Kraj Vysočina

KUJIP01H8D2L

5461/19

SERVISNÍ SMLOUVA
Plánu pro zvládání sucha a stavu nedostatku vody Kraje Vysočina

uzavřená na základě dohody smluvních stran nikoliv na úkor ochrany kterékoliv ze smluvních stran ve smyslu § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník")

Číslo smlouvy Objednatele: 149408
Číslo smlouvy Dodavatele: .....

Článek 1
Smluvní strany

1. Kraj Vysočina

se sídlem:	Žižkova 1882/57, 586 01 Jihlava
zastoupený:	Mgr. Vítězslavem Schrekem, MBA, hejtmanem kraje
k podpisu smlouvy pověřen:	Ing. Lukáš Vlček, náměstek hejtmana kraje
IČO:	70890749
DIČ:	CZ70890749
bankovní spojení:	Sberbank CZ, a. s., Jihlava
číslo účtu:	4050005000/6800

(dále jen „Objednatel")

2. HYDROSOFT Veleslavín s.r.o.

se sídlem:	U Sadu 62/13, 162 00 Praha 6
statutární orgán:	Ing. Petr Hurych, jednatel
IČO:	61061557
DIČ:	CZ61061557
bankovní spojení:	Československá obchodní banka, a.s.
číslo účtu:	162295091/0300
plátce DPH:	ano
obchodní rejstřík:	Městský soud v Praze oddíl C, vložka 43062

(dále jen „Dodavatel")

Článek 2.
Předmět smlouvy

1. Předmětem smlouvy je poskytování servisní a technické podpory (dále jen „servisní služby") **„Plánu pro zvládání sucha a stavu nedostatku vody Kraje Vysočina"** (dále jen „Dílo") při zabezpečení jeho řádného fungování, provozu, údržby a aktualizací. Dílo bylo zpracováno podle smlouvy o dílo, která byla uzavřena mezi smluvními stranami.
2. Servisními službami se rozumí:
   a) Maintenance (pravidelná údržba);
   b) Technická podpora;
   c) Řešení incidentů.
3. Servisní služby zahrnují také následující služby Dodavatele:
   a) Provádění pomocí nástrojů vzdálené správy v součinnosti s Objednatelem kontrolu a potřebné servisní zásahy v Díle, v případě potřeby v místě Objednatele.
   b) Poskytování odborné pomoci bezprostředně související s řádným fungováním Díla a jeho aktualizacemi v součinnosti s Objednatelem, pokud o ni Objednatel požádá.
   c) Poskytnout Objednateli licenci na potřebný software zajišťující řádný provoz Díla.
   d) Provádění změn a úprav v Díle v rozsahu vyplývajících ze změn v právních předpisech, Metodice k přípravě plánů pro zvládání sucha a stavu nedostatku vody,

na základě jiné obecně známé skutečnosti nebo požadavků dle specifikace Objednatele.

e) Poskytování odborné pomoci prostřednictvím telefonické podpory a vzdáleného přístupu, bezprostředně související s řádným fungováním Díla kontaktní osobě Objednatele, pokud o ni požádá.

f) Školení Objednatele nebo jiných přizvaných osob pro práci s Dílem max. 1x ročně, pokud o ně Objednatel požádá.

g) Aktualizace dodané bezpečnostně provozní dokumentace dle potřeby, minimálně však 1x ročně.

4. Součástí servisních služeb jsou i práce v tomto článku smlouvy nespecifikované, které však jsou k řádnému provádění servisních služeb nezbytné a o kterých Dodavatel vzhledem ke své kvalifikaci a zkušenostem měl nebo mohl vědět. Provedení těchto prací však v žádném případě nezvyšuje touto smlouvou sjednanou cenu.
5. Servisní služby poskytované v rámci maintenance jsou přístup k opravným balíčkům, pravidelná profylaxe Díla, kontrola funkcí Díla, aktualizace a upgrade software, optimalizace, identifikace výkonnostních problémů apod., další preventivní činnosti, aktualizace dodané provozní dokumentace. Maintenance bude Dodavatel provádět tak, aby co možná nejvíce zamezil vzniku jakýchkoli incidentů, které by znemožňovaly řádné užívání Díla a aby byla splněna jeho dostupnost.
6. Servisní služby poskytované v rámci technické podpory jsou: konzultační služby, realizace požadavků Objednatele na novou funkcionalitu Díla.
7. Servisní služby poskytované v rámci řešení incidentů budou poskytovány podle čl. 5 odst. 7 této smlouvy. Odstraňování záručních vad se také řídí lhůtami uvedených v čl. 5 odst. 7 této smlouvy.

Článek 3
Cena a platební podmínky

1. Smluvní strany se dohodly, že cena za servisní služby dle této smlouvy je stanovena na částku **60 500 Kč** (slovy šedesáttisícpětset korun českých) včetně daně z přidané hodnoty (dále jen „DPH") za 1 kalendářní rok.

cena celkem bez DPH	50 000 Kč
DPH 21 %	10 500 Kč
cena celkem včetně DPH	**60 500 Kč**

2. Tato cena je stanovena jako cena konečná a úplná.
3. Dodavatel není oprávněn požadovat po Objednateli poskytnutí zálohy.
4. Dodavatel odpovídá za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy.
5. Sjednaná celková cena uvedená v čl. 3 odst. 1 této smlouvy je cenou nejvýše přípustnou, kterou je možné překročit pouze v případě zvýšení sazby DPH a to tak, že Dodavatel ke sjednané ceně bez DPH připočítá DPH v procentní sazbě odpovídající zákonné úpravě účinné k datu uskutečnitelného zdanitelného plnění.
6. Objednatel zaplatí dohodnutou cenu dle čl. 3 odst. 1 na účet Dodatele na základě faktury vystavené Dodavatelem za každý kalendářní rok od roku 2023. Fakturu zašle Dodavatel Objednateli vždy do 31. ledna příslušného kalendářního roku se splatností 30 dnů ode dne jejího prokazatelného doručení Objednateli. Faktura musí obsahovat veškeré náležitosti daňového dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH").
7. V případě, že faktura nebude obsahovat stanovené náležitosti nebo v ní nebudou správné údaje, je Objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět Dodavateli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě se

přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury.

8. Cena bude uhrazena Objednatelem Dodavateli mezibankovním převodem z bankovního účtu Objednatele na bankovní účet Dodavatele. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu Objednatele ve prospěch účtu Dodavatele. Účet Dodavatele uvedený v záhlaví smlouvy je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 109 odst. 2 písm. c) zákona o DPH.
9. Pokud se po dobu účinnosti této smlouvy Dodavatel stane nespolehlivým plátcem ve smyslu ustanovení § 109 odst. 3 zákona o DPH, smluvní strany se dohodly, že Objednatel uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Objednatelem takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované Dodavatelem.
10. Dodavatel souhlasí s tím, aby subjekty oprávněné dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího z této smlouvy s tím, že dodavatel umožní tuto kontrolu, a bude spolupůsobit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů.

Článek 4
Práva a povinnosti Objednatele

1. Objednatel se zavazuje zaplatit včas Dodavateli dohodnutou cenu dle čl. 3 odst. 6 této smlouvy.
2. Objednatel je povinen spolupracovat s Dodavatelem a poskytovat mu veškerou nutnou součinnost potřebnou pro řádné poskytování servisních služeb podle této smlouvy. Objednatel je povinen informovat Dodavatele o veškerých skutečnostech, které jsou nebo mohou být důležité pro poskytování servisních služeb dle této smlouvy.
3. Zjistí-li Objednatel, že Dodavatel provádí předmět plnění v rozporu se svými povinnostmi, je Objednatel oprávněn písemně vyzvat Dodavatele k odstranění závad a požadovat, aby předmět plnění prováděl řádně. Jestliže tak Dodavatel neučiní, je Objednatel oprávněn od této smlouvy odstoupit.

Článek 5
Práva a povinnosti Dodavatele

1. Dodavatel 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. Dodavatel se zavazuje řádně a včas dle dohodnutých termínů poskytovat servisní služby dle předmětu této smlouvy.
3. Dodavatel provádí servisní služby vzdálenou správou nebo přímo příjezdem pracovníka Dodavatele na místo plnění Objednatele.
4. Dodavatel je povinen po celou dobu účinnosti této smlouvy v případě poruchy Díla provádět obnovu provozu Díla včetně načtení dat ze zálohy potřebných pro řádný chod Díla.
5. Dodavatel eviduje průběh prací včetně časové náročnosti a tato evidence za kalendářní rok je každoročně zasílána emailem kontaktní osobě Objednatele do 31. ledna následujícího kalendářního roku, případně kdykoli na vyžádání Objednatelem.
6. Dodavatel je oprávněn zajistit provádění části servisních služeb poddodavateli, přičemž poddodavatel je povinen dodržovat veškeré podmínky dle této smlouvy.
7. Dodavatel není oprávněn tuto smlouvu poskytnout jiné osobě než Objednateli.

8. Dodavatel se zavazuje odstraňovat vady Díla podle kategorie incidentů a kategorie bezpečnostních zranitelností ve lhůtách uvedených níže v tabulce:

Kategorie	Popis (kategorie incidentů / kategorie bezpečnostních zranitelností dle obecného systému hodnocení zranitelností - otevřený standard CVSSv3 base score)	Doba vyřešení (pracovní dny)
Kritická	Situace, kdy dílo nebo část díla je zcela nefunkční, neumožňuje práci uživatelů s Dílem. Dílo obsahuje bezpečnostní zranitelnost s kritickou mírou závažnosti (zranitelnost dosáhne základního skóre 7,0 – 10,0 bodů).	2
Střední	Situace, kdy Dílo je částečně funkční, umožňuje částečné poskytování služeb, po přechodnou dobu se sníženým komfortem uživatelů, případně provizorním způsobem. Dílo obsahuje bezpečnostní zranitelnost se střední mírou závažnosti (zranitelnost dosáhne základního skóre 4,0 – 6,9 bodů).	10
Nízká	Nedostatky a vady drobného rozsahu, které nebrání užívání Díla, nicméně nejsou v souladu s požadovaným technickým stavem. Dílo obsahuje bezpečnostní zranitelnost s nízkou mírou závažnosti (zranitelnost dosáhne základního skóre 0 – 3,9 bodů).	20

9. Ostatní požadavky Objednatele provádí Dodavatel ve lhůtách stanovených po vzájemné dohodě.
10. Dodavatel je povinen dodržovat platné právní předpisy.
11. Dodavatel je povinen neporušovat autorská práva ani jiná vlastnická práva třetí strany.
12. Dodavatel se zaručuje, že veškeré vlastnosti Díla včetně jeho případných aktualizací budou po celou dobu účinnosti smlouvy v souladu s obecně platnými právními předpisy.

Článek 6
Součinnost smluvních stran, vzájemná komunikace

1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškerou součinnost a informace potřebné pro řádné plnění svých závazků vyplývajících z této smlouvy. Smluvní strany jsou povinny informovat se navzájem o všech jim známých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.
2. Smluvní strany jsou povinny plnit své závazky tak, aby nedocházelo k prodlení s plněním jednotlivých termínů stanovených v této smlouvě.
3. Veškerá komunikace mezi smluvními stranami v záležitostech této smlouvy bude probíhat prostřednictvím kontaktních osob. Každá ze smluvních stran má právo změnit kontaktní osobu, ale je povinna vyrozumět o této změně druhou smluvní stranu. Změna kontaktní osoby je vůči druhé straně účinná teprve okamžikem prokazatelného doručení takového vyrozumění.

   Kontaktními osobami za Objednatele jsou:
   Ing. Radek Zvolánek, email: zvolanek.r@kr-vysocina.cz, telefon: 564 602 363
   Ing. Petr Novák, email: novak.p@kr-vysocina.cz, telefon: 564 602 158
   Kontaktními osobami za Dodavatele jsou:
   Ing. Ivan Blažek, email: blazek@hv.cz, telefon: 220 611 045
   Ing. Petr Hurych, email: hurych@hv.cz, telefon: 220 611 045
4. Komunikace mezi kontaktními osobami bude uskutečňována přednostně emaily, v naléhavých případech telefonicky.
5. Doručování mezi smluvními stranami se uskutečňuje na adresy sídla uvedené v čl. 1 této smlouvy (dále jen „kontaktní adresy"). Smluvní strana má povinnost oznámit do 5 dnů druhé smluvní straně písemně změnu kontaktní adresy, popř. jiných údajů. Změna kontaktní adresy je vůči druhé smluvní straně účinná okamžikem, kdy o ní byla prokazatelně vyrozuměna. Do doby oznámení změny kontaktní adresy druhé smluvní

straně zůstává kontaktní adresou adresa uvedená v čl. 1 této smlouvy, resp. jiná kontaktní adresa, která byla druhé straně již dříve písemně oznámena.

6. Ukládá-li smlouva učinit a doručit některý dokument v písemné podobě, může být učiněn a doručen buď v listinné formě nebo (nemusí-li být takovýto dokument podepsán) v elektronické formě na dohodnutém médiu nebo elektronickou poštou na dohodnutou adresu.
7. Dodavatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů, tj. Dodavatel je povinen poskytnout požadované informace a dokumentaci zaměstnancům nebo zmocněncům pověřených orgánů a vytvořit výše uvedeným orgánům podmínky k provedení kontroly vztahující se k předmětu dle této smlouvy a poskytnout jim součinnost.

Článek 7
Bezpečnost informací

1. Dodavatel se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele uvedené v příloze č. 1 této smlouvy.
2. Dodavatel 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 Objednatele prostřednictvím Dodavatele.
3. Dodavatel 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 seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Dodavatele veřejně přístupnými stanou (dále jen „důvěrné informace"). Dodavatel 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 Objednatel povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění Dodavatele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Objednatel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené Dodavateli právním předpisem nebo rozhodnutím orgánu veřejné moci.

Článek 8
Smluvní sankce

1. Pro případ prodlení se zaplacením smluvní ceny je Objednatel povinen Dodavateli uhradit smluvní pokutu ve výši 0,05 % z dlužné částky za každý den prodlení.
2. Nedodrží-li Dodavatel z vlastní viny plnění předmětu této smlouvy, má povinnost uhradit škodu prokazatelně způsobenou Objednateli.
3. V případě prodlení Dodavatele s provedením servisní služby dle této smlouvy je Objednatel oprávněn požadovat na Dodavateli a Dodavatel je povinen uhradit Objednateli smluvní pokutu ve výši 500 Kč za každý den prodlení.
4. Za nesplnění kterékoliv povinnosti obsažené v čl. 7, je Objednatel oprávněn účtovat Dodavateli smluvní pokutu ve výši 100 000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku.
5. Zaplacením smluvní pokuty není dotčeno právo poškozené strany na náhradu škody.
6. Výši smluvních pokut považují obě smluvní strany za přiměřenou. Smluvní pokuta je splatná do 30 dnů od doručení jejího vyúčtování.

Článek 9
Trvání a ukončení smlouvy

1. Tato smlouva je uzavřena na dobu neurčitou a to od převzetí díla Objednatelem dle smlouvy o dílo.
2. Platnost smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran.
3. Kterákoliv ze smluvních stran může od této smlouvy odstoupit z důvodu podstatného porušení povinností vyplývajících z této smlouvy druhou smluvní stranou a z dalších důvodů stanovených touto smlouvou. Odstoupení od smlouvy nabývá účinnosti dnem následujícím po dni prokazatelného doručení jeho písemného vyhotovení druhé smluvní straně.
4. Objednatel je oprávněn od této smlouvy písemně odstoupit:
   a) pokud bylo vůči Dodavateli zahájeno insolvenční řízení, včetně případů, kdy byl na majetek Dodavatele vyhlášen konkurs nebo byl insolvenční návrh zamítnut pro nedostatek majetku, nebo Dodavatel vstoupil do likvidace;
   b) pokud má Dodavatel prodlení s plněním povinností dle této smlouvy o více než 30 dní, pokud toto prodlení způsobil Dodavatel, na které byl Objednatelem nejméně dvakrát upozorněn.
5. Dodavatel je oprávněn od této smlouvy písemně odstoupit, pokud má Objednatel prodlení s úhradou faktur podle této smlouvy o více než 30 dní.
6. Odstoupením od smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, ochrany důvěrných informací a ustanovení týkajících se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení od smlouvy.
7. Jestliže některá ze smluvních stran odstoupí od smlouvy o dílo na zpracování Díla nebo smlouva o dílo bude jinak ukončena, aniž by dílo bylo zpracováno, tato smlouva zaniká v den účinnosti odstoupení od smlouvy o dílo.
8. V případě odstoupení od smlouvy předá Dodavatel Objednateli manuál a zdrojové formy Díla včetně dalších potřebných dat a informací pro provoz Díla a to v takové formě, kterou Objednatel odsouhlasí.

Článek 10
Závěrečná ustanovení

1. Výběr Dodavatele byl proveden v souladu s Pravidly Rady Kraje Vysočina pro zadávání veřejných zakázek ze dne 29. 6. 2021 č. 05/21.
2. V záležitostech touto smlouvou přímo neupravených se smluvní strany dohodly, že se jejich vzájemná práva a povinnosti budou řídit příslušnými ustanoveními občanského zákoníku.
3. Tuto smlouvu je možné měnit pouze písemnými vzestupně číslovanými dodatky podepsanými oprávněnými zástupci obou smluvních stran.
4. Tato smlouva byla sepsána ve dvou stejnopisech, z nichž každý má povahu originálu a každá smluvní strana obdrží jeden z nich.
5. Nedílnou součástí této smlouvy je příloha č. 1 Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele.
6. Tato smlouva nabývá platnosti dnem jejího podpisu smluvními stranami a účinnosti dnem 1. 1. 2023. Dodavatel výslovně souhlasí se zveřejněním celého textu této smlouvy včetně podpisů v informačním systému veřejné správy – Registru smluv. Smluvní strany se dohodly, že smlouvu v Registru smluv zveřejní Objednatel.
7. Smluvní strany prohlašují, že tato smlouva byla sepsána dle jejich pravé a svobodné vůle, že si ji před jejím podpisem přečetly a s celým jejím obsahem souhlasí.

Za Objednatele

V Jihlavě dne 14. 12. 2021

Kraj Vysočina
Žižkova 1882/57, 586 01 Jihlava
28

....

Ing. Lukáš Vlček
náměstek hejtmana kraje

Za Dodavatele

V JIHLAVĚ dne 2.12.2021

....

Ing. Petr Hurych
jednatel společnosti

hydrocoft Veleslavín
U Sadu 13, 162 00 Praha 6

Příloha č. 1 servisní smlouvy „Plánu pro zvládání sucha a stavu nedostatku vody Kraje Vysočina“

Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele

1. **Bezpečnost přístupových oprávnění**
   - Dodavatel je povinen chránit veškeré své přístupové údaje k informačním aktivům Objednatele včetně přístupů k informačním aktivům Dodavatele, které umožňují přístup k informačním aktivům Objednatele či umožnují jejich správu.
   - Dodavatel 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.
   - Dodavatel je povinen pro výše uvedené přístupy 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 Dodavatel zřizoval přístupová oprávnění třetí straně, je Dodavatel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.
2. **Řízení kybernetických bezpečnostních incidentů**
   - Dodavatel 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.
   - Dodavatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Objednatele.
3. **Řízení změn**
   - Dodavatel se zavazuje zaznamenávat všechny změny, které v informačním aktivu provedl.
   - Dodavatel 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.
   - Dodavatel se zavazuje všechny jím provedené změny i změny případných subdodavatelů poskytnout zadavateli formou pravidelného čtvrtletního reportu.
4. **Kryptografie:**

Dílo musí splňovat níže uvedené požadavky pouze u těch operací/akcí, které jsou pro Dílo aplikovatelné.

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 tzv. pomalé hashovací funkce:
  - Argon2i
  - bcrypt
  - scrypt
  - PBKDF2
- 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.

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

<u>Symetrická kryptografie</u>

- 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