskytovatel odstoupí od smlouvy o dílo nebo smlouva o dílo bude jinak ukončena, aniž by bylo provedeno dílo, tato servisní smlouva zaniká v den účinnosti odstoupení od smlouvy o dílo.
3. Poskytovatel se zavazuje v případě ukončení smlouvy zajistit předání informací nezbytný pro zajištění kontinuity provozu servisovaného informačního díla objednateli, včetně předání dostupné dokumentace s vazbou na servisovaný informační systém.

9. ODPOVĚDNOST POSKYTOVATELE A SANKCE

1. Dostane-li se Objednatel do prodlení s placením úhrady za servisní služby poskytované dle této smlouvy, je povinen zaplatit Poskytovateli úrok z prodlení ve výši 0,05 % z dlužné částky za každý den prodlení.
2. Jestliže dostupnost díla klesne pod hodnotu dle čl. 3 odst. 5 této smlouvy, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 15 000,- Kč za každý kalendářní rok, ve kterém dostupnost díla nedosáhne hodnoty dle čl. 3 odst. 5 této smlouvy, ale dosáhne hodnoty alespoň 99 %;
3. Ustanovením o smluvních pokutách a úrocích z prodlení není dotčeno právo smluvních stran na náhradu škody či nemajetkové újmy.

10.ZÁVĚREČNÁ USTANOVENÍ

1. Vzhledem k veřejnoprávnímu charakteru Objednatele i Poskytovatele smluvní strany výslovně prohlašují, že souhlasí se zveřejněním celého textu smlouvy v Registru smluv. Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona o registru smluv splní Objednatel.
2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a může být měněna pouze písemnými dodatky k této smlouvě podepsanými Objednatelem a Poskytovatelem.
3. Tato smlouva nabývá účinnosti dnem předání díla dle smlouvy o dílo.
4. Tato smlouva je vyhotovena elektronicky.
5. Nedílnou součástí této smlouvy jsou Příloha č. 1 – Specifikace servisních služeb a Příloha č. 2 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele.
6. Výběr poskytovatele byl proveden v souladu s platnými Pravidly Rady Kraje Vysočina pro zadávání veřejných zakázek.

V Jihlavě

RNDr. Jan Bříždala Ph.D.

Digitálně podepsal RNDr. Jan Bříždala Ph.D.
Datum: 2024.06.03 13:36:18 +02'00'

Jan Bříždala
radní

V Jihlavě

Ing. Eva Janoušková

Datum: 2024.05.22 09:28:21 +02'00'

Ing. Eva Janoušková
ředitelka Spolku BISON

Příloha č. 1 – Specifikace servisních služeb

I. Seznam zkratek a pojmů

Pro potřeby dalšího textu budou používány následující pojmy:

Pojem	Význam
Incident	Indikovaný problém díla, případně části díla, který není v souladu s technickým stavem díla dle smlouvy o dílo. Kategorizace incidentů je uvedena dále v textu.
Okamžik nahlášení	Okamžik nahlášení incidentu nebo požadavku prostřednictvím Helpdesk
Reakční doba (Reakce)	Doba od Okamžiku nahlášení incidentu nebo požadavku prostřednictvím Helpdesk do okamžiku zahájení činnosti Poskytovatele na identifikaci a odstranění incidentu nebo zahájení realizace požadavku Objednatele
Doba vyřešení (Vyřešení)	Doba od Okamžiku nahlášení incidentu nebo požadavku do okamžiku odsouhlasení vyřešení incidentu nebo požadavku Objednatelem.
SLA	Konkrétní smluvní parametry pro poskytování služeb v daných úrovních servisních služeb.
NBD	Následující pracovní den od doby nahlášení incidentu nebo požadavku.
HW	Hardware
SW	Software
Helpdesk	Technické řešení systému podpory na straně poskytovatele

II. Komunikace smluvních stran

Smluvní strany se dohodly na následujících prostředcích komunikace v závislosti na kategorii servisních služeb:

- Maintenance - prostřednictvím e-mailu
- Technická podpora - Helpdesk
- Řešení incidentů - Helpdesk

Webová adresa Helpdesku Poskytovatele: http://spolek-bison.cz/helpdesk

Kontaktní údaje za objednatele (osoby oprávněné k zadávání servisních požadavků):

Jaroslav Krotký, krotky.j@kr-vysocina.cz, tel. 724650193

III. Maintenance

Maintenance (pravidelná údržba) dle této smlouvy je realizována Poskytovatelem v intervalu uvedeném níže (dále jen „**Maintenance**“).

Maintenance bude Poskytovatel provádět tak, aby co možná nejvíce zamezil vzniku jakýchkoli incidentů, které by znemožňovaly řádné užívání díla objednateli a aby byla splněna dostupnost dle čl. III odst. 5 této smlouvy po celou dobu účinnosti této smlouvy.

Služby poskytované v rámci Maintenance min 1x měsíčně:

- kontrola funkčnosti všech modulů, stavu databáze a dodaného IS

Služby poskytované v rámci Maintenance min 1x ročně:

- pravidelné čištění a optimalizace databáze

Služby poskytované v rámci Maintenance průběžně případně na vyžádání:

- 2 hodiny měsíčně na řešení incidentů
- identifikace výkonnostních problémů a optimalizace běhu systému
- údržba a aktualizace veškeré dodané dokumentace
- úprava dle legislativních změn
- opravy bezpečnostních vad

IV. Technická podpora a vývoj

V rámci servisních služeb kategorie Technická podpora a vývoj dle této smlouvy jsou poskytovány následující služby:

- konzultační služby;
- realizace požadavků na novou funkcionalitu systému;

Objednatel je oprávněn objednat další služby v této kategorii v ceně dle článku V. odst. 1 této smlouvy.

V. Řešení incidentů

Kategorie servisních služeb „řešení incidentů“ definuje požadavky na činnost Poskytovatele k zajištění plynulého a bezproblémového provozu SW, tak aby byl zajištěn účel smlouvy o dílo a požadované parametry dostupnosti SW.

Kategorie incidentů:

Kategorie	Popis
A	Situace, kdy dílo nebo část díla je zcela nefunkční, neumožňuje práci uživatelů a nelze používat Objednatelem nebo dílo obsahuje bezpečnostní zranitelnost s kritickou mírou závažnosti.
B	Situace, kdy dílo nebo část díla je částečně funkční, umožňuje částečné poskytování služeb, po přechodnou dobu se sníženým komfortem uživatelů, případně provizorním způsobem z důvodů na straně díla nebo jeho části, na niž je Poskytovatel povinen poskytovat servisní služby nebo dílo obsahuje bezpečnostní zranitelnost se střední mírou závažnosti

C	Nedostatky a vady drobného rozsahu, které nebrání užívání díla nebo jeho části, nicméně nejsou v souladu s technickým stavem díla dle smlouvy o dílo nebo dílo obsahuje bezpečnostní zranitelnost s nízkou mírou závažnosti.

Kategorizaci jednotlivých incidentů provede Poskytovatel, míra závažnosti bezpečnostní zranitelností je dána následující tabulkou:

Kategorie bezpečnostních zranitelností

Kategorie	Popis
Kritická	Zranitelnost dosáhne základního skóre 8.0 – 10.0 bodů dle obecného systému hodnocení zranitelností (otevřený standard CVSSv3 base score)
Střední	Zranitelnost dosáhne základního skóre 4.0-7.9 bodů dle obecného systému hodnocení zranitelností (CVSSv3 base score)
Nízká	Zranitelnost dosáhne základního skóre 0.0-3.9 bodů dle obecného systému hodnocení zranitelností (CVSSv3 base score)

V následující tabulce jsou pak pro jednotlivé úrovně servisních služeb definovány reakční doby a doba vyřešení dle jednotlivých kategorií incidentů.

Reakční doba pro kategorie incidentů:

A		B		C	
Reakce	**Vyřešení**	**Reakce**	**Vyřešení**	**Reakce**	**Vyřešení**
NBD	2 pracovní dny	2 pracovní dny	10 pracovních dnů	10 pracovních dnů	20 pracovních dnů

VI. Metodika výpočtu dostupnosti

Pro potřeby výpočtu dosažené dostupnosti (požadovaná úroveň SLA 99%) bude využita měsíční suma výpadků v kategorii incidentu A.

Pro výpočet skutečně dosažené dostupnosti SW se pak použije následující vzorec:

$$\text{dostupnost} = \frac{(T_S - T_N)}{T_S} \times 100\ \%$$

T_S značí celkový počet hodin, po které má být v daném kalendářním roce SW provozován, s výjimkou doby oprávněného omezení provozu.

$\mathbf{T_N}$ značí celkový počet hodin, po které byl SW nedostupný nebo neplnil svoji funkci (viz. kategorie A incidentu) , s výjimkou doby oprávněného omezení provozu SW.

Do nedostupnosti SW nebudou započítány výpadky ani přerušení nebo vady SW vyplývající zejména z níže uvedených příčin:

a) SW je změněn nebo upraven na pokyn Objednatele a s jeho vědomím takovým způsobem, že parametry definované dostupnosti nemohou být splněny.

b) V případě zásahu vyšší moci.

Příloha č. 2 – Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele

1 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.

2 Řízení změn

- Poskytovatel se zavazuje zaznamenávat všechny změny, které v informačním aktivu provedl.
- Poskytovatel se zavazuje vynucovat zaznamenávání změn i u případných subdodavatelů.
- Záznam změny musí obsahovat minimálně tyto informace:
  - Datum a čas změny
  - Jméno osoby, která změnu provedla
  - Název, popis a účel změny
- Objednatel si vyhrazuje právo na pravidelné informace o záznamech všech změn provedených dodavatelem i případnými subdodavateli.
- Poskytovatel se zavazuje všechny jím provedené změny i změny případných subdodavatelů poskytnout zadavateli formou zápisu do provozního deníku vedeného v SW objednatele (Technet).

3 Řízení rizik

- Objednatel si vyhrazuje právo na informace o tom, jakým způsobem Zhotovitel řídí rizika v souvislosti s plněním této smlouvy, 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.

4 Řízení kybernetických bezpečnostních incidentů:

- Zhotovitel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které by mohli mít nějakou sou vislost 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.
- Poskytovatel je povinen objednateli hlásit veškeré nestandardní chování informačních aktiv objednatele, které zjistí v rámci své servisní činnosti.
- Poskytovatel informuje objednatele o zranitelnostech servisovaných aktiv, které zjistil v rámci své servisní činnosti a které dosáhnou CVSS v3.1 basic score 6.0 a vyšší.

5 Bezpečnost vývojového prostředí a zdrojového kódu

- ochrana před škodlivým kódem musí být zajištěna:
    - na pracovních stanicích vývojářů a programátorů,
    - na serverech/zařízení, kde je uložen zdrojový kód aplikací pro editaci.
- Ke zdrojovým kódům musí být řízen přístup tak, aby k němu měli přístup pouze oprávnění vývojáři a jiné oprávněné osoby Poskytovatele.
- Přístupy ke zdrojovým kódům a jejich změny musí být monitorovány a logovány.
- Pro správu zdrojového kódu musí být použit tzv. verzovací systém.
- Zdrojové kódy systému musí být pravidelně zálohovány a zálohy pravidelně testovány na jejich obnovitelnost.
- Zdrojový kód musí být řádně dokumentován.

6 Zákaznický audit

- Objednatel si vyhrazuje právo na provedení kontroly či auditu plnění požadavků a ustanovení této přílohy č. 3 smlouvy u Zhotovitele.
- V rámci kontroly či auditu u Zhotovitele se Zhotovitele zavazuje poskytnout důkaz o plnění objednatelem vybraného požadavku a to buď fyzicky přímo v provozovně Zhotovitele nebo vzdáleně pomocí elektronických prostředků.

7 Kryptografie:

7.1 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.

Pokud budou v souvislosti s touto smlouvou v dílu, informačních aktivech objednatele nebo pomocných aktivech pro správu a implementaci díla použity kryptografické funkce a algoritmy, musí splňovat tyto níže uvedené požadavky, a to tam, kde je to relevantní.

7.2 Hashovací funkce

7.2.1 Ukládání otisků hesel

- pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  - Argon2 s funkcí Argon2id a parametry alespoň t=1, m=2^{21}(případně t=3, m=2^{16} pro prostředí s omezenou pamětí – podléhá schválení)
  - scrypt s parametry alespoň N=32768 (2^{15}), r=8, p=1
  - PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2 (viz níže)
- při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
- pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

7.2.2 Elektronické podepisování e-mailů a dokumentů

- SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- Kde je možné, tak preferovat minimální délku otisku 384 bitů a vyšší

7.2.3 Ověřování integrity souborů

- SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- Kde je možné, tak preferovat minimální délku otisku 384 bitů a vyšší

7.3 Asymetrická kryptografie

7.3.1 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 a ANON 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
        - minimální délky klíčů:
            - pro Diffie-Hellman (DHE) - 3072 bitů
            - pro Elliptic Curve Diffie-Hellman (ECDHE) – 256 bitů
        - nesmí být použita anonymní výměna klíčů
    - algoritmy a funkce pro autentizaci
        - minimální délky klíčů:
            - RSA - 3072 bitů
            - DSA – 3072 bitů
            - 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 SHA2 funkce s minimální délkou hashe 256 bitů
        - vyšší délky otisků musí mít vyšší prioritu v cipher suites
- Certifikáty
    - minimální délka privátního klíče
        - RSA 3072 bitů
        - DSA 3072 bitů
        - ECDSA - 256 bitů
    - hash funkce pro podpis
        - SHA-2 s minimální délkou 256 bitů (případně SHA3 s délkou 256b)
    - v případě veřejně publikované webové aplikace (pokud VKB neurčí jinak)

- webová aplikace publikovaná přes WAF (webový aplikační FW)
  - certifikát určený pro navázání komunikace mezi klientem a WAF
    - Pro doménu kr-vysocina.cz
      - musí být vydaný důvěryhodnou certifikační autoritou
      - může se jednat o wildcard certifikát (*.kr-vysocina.cz)
      - nesmí mít platnost delší než 1 rok
      - wildcard certifikáty musí být uloženy pouze na WAF
    - Pro ostatní domény (mimo kr-vysocina.cz)
      - Může být vydaný Let´s encrypt certifikační autoritou
      - Může se jednat o DV certifikát
      - nesmí mít platnost delší než 1 rok
  - certifikát určený pro navázání komunikace mezi WAF a aplikací
    - je vydaný interní certifikační autoritou
    - je možné použít multi-domain certifikát
    - Nesmí mít platnost delší než 1 rok
- Webová aplikace publikovaná mimo WAF
  - Nesmí být použit wildcard certifikát druhého a nižšího řádu
    - Je přípustné použít wildcard certifikát čtvrtého a vyššího řádu, pakliže certifikát bude uložen pouze na 1 místě (VM)
  - Může se jednat o DV certifikát
  - Certifikát nesmí mít platnost delší než 1 rok
  - Může být vydaný Let´s encrypt certifikační autoritou

7.3.2 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
  - TLS_AES_128_CCM_8_SHA256

- TLS1.2:
  - "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384"
  - "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384"
  - "TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256"
  - "TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384"
  - "TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256"
  - "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256"
  - "TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384"

- "TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256"
- "TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256"
- "TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8"
- "TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8"
- "TLS_ECDHE_ECDSA_WITH_AES_256_CCM"
- "TLS_ECDHE_ECDSA_WITH_AES_128_CCM"
- "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
- "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
- "TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384"
- "TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256"
- "TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384"
- "TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256"
- "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"

7.3.3 Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
  - algoritmus DSA – 3072 bitů
  - algoritmus RSA - 3072 bitů (s využitím schéma PSS)
  - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
  - délka klíče minimálně 3072 bitů u RSA a DSA algoritmů
  - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky (např. ECDSA, Ed25519)

7.4 Symetrická kryptografie

- Mohou být použity tyto šifry (preference dle tohoto pořadí):
  - AES, Camellia, Serpent, ChaCha20, Twofish, Snow2.0, Snow 3G
- nesmí být použity tyto šifry:
  - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 256 bitů
  - ve výjimečných, odůvodněných a schválených případech může být délka klíče 128 nebo 192 b
  - 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