SMLOUVA O POSKYTOVÁNÍ SLUŽEB

SPRÁVA INFORMAČNÍCH TECHNOLOGIÍ MĚSTA PLZNĚ, příspěvková organizace
se sídlem: Dominikánská 4, 301 00 Plzeň
IČ: 66362717
bankovní spojení: xxx
Jednající: Ing. Luděk Šantora, MBA, ředitel
Dále pro účely této smlouvy jako poskytovatel nebo dodavatel

a

VODÁRNA PLZEŇ a.s.
se sídlem: Malostranská 143/2, Doudlevce, 326 00 Plzeň
IČ: 25205625
bankovní spojení: xxx
Jednající: Ing. Jiří Kozohorský, MBA, generální ředitel
Dále pro účely této smlouvy jako objednatel nebo organizace

objednatel a poskytovatel dále též společně označování jako smluvní strany, nebo účastníci smlouvy

uzavřely níže uvedeného dne, měsíce a roku tuto smlouvu o poskytování služeb ve smyslu ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění

1. PŘEDMĚT A CENA PLNĚNÍ

1.1. Předmětem plnění této smlouvy je poskytování služeb objednateli poskytovatelem, a to v rozsahu a za podmínek stanovených touto smlouvou a přílohou číslo 1 této smlouvy.
1.2. Cena za předmět plnění je stanovena dohodou smluvních stran takto:
  1.2.1. paušální ceny za služby uvedené v příloze číslo 1 smlouvy bod 3 jsou uvedeny v příloze číslo 1 smlouvy v bodu 3.7.1;
  1.2.2. ceny za služby uvedené v příloze číslo 1 smlouvy bod 3 jsou uvedeny v příloze číslo 1 smlouvy v bodu 3.7.2. Rozsah skutečného čerpání těchto služeb stanoví oprávněné osoby dle této smlouvy dohodou vždy první pracovní den měsíce následujícího po měsíci, ve kterém byly služby poskytnuty. Bez dohody oprávněných osob o rozsahu skutečného čerpání služeb nevzniká nárok poskytovatele na úhradu ceny nad rámec roční ceny;
  1.2.3. ceny za zřízení služby uvedené v příloze číslo 1 smlouvy body 3.6.b) a 3.6.d) jsou uvedeny v příloze číslo 1 smlouvy v bodu číslo 3.7.3.
1.3. Cena dle bodu 1.2.1. a 1.2.2. může být navýšena maximálně o míru inflace vyjádřenou indexem spotřebitelských cen zveřejněnou za uplynulý rok Českým statistickým úřadem.

2. DOBA A MÍSTO PLNĚNÍ SMLOUVY

Plnění dle této smlouvy bude poskytováno průběžně ode dne účinnosti této smlouvy po celou dobu její účinnosti. Místem plnění jsou sídla, provozovny a objekty objednatele a poskytovatele uvedené v příloze č. 3 této smlouvy.

3. PRÁVA A POVINNOSTI VZTAHUJÍCÍ SE K PŘEDMĚTU PLNĚNÍ

3.1. V kontextu předmětu a rozsahu plnění této Smlouvy, doby trvání smluvního vztahu a znění Zákona č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti) a vyhlášky č. 82/2018 Sb., si je poskytovatel vědom, že se podpisem této Smlouvy stává z pohledu Zákona o kybernetické bezpečnosti pro objednatele Významným poskytovatelem. V této souvislosti, byla před podpisem této smlouvy provedena identifikace dotčených podpůrnách aktiv, která jsou nedílně spjaty s primárním aktivem. V rámci tohoto smluvního vztahu je soubor těchto podpůrných aktiv označován jako aktiva spadající do kritické kategorie. K podpůrným aktivům, která nebyla explicitně zařazena mezi aktiva spadající do kritické kategorie se přistupuje jako k běžným podpůrným aktivům. Toto rozdělení je uvedeno v příloze č. 5 této smlouvy.
3.2. Objednatel i poskytovatel se v této souvislosti zavazují postupovat plně v souladu s vyhláškou č. 82/2018 Sb.

3.3. Poskytovatel je povinen pří poskytování služeb dodržovat relevantní bezpečnostní politiky Objednatele.
   3.3.1. Všechny bezpečnostní politiky Objednatele budou vydávány v souladu s požadavky č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti) a vyhlášky č. 82/2018 Sb.
   3.3.2. Veškeré platné bezpečnostní politiky budou přístupné Poskytovateli v elektronické podobě na společném uložišti, k tomu určeném.
   3.3.3. Každá nově připravovaná bezpečnostní politika Objednatele, bude před jejím vydáním předána do revizního procecu oprávněné osobě Poskytovatele, aby bylo možné ze strany Poskytovatele provést pozouzení dopadu zaváděných změn na rozsah a způsob poskytovaných služeb na základě této smlouvy.
   3.3.4. Nově vydané bezpečnostní politiky se v kontextu této smlouvy stávají účinné 15 dnů po jejich schválení Poskytovatelem a vydáním ze strany Objednatele a jejich vložením na společné uložiště, k tomu určeném.

3.4. Smluvní strany činí k předmětu plnění nesporné, že si jsou vědomi, že podstatná část plnění vyplývající z této Smlouvy, je a i v budoucnu bude ovlivněna konkrétním zněním bezpečnostních politik Objednatele, z tohoto důvodu bude mít v případě rozdílného výkladu mezi touto Smlouvou a schválenou bezpečnostní politikou Objednatele přednost schválená a vydaná bezpečnostní politika Objednatele.

4. FAKTURACE

4.1. Daňové doklady (faktury) za služby dle této smlouvy budou poskytovatelem vystaveny měsíčně, a to:
   4.1.1. na 1/12 ceny uvedené v bodě 1.2.1. této smlouvy;
   4.1.2. na cenu uvedenou v bodě 1.2.2. smlouvy podle skutečného čerpání těchto služeb;
   4.1.3. poskytovatel je povinen vystavit každou fakturu do 10. kalendářního dne měsíce následujícího po měsíci, ve kterém byly služby poskytovány.

4.2. Daňové doklady (faktury) za služby dle bodu 1.2.3. budou vystaveny poskytovatelem po akceptaci poskytnuté služby.

4.3. Doba splatnosti daňových dokladů je 21 kalendářních dnů ode dne doručení daňového dokladu objednateli.

4.4. Platby budou probíhat výhradně v Kč a rovněž veškeré cenové údaje budou v této měně.

4.5. Překročení cen je možné pouze zákonnou změnou sazeb DPH.

4.6. Každá faktura musí obsahovat náležitosti daňového dokladu dle ustanovení příslušných obecně závazných předpisů platných na území České republiky, a dále číslo této smlouvy.

4.7. Poskytovatel se zavazuje, že na jím vydaných daňových dokladech bude uvádět pouze čísla bankovních účtů, která jsou správcem daně zveřejněna způsobem umožňujícím dálkový přístup (§ 98 písm. d) zákona č.235/2004 Sb., o dani z přidané hodnoty. V případě, že daňový doklad bude obsahovat jiný než takto zveřejněný účet, bude takovýto daňový doklad považován za neúplný a objednatel vyzve poskytovatele k jeho doplnění. Do okamžiku doplnění si objednatel vyhrazuje právo neuskutečnit platbu na základě tohoto daňového dokladu.

4.8. V případě, že kdykoli před okamžikem uskutečnění platby ze strany objednatele na základě této smlouvy bude o poskytovateli správcem daně z přidané hodnoty zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že poskytovatel je nespolehlivým plátcem (§ 106a zákona č.235/2004 Sb., o dani z přidané hodnoty), má objednatel právo od okamžiku zveřejnění ponížit všechny platby poskytovateli uskutečňované na základě této smlouvy o příslušnou částku DPH. Smluvní strany si sjednávají, že takto poskytovateli nevyplacené částky DPH odvede správci daně sám objednatel v souladu s ustanovením § 109a zákona č. 235/2004 Sb.

4.9. Poskytovatel je oprávněn fakturovat objednateli v písemné, tedy v tištěné podobě, nebo v elektronické podobě. Písemná faktura se doručuje na adresu objednatele. Elektronická faktura se doručuje elektronicky na emailovou adresu: xxx

5. OPRÁVNĚNÉ OSOBY, SOUČINNOST A KOMUNIKACE

5.1. Každá ze smluvních stran jmenuje oprávněnou osobu ve věcech technických, které jsou uvedeny v příloze číslo 1 této smlouvy. Oprávněné osoby ve věcech smluvních jsou uvedeny v záhlaví této smlouvy.

5.2. Smluvní strany spolu budou komunikovat buď písemně na adrese stanovené v záhlaví této smlouvy, nebo prostřednictvím oprávněných osob.

5.3. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.
5.4. Smluvní strany jsou povinny plnit své závazky vyplývající z této smlouvy tak, aby nedocházelo k prodlení s plněním termínů a s prodlením splatnosti jednotlivých peněžních závazků.

6. ODPOVĚDNOST ZA ŠKODU (§ 2913 Z.Č. 89/2012)

6.1. Poskytovatel odpovídá za činnosti svých zaměstnanců, popřípadě dalších fyzických osob vykonávajících práci v jeho prospěch pro Objednatele v rozsahu této Smlouvy. Všechny vykonáváné úkony musí být v souladu s bezpečnostními politikami Objednatele nebo instrukcemi dodavatelů spravovaných aktiv v souladu s touto Smlouvou. Veškeré škody, které vzniknou porušením bezpečnostních politik zaměstnanci Poskytovatele nebo dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, jdou k tíži Poskytovatele.
6.2. Poruší-li strana povinnost ze smlouvy, nahradí škodu z toho vzniklou druhé straně nebo i osobě, jejímuž zájmu mělo splnění ujednané povinnosti zjevně sloužit.
6.3. Povinnosti k náhradě se škůdce zprostí, prokáže-li, že mu ve splnění povinnosti ze smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním smluvené povinnosti v prodlení, ani překážka, kterou byl škůdce podle smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí.
6.4. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této smlouvy. Smluvní strany se zavazují vyvíjet maximální úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

7. OCHRANA OSOBNÍCH ÚDAJŮ

7.1. Objednatel tímto informuje poskytovatele a jeho zástupce, že osobní údaje jsou zpracovávány v souladu s Informacemi o zpracování osobních údajů dodavatelů a smluvních partnerů, které jsou dostupné na webu objednatele v sekci GDPR na webovém portálu Objednatele. V tomto dokumentu jsou také uvedeny informace o účelech a době zpracování, právních titulech a o právech, které v souvislosti se zpracováním osobních údajů subjektům údajů náleží.
7.1.1. Jakékoliv aktualizace související dokumentace bude oznámena oprávně osobě Poskytovatele elektronicky nejpozději v době jejího zveřejnění.
7.2. Každá ze Smluvních stran informuje své zaměstnance dotčené toutou smlouvou a případné a další subjekty údajů o zpracování osobních údajů druhou smluvní stranou. Objednatel zpracovává osobní údaje v souladu s Informacemi o zpracování osobních údajů dodavatelů a smluvních partnerů dle předchozího odstavce.
7.3. Smluvní strany se touto smlouvou zavazují učinit veškerá smluvní, organizační a technická opatření zabraňující zneužití či prozrazení osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně osobních údajů (GDPR) a zákona o ochraně osobních údajů č. 110/2019 Sb.
7.4. S ohledem na předmět této smlouvy bude poskytovatel během plnění této smlouvy zpracovávat osobní údaje zaměstnanců a pracovníků objednatele, stejně jako dalších osob, které budou pracovat se Systémem, a za tímto účelem se Smluvní strany dohodly uzavřít ve smyslu čl. 28 odst. 3 Nařízení 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) (dále jen „GDPR“) ujednání o zpracování osobních údajů, které tvoří Přílohu číslo 4 této Smlouvy.

8. OCHRANA DŮVĚRNÝCH INFORMACÍ

8.1. Smluvní strany se touto smlouvou zavazují učinit veškerá smluvní, organizační a technická opatření zabraňující zneužití či prozrazení důvěrných informací, a to zejména:
8.1.1. informací, které tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení (obchodní tajemství dle § 504 Z.Č. 89/2012);
8.1.2. informace provozního nebo technického charakteru týkající se vodohospodářského majetku a činnosti nad ním prováděných.

8.2. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:
8.2.1. si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen „Důvěrné informace“);
8.2.2. mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé Smluvní strany nebo i jejím opomenutím přístup k Důvěrným informacím druhé Smluvní strany.
8.3. Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě Důvěrné informace, které při plnění této Smlouvy získala od druhé Smluvní strany.

9. DŮSLEDKY PORUŠENÍ SMLUVNÍCH POVINNOSTÍ

9.1. V případě nedodržení sjednaných parametrů kvality dodaného plnění uvedených v přílohách této smlouvy vzniká objednateli vůči poskytovateli nárok na smluvní pokutu v závislosti na míře neplnění kvality jednotlivých služeb. Rozsah smluvních pokut je uveden v Příloze číslo 1 této smlouvy.
9.2. Celková výše smluvní pokuty dle této smlouvy se vypočte měsíčně jako součet jednotlivých dílčích smluvních pokut za nedodržení smluvené kvality jednotlivých služeb poskytovaných dle této smlouvy.
9.3. Byly-li naplněny podmínky pro vznik smluvní pokuty dle odst. 6.1 a příloh této smlouvy, je poskytovatel povinen provést výpočet její výše a předat podklady pro její vyúčtování oprávněné osobě ve věcech technických objednatele. Schválením těchto podkladů oběma stranami vzniká povinnost poskytovatele ponížit v nejbližší fakturaci fakturovanou částku o výši smluvní pokuty. Nedojde-li k odsouhlasení celkového rozsahu smluvní pokuty dle této smlouvy, je poskytovatel povinen ponížit v nejbližší fakturaci fakturovanou částku o výši smluvní pokuty v rozsahu, který není smluvními stranami rozporován. Konečné vyúčtování bude provedeno smluvními stranami po odstranění rozporů.

10. PLATNOST A ÚČINNOST SMLOUVY

10.1. Tato smlouva je uzavřena na dobu neurčitou, nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění v registru smluv, které je povinen zajistit poskytovatel.
10.2. Obě smluvní strany jsou oprávněny ukončit tuto smlouvu (vedle zákonem stanovených důvodů):
- dohodou smluvních stran;
- výpovědí bez udání důvodu s výpovědní lhůtou 6 měsíců. Lhůta počíná běžet prvním dnem měsíce následujícího po prokazatelném doručení výpovědi.

10.3. Po dobu výpovědní lhůty je poskytovatel služeb povinen objednateli, případně jím určené osobě nebo subjektu, poskytnout plnou součinnost při předání veškerých informací souvisejících se službami poskytovanými na základě této smlouvy objednateli ve strojově čitelném formátu.
10.4. Smluvní strany se dohodly, že tato smlouva dnem své účinnosti ukončuje platnost a účinnost smlouvy o poskytování služeb mezi smluvními stranami této smlouvy ze dne 24.9.2021, vedená u poskytovatele pod číslem 2021/SITMP/0139.

11. ŘEŠENÍ SPORŮ

11.1. Práva a povinnosti Smluvních stran touto smlouvou výslovně neupravené se řídí zák. č. 89/2012 Sb., občanským zákoníkem, v platném znění a příslušnými právními předpisy souvisejícími.
11.2. Smluvní strany se zavazují řešit případné spory vzniklé na základě této smlouvy přednostně dohodou.
11.3. Pokud se případný spor z této smlouvy nepodaří vyřešit smírně, všechny spory vznikající z této smlouvy a v souvislosti s ní přitom budou rozhodovány soudy.

12. ZÁVĚREČNÁ USTANOVENÍ

12.1. Tato smlouva byla sepsána ve dvou vyhotoveních, každá ze smluvních stran obdrží jedno vyhotovení.
12.2. Tuto smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této smlouvy, podepsaných oprávněnými zástupci obou smluvních stran.
12.3. Tato smlouva představuje úplnou dohodu smluvních stran o předmětu této smlouvy.

12.4. Účastníci smlouvy prohlašují, že si smlouvu přečetli a shledali, že byla sepsána podle jejich pravé, svobodné a vážně míněné vůle, prosté omylu, a že nebyla ujednána v tísni, za nápadně nevýhodných podmínek. Na důkaz toho smlouvu podepisují

Přílohy:
Příloha číslo 1 – Specifikace služeb
Příloha číslo 2 – Obecné principy v oblasti kybernetické bezpečnosti
Příloha číslo 3 – Sídla, provozovny a objekty objednatele a poskytovatele
Příloha číslo 4 – Kategorizace podpůrných aktiv

V Plzni dne: 21.9.2023

……
Ing. Jiří Kozohorský, MBA
generální ředitel

V Plzni dne: 26.9.2023

……
Ing. Luděk Šantora, MBA
ředitel

Příloha číslo 1 – Specifikace služeb

1. ÚVOD

Tento dokument obsahuje specifikaci poskytovaných služeb, které zajišťují pracovníci SPRÁVY INFORMAČNÍCH TECHNOLOGIÍ MĚSTA PLZNĚ nebo pověřená třetí osoba společnosti VODÁRNA PLZEŇ a.s..

Oprávněné osoby ve věcech technických dle čl. 4 těla smlouvy:

Oprávněná osoba poskytovatele:
Ing. Bohuslav Horais, xxx
Ing. Tomáš Krblich, xxx
Ing. Libor Červený, xxx

Oprávněná osoba objednavatele:
Ing. Jan Taušl, xxx

2. POUŽITÉ ZKRATKY

Zkratka	Popis
SITMP	SPRÁVA INFORMAČNÍCH TECHNOLOGIÍ MĚSTA PLZNĚ, příspěvková organizace
SLA	Service Level Agreement – Smlouva o úrovni/kvalitě poskytovaných služeb
VP	VODÁRNA PLZEŇ a.s.

3. POSKYTOVANÉ SLUŽBY

Předmětem poskytovaných služeb je správa IT infrastruktury (mimo technologickou část provozu), technická podpora uživatelů, řízení bezpečnosti, technická podpora aplikací a projektové řízení ICT projektů. Pro všechny níže uvedené body je povinností Poskytovatele zajistit předání dokumentace, operačních postupů, zdrojových kódů (v případě, že se jedná o vývoj skriptů a aplikací na míru), adresních plánů a přístupových údajů do jednotlivých prvků v síti do rukou oprávněné osoby objednatele.

3.1 Zajištění podpory aplikací

Správu centrálních aplikací primárně řeší zaměstnanci VP – správci aplikací. SITMP ve spolupráci se správci aplikací zajišťuje tyto činnosti:

- správa operačních systému aplikačních a databázových serverů
- zálohování serverů
- instalace aplikací na servery
- povolení potřebné komunikace v počítačové síti VP
- nastavování přístupů k serverům správcům aplikací a externím dodavatelům

3.2 Rozvoj informačního systému

Zajištění rozvoje informačního systému VP s ohledem na firemní a globální podnikové strategie:

- Příprava podkladů pro plánu investic

- Návrhy změn informačního systému
- Součinnost při výběru a implementaci nových informačních systémů

Zajištění rozvoje infrastruktury (počítačová síť, servery) informačního systému:

- Příprava podkladů pro plánu investic
- Návrhy změn infrastruktury informačního systému
- Součinnost při výběru a implementaci nové infrastruktury informačního systému

Zajištění rozvoje komunikačních technologií:

- Příprava podkladů pro plánu investic
- Návrhy změn komunikačních technologií
- Součinnost při výběru a implementaci nových komunikačních technologií

Podpora Objednatele při realizaci výběrových řízení v oblasti ICT a implementaci nových komponent

- Revize Zadávacích dokumentací
- Účast v implementačních týmech
- Technická podpora při technických analýzách, testování a implementaci

Veškeré činnosti související s rozvojem informačních systémů, infrastruktury a komunikační technologie budou probíhat v souladu s bezpečnostní politikou řízení změn Objednatele.

3.3 Security management

Poskytované služby:

Spolupráce s Objednatelem při analýze bezpečnostních rizik a jejich dopadů na činnost společnosti. Charakterizuje systémové požadavky, procesy a vzájemné závislosti tak, aby bylo možno determinovat požadavky a priority havarijního plánování.

Součinnost při zavádění bezpečnostních politik a specifikace bezpečnostních standardů společnosti, které budou opřeny o doporučení metodicko-regulačního úřadu NUKIB a dále pak reflektování celosvětově uznávaných standardů NIST a CIS.

Spolupráce s Objednatelem při implementaci ISMS.

Součinnost při zabezpečení ICT (zabezpečení serverů, stanic, vnitřní sítě, nastavení komunikačních standardů, QoS – Quality of Services).

Zajištění podpory při aplikaci bezpečnostní politiky a bezpečnostních standardů. Bezpečnostní standardy by měly vycházet z doporučení NIST, případně CIS.

Tvorba a kontrola dodržování personální bezpečnosti

- řízení přístupu k datům,
- určení zodpovědností osob s ohledem na bezpečnost,
- kontrola dodržování zákonných norem pro práci s osobními informacemi.

Spolupráce s Objednatelem při vytváření a realizaci strategie obnovy klíčových IT/IS systému ve správě Poskytovatele a revize a podpora Objednatele při sestavovávní a realizaci strategie obnovy klíčových IT/IS systémů, které nejsou ve správě Poskytovatele. Součastí bude specifikace parametrů pro každý strategicky významný IS, informací a dalších zdrojů, které jsou nutné pro zajištění procesu obnovy tohoto IS (navrácení do původního stavu). Spolupráce s Objednatelem při vytvoření havarijních plánů organizace proti:

- cíleným útokům na informační systém,
- virové nákazy, spamu, DoS útokům, hackování,
- neúmyslnému selhání obsluhy s důsledkem výpadku informačního systému,
- nedostatku obslužného personálu,

- výpadku subPoskytovatele (elektrické energie, plynu,…),
- poruchy internetové konektivity,
- ztrátě dat nebo poruchy jejich konzistence,
- přírodní nebo technické/technologické havárie.

Hlášení a řešení bezpečnostních incidentů ve spolupráci s MKB Objednatele

.Spolupráce s Objednatelem při vytvoření hardening standardů a jejich aplikace do prostředí pro systémy, které jsou ve správě Poskytovatele a podpora Objednatele při jejich zavádění s ostatními Dodavateli informačních systémů.

3.4 Technická podpora uživatelů

Poskytované služby:

Koordinace nákupu hardware, software (jednouživatelský SW, který není součástí komplexního SW) a služeb

- Nákup a řešení hardware (HW) na základě dlouhodobého plánu obnovy techniky
- Nákup HW na základě specifikovaných požadavků ze strany zákazníka
- Nákup software (SW) na základě dlouhodobého plánu
- Nákup SW na základě schváleného požadavku
- Konzultační služba a rada při řešení práce na výpočetní technice, doporučení např. nákupů HW a SW

Poskytování součinnosti při relokace hardwaru Objednatele.

Tiskové služby (spolupráce s externím Poskytovatelem tiskového řešení + instalace tiskáren na koncové stanice)

Správa licencí

- Předání nebo zavedení placených komerčních licencovaných programů a jejich čísel do evidence dle nastavených pravidel vč. zajištění, že nebude instalován SW, který není licenčně správně zakoupen nebo v případě free verze podporován pro komerční využití.

Služby pracovníků IT

- Příprava a instalace výpočetní techniky dle plánu obnovy a předání koncovému uživateli
- Instalace uživatelského SW na koncové stanice dle rozdělení a nároků
- Servisní podpora koncového uživatele na výpočetní technice (VT) v případě poruchy na základě zadaného servisního požadavku do konečného vyřešení dle SLA
- Získávání informací ze strany koncového uživatele k zefektivnění práce na VT vč. návrhů řešení SW
- Komunikace a zajištění podpory v případě řešení požadavků na komplexní SW s ostatními úseky – předávání informací na správná místa
- Podpora mobilních zařízení, které přistupují do interní sítě Objednatele

3.5 Správa serverů a sítě (infrastruktura)

Poskytované služby:

Koordinace nákupu hardware, software a služeb z oblasti infrastruktury

- Příprava podkladů pro nákup a řešení hardware (HW) na základě dlouhodobého plánu Vodárny a.s., popř. jednorázových požadavků. (samotný nákup HW není součástí této služby, HW si pořizuje Vodárna Plzeň a.s. ze svých zdrojů)
- Příprava podkladů pro nákup software (SW) na základě dlouhodobého plánu Vodárny a.s., popř. jednorázových požadavků. (samotný nákup SW není součástí této služby, SW si pořizuje Vodárna Plzeň a.s. ze svých zdrojů)
- Příprava podkladů pro nákup služeb na základě dlouhodobého plánu Vodárny a.s., popř. jednorázových požadavků. (samotný nákup služeb není součástí této služby, SW si pořizuje Vodárna Plzeň a.s. ze svých zdrojů)

Správa internetového připojení

- Konfigurace internetového připojení a zajištění požadované konektivity

Správa sítí,WiFi a bezpečnosti sítě

- Konfigurace aktivních prvků, firewallů a správa síťového prostředí
- Konfigurace bezdrátových sítí a zapojení wifi AP
- aktualizace SW a firmware zařízení
- správa pronajatých datových okruhů
- proaktivní monitoring zvěřejňovaných zranitelností síťových prvků, implementace bezpečsnostních aktualizaci a jejich aplikace do produkčního prostředí po řádném testování

Správa serverů a diskových polí

- instalace, reinstalace, nastavení a správa serverového prostředí (fyzického i virtuálního)
- instalace, reinstalace, nastavení a správa diskových polí
- aktualizace SW a firmware zařízení

Správa licencí

Bezdrátové spoje

- Zajištění technické podpory Objednatele při řešení žádostí o oprávnění k využívání rádiových kmitočtů
- Zajištění technické podpory Objednatele při jednání s ostatními Dodavateli

Elektronická pošta

- Instalace, konfigurace a správa prostředí el. Pošty
- Ochrana proti emailovým podvodům zavedením adekvátních ochran poštovních systémů v souladu s „best effort“

Pevná telefonie

- Zajištění podpory a servisu tel. ústředen a telefonů

Mobilní telefonie

- Zajištění podpory

Vzdálený přístup do sítě

- Instalace, konfigurace a správa vzdáleného přístupu pro uživatele a externí Poskytovatele

Zálohování a obnova dat

- Instalace, konfigurace a správa zálohování
- Kontrola funkčnosti záloh minimálně 1x za měsíc/kvartál/rok
- Záloha pracovních dat na zálohovací server a externí zálohovací médium

Filtrace SPAMu

- Instalace, konfigurace a správa SPAM filterů

Technická podpora ostatních oblastí (IoT, technologické provozy atd.)

- Zajistění technické podpory Objednatele při jednání s ostatními Dodavateli zajišťujícími provoz nebo rozvoj IoT, technologických provozů, aplikací atd.

3.6 Správa a podpora aplikací

Poskytované služby:

a) DMS ELO

Správu aplikace DMS ELO primárně řeší SITMP určenými zaměstnanci – správci aplikace. SITMP ve spolupráci se zaměstnanci VP zajišťuje tyto činnosti:

- provoz a údržba serverového prostředí aplikace
- zajištění nastavení klientských stanic VP pro provoz aplikace
- zajištění funkčnosti vazeb DMS ELO s dalšími aplikacemi VP
- nastavování přístupů do aplikace na základě žádostí VP
- řešení uživatelských požadavků na provoz a úpravy aplikace
- podpora a školení uživatelů aplikace
- komunikace s Poskytovatelem aplikace

b) Aplikace pro schvalování práv

- provoz a údržba serverového prostředí aplikace
- zajištění nastavení klientských stanic VP pro provoz aplikace
- nastavování přístupů do aplikace na základě organizační struktury a určení metodiků aplikací VP
- řešení uživatelských požadavků na provoz a úpravy aplikace
- podpora a školení uživatelů aplikace

c) Aplikace poskytování elektronických podpisů – SOFA602 (klíčenka)

- provoz a údržba serverového prostředí aplikace
- zajištění nastavení klientských stanic VP pro provoz aplikace
- nastavování přístupů do aplikace na základě žádostí VP
- řešení uživatelských požadavků na provoz a úpravy aplikace
- podpora a školení uživatelů aplikace
- komunikace s Poskytovatelem aplikace
- cena za poskytování elektronických podpisů vč. aplikace a certifikovaného úložiště je měsíčně 599,- Kč měsíčně bez DPH

d) Aplikace rezervační systém pro cisterny

- provoz a údržba serverového prostředí aplikace
- zajištění nastavení klientských stanic VP pro provoz aplikace
- nastavování přístupů do aplikace na základě organizační struktury a určení metodiků aplikací VP
- řešení uživatelských požadavků na provoz a úpravy aplikace
- podpora a školení uživatelů aplikace

3.7 Cena za služby

3.7.1 Paušální ceny:

3.7.1.1 roční cena za služby uvedené mimo body 3.6 b), c) a d) činí 6 097 000,- Kč bez DPH. Rozsah těchto služeb je dán kapacitou 6 pracovníků IT a jejich pracovním zařazením a pracovní náplní vyplývající ze smluvního vztahu s poskytovatelem

3.7.1.2 roční cena za poskytování aplikace dle bodu 3.6.b) činí 18.000,- Kč bez DPH, služba bude poskytována od data akceptace funkčnosti;

3.7.1.3 roční cena za poskytování aplikace dle bodu 3.6.c) činí 7188,- Kč bez DPH;

3.7.1.4 roční cena za poskytování aplikace dle bodu 3.6.d) činí 9.540,- Kč bez DPH, služba bude poskytována od data akceptace funkčnosti.

3.7.2 Ceny služeb nad rámec paušálu:

3.7.2.1 cena služby uvedené v bodech 3.1, 3.2, 3.3, 3.5, 3.6 nad rámec paušální ceny činí 1 250,- Kč bez DPH za jednu osobu a jednu pracovní hodinu;

3.7.2.2 cena služby uvedené v bodu 3.4 nad rámec paušální ceny činí 750,- Kč bez DPH za jednu osobu a jednu pracovní hodinu;

3.7.2.3 rozsah skutečného čerpání služeb dle tohoto bodu stanoví oprávněné osoby dle této smlouvy dohodou vždy první pracovní den měsíce následujícího po měsíci, ve kterém byly služby poskytnuty. Bez dohody oprávněných osob o rozsahu skutečného čerpání služeb nevzniká nárok poskytovatele na úhradu ceny nad rámec roční ceny.

3.7.3 Ceny za zřízení služby:

3.7.3.1.1 cena za zřízení služby poskytování aplikace dle bodu 3.6.b) činí 30.000,- Kč bez DPH, cena bude fakturována k datu akceptace funkčnosti;

3.7.3.1.2 Cena za zřízení služby poskytování aplikace dle bodu 3.6.d) činí 22.770,- Kč bez DPH, cena bude fakturována k datu akceptace funkčnosti.

4. PARAMETRY SLUŽEB

Parametry jednotlivých služeb jsou rozčleněny do těchto čtyř oblastí: Společné parametry, Project management, Security Management a Technická podpora.

4.1 Součinnost VP

Aby bylo možné vykonávat jednotlivé služby, je nutné, aby VP zajistila nezbytnou součinnost například:

1. předávání podkladů pro nastavení přístupových práv nezbytná pro plnění služeb,
2. fyzické přístupy do prostor objektů VP,
3. součinnost při řešení problémů,
4. poskytnutí nezbytných technických prostředků pro plnění služeb.

4.2 Definice úrovně služeb

4.2.1 Záznam o provedení služby

Vždy po provedení daného typu služby bude proveden záznam v systému pro správu požadavků (HelpDesk), způsob provedení záznamu je závislý na typu služby.

4.2.2 Měřící období služeb

Měřícím obdobím poskytovaných služeb je kalendářní měsíc. Ze strany poskytovatele bude na základě vykonaných služeb ve sledovaném období vytvořena statistika provedených služeb a plnění SLA, která bude součástí servisní zprávy za sledované období.

4.2.3 Servisní zprávy

Servisní zpráva za dané období bude VP předávána vždy nejpozději do 10. dne následujícího kalendářního měsíce. Zpráva bude obsahovat:

- Statistika nahlášených a realizovaných služeb.
- Měsíční vyhodnocení plnění SLA.

4.2.4 Sankce

V případě nedodržení SLA, bude společnost VP za každé prokázané porušení SLA od společnosti SITMP požadovat sankce ve výši 0,05 % z fakturované měsíční částky.

4.2.5 Akceptace služeb

Akceptace služeb a SLA bude prováděna na základě pravidelné měsíční servisní zprávy. V případě, že VP do 10 dnů nevyjádří nesouhlas považuje měsíční servisní zpráva za akceptovanou.

4.3 Společné parametry

Níže uvedené parametry platí obecně pro všechny služby, pokud není u konkrétní služby uvedeno jinak.

Jméno služby	Popis	Hodnota
Standardní doba služeb	Období, kdy jsou poskytovány služby za standardních podmínek	Pracovní dny od 7:00 do 15:00

4.4 Podpora aplikací

Služba	Popis	Hodnota
Vyhodnocení SLA	Vyhodnocování poskytovaných služeb dle definovaných SLA parametrů. V případě problémů s dodržením SLA, eskalace těchto problémů.	1 x měsíčně, k 10. dni následujícího kalendářního měsíce
Příprava plánu	Příprava plánů rozvoje a údržby IS a IT na následující období, včetně plánů nákladů a příjmů.	1 x ročně, nejpozději k 31.7.

4.5 Security management

Služba	Popis	Hodnota
Reakční lhůta v základní době služeb	Lhůta na zahájení řešení bezpečnostního incidentu	2 hod od nahlášení
Příprava plánu	Příprava plánů řešení bezpečnostních rizik na následující období, včetně plánů nákladů	1 x ročně, nejpozději k 31.7.
Implementace informační bezpečnosti	Implementace informační bezpečnosti ve společnosti VP	Průběžně

4.6 IT Management

Služba	Popis	Hodnota
Poskytování součinosti při zpracování podkladů pro fakturaci	Příprava podkladů pro rozúčtování vynaložených finančních nákladů na jednotlivý nákladová střediska v rámci organizace Vodárna Plzeň	průběžně dle potřeby

Plán investic - příprava	Příprava plánu investic pro oblast výpočetní techniky a informačních technologií	1 x ročně
Plán investic - vyhodnocení	Kontrola plnění plánu investic a jeho případné upřesnění	k 1.4. k 1.9.
Provozní plán - příprava	Návrh plánu provozních nákladů IT	1 x ročně
Provozní plán - vyhodnocení	Kontrola dodržování plánu provozních nákladů IT	průběžně

4.7 Technická podpora

	Služba (Popis)	Hodnota SLA
Zahájení řešení požadavku*	**Servis – mimo pracovní dobu**	
	Poskytnutí součinnosti při výpadku či jiných problémech u aplikacích jejichž podpora je poskytována na základě smlouvy o podpoře s jiným Poskytovatelem než-li SITMP	Po nahlášení na HelpDesk osobou ze seznamu kritických služeb bude řešeno bezodkladně první pracovní den, následující po nahlášení požadavku
	Servis – v pracovní dobu	Pracovní dny 7:00 – 15:00
	Kategorie A problémy spojené s funkčností serverů a serverových aplikací, aktivních prvků, datový spojů, internetového připojení a zavirováním počítačové sítě	Do 1 hodiny po nahlášení na HelpDesk osobou ze seznamu kritických služeb
	Kategorie B problémy znemožňující jakoukoliv práci na	Do 4 hodin po nahlášení na HelpDesk
	Poskytnutí součinnosti při výpadku či jiných problémech u aplikacích jejichž podpora je poskytována na základě smlouvy o podpoře s jiným Poskytovatelem než-li SITMP	Do 1 hodiny po nahlášení na HelpDesk osobou ze seznamu kritických služeb

*Zahájení řešení požadavku se prokazuje záznamem v HelpDesku.

	Služba (Popis)	Hodnota SLA
Lhůta na vyřešení požadavku*	Kategorie A problémy spojené s funkčností serverů a serverových aplikací, aktivních prvků, datový spojů, internetového připojení a zavirováním počítačové sítě	Do 14 hodin po nahlášení
	Kategorie B problémy znemožňující jakoukoliv práci na výpočetní technice, nefunkční software problémy omezující či komplikující užívání výpočetní techniky (omezení je překonatelné náhradním postupem, problém není v současné době kritický), instalace HW/SW	Do 2 dnů po nahlášení

	Informování VP, že výpadek či jiný problém u aplikacích jejichž podpora je poskytována na základě smlouvy o podpoře s jiným Poskytovatelem než-li SITMP není schopna SITMP zajistit a VP musí tyto Poskytovatele kontaktovat.	Do 1 hodiny po nahlášení
	Opravy prováděné externě	Dle servisních podmínek příslušného Poskytovatele (SITMP do 1 hodiny od nahlášení informuje VP o potřebě kontaktovat exerního Poskytovatele služby VP)
	Ostatní problémy, uživatelská podpora	Do dvou měsíců od nahlášení

*Za odstranění problému se považuje i zajištění funkčního náhradního řešení, v tomto případě se lhůta na dořešení požadavku stanovuje individuálně dohodou se zástupcem odběratele.

Služba	Popis	Hodnota
Zálohování	Záloha pracovních dat na zálohovací server a externí zálohovací médium	1 x denně (1x týdně na externí zálohovací médium)
	Kontrola funkčnosti záloh	1 x měsíčně
Kontrola stavu HW	Provádění pravidelné kontroly stavu HW (HW sken)	1 x za 3 měsíce
Kontrola stavu SW	Kontrola licencí a kontrola legálnosti nainstalovaných aplikací (SW sken)	1 x za 3 měsíce
Aktualizace SW		Průběžně

Služba	Popis	Hodnota
Povinnost evidovat důležité záznamy	Předávací protokoly k HW a SW	5 let
	Zápisy o zjištění nelegálního SW či změn HW	2 roky (Incicent HelpDesk)
	Log soubory (serverů, koncových stanic a aktivních prvků)	6 měsíců na koncových stanicích se drží průběžně z důvodu řešení případného odstraňování problémů, zejména pak logy operačního systému.
	Podrobný výpis nepovolených aktivit z log souborů (týká se zejména neoprávněných aktivit směrem od koncové stanice do síťového prostředí jako je Internet, komunikace s dalšími koncovými stanicemi apod.)	2 roky (Incident HelpDesk)

4.8 Bezdrátové spoje

Služba	Popis	Hodnota
Bezdrátové spoje	Správa a servis – dodavatelsky	Dle servisních podmínek příslušného Poskytovatele

4.9 Seznam kritický služeb

Služby Kategorie A (problémy spojené s funkčností serverů a serverových aplikací, aktivních prvků, datový spojů, internetového připojení a zavirováním počítačové sítě)

Aplikace	Dodavatel	Odpovědná osoba
Promotic	Promotic	Košek
Reliance	Geovap	Košek
MEAM Client	Merz/FOXON	Karel Kučera
MScada Client	Merz/ FOXON	Karel Kučera, M. Šilhavý
MOS SAIA S-Bus comm	Ingos	Rataj
GDF Control	GDF	Šiml (Hobel), Košek
Most	Fiedler	ÚV Kralovice - Šiml, Hobl, ÚV Nýřany - L. Kučera, Vacek, ÚV Plzeň - K. Kučera, Šilhavý, OV_Košek, Vacek Martin, Mádr
HelpDesk	SITMP	Taušl
DMS ELO	EXON s.r.o.	Taušl

Změna Odpovědné osoby bude Poskytovateli oznamována oprávněnou osobou Objednatele elektronickou formou nejpozději při změně Odpovědné osoby. Při změně Odpovědné osoby nebude nutné uzavírat dodatek k této Smlouvě.

Příloha číslo 2 – Obecné principy v oblasti bezpečnostních opatření

V souladu s požadavkem vyhlášky č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VKB“) VODÁRNA PLZEŇ, a.s. připravila bezpečnostní pravidla pro identifikované významné Poskytovatele v souladu s požadavkem VKB, §8 odstavce 1 písmene a). Tato pravidla jsou součástí smluvního ujednání mezi Objednatelem a významným Poskytovatelem a jejich porušení je bráno jako porušení smluvního vztahu a je postihováno v souladu s ustanoveními konkrétní smlouvy s Poskytovatelem.

1. POVINNOSTI POSKYTOVATELE A JEHO PODDODAVATELŮ

1.1 Poskytovatel jako zaměstnavatel při provádění prací při plnění smlouvy odpovídá za dodržování předpisů BOZP a PO svými zaměstnanci, popř. dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, a odpovídá za dodržování podmínek vstupu osob a vjezdu vozidel do areálů, objektů, a na pozemky Objednatele.

1.2 a bezpečnostního režimu pro ně stanoveného.

1.3 Každý zaměstnanec Poskytovatele, podílející se na plnění smlouvy výpočetními prostředky Poskytovatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých určených systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec Poskytovatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.

1.4 Každý zaměstnanec Poskytovatele, pokud přistupuje k interním systémům Objednatele, má u Objednatele veden a evidován uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy. Pakliže to systém dovoluje, pak je povinností aktivovat více-faktorové zabezpečení. Zavádění konkrétních technických opatření bude podléhat schválení VŘKB Objednatele, kam mu bude předkládán návrh skrze oprávněnou osobu Objednatele.

1.5 Každý zaměstnanec Poskytovatele podílející se na plnění předmětu díla v rozsahu této Smlouvy musí být prokazatelně proškolen, a musí mít znalosti příslušných bezpečnostních politik Objednatele souvisejících s předmětem plnění smlouvy. Za proškolení zaměstnanců Poskytovatele a jejich prokazatelné seznámení s požadavky smlouvy a jejich příloh odpovídá Poskytovatel. Seznámení s pravidly, jež mají být dodržována Poskytovatelem a jeho zaměstnanci, je dokumentováno odpovědným zaměstnancem Objednatele.

1.6 Přístup Poskytovatele a jeho zaměstnanců je pravidelně revidován s důrazem na privilegované oprávnění a přístup k chráněným informacím Objednatele, a je upraven v souladu s principem minimálního přístupu, resp. přístup je přidělen pouze nezbytnému počtu osob, které jej potřebují pro výkon pracovních činností.

1.7 Zaměstnanci Poskytovatele jsou povinni v ICT infrastruktuře Objednatele využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou určeného systému.

1.8 Poskytovatel odpovídá za činnosti svých zaměstnanců, popřípadě dalších fyzických osob vykonávajících práci v jeho prospěch, které musí být v souladu s pravidly předanými ze strany Objednatele. Veškeré škody, které vzniknou porušením těchto pravidel zaměstnanci Poskytovatele nebo dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, jdou k

tíži Poskytovatele, který je povinen tyto škody organizaci nahradit v souladu s pravidly uvedenými ve smluvním plnění, pokud není stanoveno jinak.

1.9 Přístup výpočetní techniky Poskytovatele (PC, notebooky) k chráněným interním informacím a k informačním a telekomunikačním systémům musí odpovídat bezpečným HW a SW konfiguracím. Poskytovatel odpovídá za bezpečnou HW a SW konfiguraci vlastní výpočetní techniky přistupující prostřednictvím VPN k systémům Objednatele. Takováto technika musí zejména mít:

- Mít pokročilou funkční antivirovou ochranu, certifikovanou podle AV-TEST (av-test.org), nebo podle VB100 (virusbulletin.com);
- Mít funkční personal firewall (FSCS);
- Mít aktuální operační systém;
- Mít operační systém, který není mimo servisní podporu výrobce (pokud to není smluvním ujednáním upraveno jinak);
- Mít pro každý schválený operační systém zajištěny výše definované podmínky – AV, FW, UPDATE, OS.
- Pracovat na zařízení výhradně s oprávněním běžného uživatele a privilegovaný přístup využívat pouze v případě, že je to nezbytně nutné.
- Mít šifrovaná data na pevném disku.
- Mít nastaveno heslo ochrany BIOSu.
- Využívat do počítače silné heslo v souladu s bezpečnostní politkou Objednatele, případně PIN v kombinaci s Windows Hello nebo Windows Hello for Business, případně používat alternativní ochrany přístupu do počítače v podobě dvoufaktorové autentizace pro přístup ke chráněným datům.

1.10 V případě, že Poskytovatel výše definované standardy při podpisu této smlouvy nesplňuje, je popinen učit opatření, které povedou k nápravě situace nejpozději do 90 dnů od podpisu této Smlouvy.

2. BEZPEČNOST INFORMACÍ Z POHLEDU DŮVĚRNOSTI, DOSTUPNOSTI A INTEGRITY

2.1 Poskytovatel v rámci plnění smlouvy zajišťuje komplexní správu infrastruktury, zejména zajištění bezpečné infrastruktury, zpracování informací, ukládání, provoz a bezpečnost sítě, využívání základní výpočetních zdrojů, pravidelnou aktualizací OS a aplikací ve správe Postytovatele, antivirové ochrany, IPS/IDS systémů, vyhledání potenciálních zranitelností a instalací bezpečnostních záplat do OS systémů, aplikací a technické infrastruktury, kapacity monitoring atd.

2.2 Poskytovatel v rámci plnění smlouvy zajištuje pravidelné zálohování dat a systému pro případnou obnovu dat po havárii, jejich testování a obnovu infrastruktury a systémů po havárii dle požadavků RTO (recovery time objective) a RPO (recovery point objective) OBJEDNATELE.

2.3 Poskytovatele Objednateli poskytně součinnost při specifikaci parametrů řízení kontinuity činností (BCM) a specifikaci povinností, které budou v rámci implementace navržených opatření poskytovány nad rámec rámec bežných činností vyplývajích z této smlouvy.

3. BEZPEČNOST INFORMACÍ A PRÁCE S NIMI

3.1 Vlastníkem veškerých dat a informací je Objednatel, která má ke spravovaným datům také užívací právo.

3.2 Zaměstnanci Poskytovatele jsou informováni Objednatelem, ke kterým klasifikovaným informacím Objednatele mají přístup, a jak s nimi mohou nakládat. Jakákoliv manipulace

(rozmnožování, stahování, nahlížení apod.) a další operace s klasifikovanými informacemi Objednatele, které nebyly výslovně v instrukcích uvedeny, nemá Poskytovatel povoleny.

3.3 Při práci a v rámci oprávněného přístupu Poskytovatele ke klasifikovaným informacím a údajům Objednatele je požadováno, aby se Poskytovatel a jeho zaměstnanci vykonávající práci v rozsahu této Smlouvy vyvarovali jakýmkoliv úkonům v rozporu s interními bezpečnostními politikami nebo provozními pravidly Objednatele. V případě, že je to technicky možné musí Poskytovatel a jeho zaměstnanci při práci s klasifikovanými informacemi využívat více faktorové autentizace pro přístup k těmto informacím.

3.4 Uložení klasifikovaných informací Objednatele na přenosná média a případný transport médií mimo prostory Objednatele podléhá jeho schválení.

3.5 Podmínky při autentizaci pro přístup do ICT infrastruktury Objednatele:

- K jednoznačné identifikaci privilegovaných uživatelů určených systémů se využívá primárně více faktorová autentizace;
- K přístupu privilegovaných uživatelů určených systémů se primárně využívá přístup přes „systém pro správu privilegovaných uživatelů Objednatele“;
- Ověření heslem – pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s vyžadovanými pravidly.

3.6 Pro vzdálený přístup zaměstnanců Poskytovatele předkládá Poskytovatel podklady, na základě, kterých je pak případně vzdálený přístup schválen a zřízen na požadovanou dobu.

3.7 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou stanoveny odpovědnou osobou Objednatele. Přístup zaměstnanců Poskytovatele do infrastruktury Objednatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům Objednatele, může být nepřetržitě zaznamenáván, monitorován a vyhodnocován.

4. LIKVIDACE DAT

4.1 V případě ukládání klasifikovaných informací Objednatele na přenosná média má Poskytovatel povinnost, pokud je to technicky možné, ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.

4.2 Poskytovatel je povinen zajistit likvidaci operativních dat obsahujících chráněné informace Objednatele ihned po pominutí účelu jejich zpracování a/nebo uložení v souladu s Přílohou č. 4 VKB. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí Poskytovatel l vyhotovit protokol.

4.3 Veškeré poskytnuté informace Objednatele a aktiva v jakékoliv podobě budou bezpečně zlikvidovány Poskytovatelem, pokud nastane změna a ukončení smluvního ujednání s Poskytovatelem.

4.4 Poskytovatel poskytne písemné potvrzení Objednateli o provedené bezpečné likvidaci aktiv v souladu s požadavky VKB. Poskytovatel i zajistí a aplikuje způsoby likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat Objednatele v souladu s Přílohou č. 4 VKB.

5. ŘÍZENÍ ZMĚN

5.1 Poskytovatel zajistí, že každá významná změna ICT prostředí, systému a infrastruktury, kterou mám Poskytovatel ve své správě je dokumentována, testována, posouzena formou analýzy rizik a schválena před tím, než je implementována do produkčního systému Objednatele.

5.2 Poskytovatel dále zajistí, aby vždy při významných změnách na aktivech ve správě Poskytovatele byla provedena analýza rizik, a v rámci jejího rozsahu za účelem řízení rizik a ověření funkčnosti této změny, byla provedena analýza eliminace negativních účinků. Cílem analýzy eliminace negativních účinků této změny je ověření, že nebyly zrušeny nebo zmírněny stávající kontrolní mechanismy a opatření, které byly implementovány před zavedením změny, a že změna nemá negativní dopad na existující funkčnost, bezpečnost a stabilitu systému. Ověřování těchto požadavků se provádí v testovacím prostředí.

5.3 Poskytovatel má právo, aby si v souvislosti s realizaci významné změny jiným Dodavatelem Objednatele, vyžádal k náhledu analýzu rizik k prováděné významné změně. Za tímto účelem je též Objednatel oprávněn si vyžádat součinnost Poskytovatele.

6. ŘÍZENÍ RIZIK

6.1 Poskytovatel je povinnen Objednateli pravidelně podávat informace o způsobu jakým řídí svá rizika ve ztahu k předmětu této Smlouvy a jaká jsou zbytková rizika s nimi související.

6.2 Poskytovatel informace předává nejméně jednou za rok a při identifikace každé významné změně.

6.3 Objednatel je oprávněn provést kontrolu řízení rizik na straně Poskytovatele v souladu s příslušným právním předpisem v rozsahu, který se dotýká plnění této Smlouvy.

7. BEZPEČNOSTNÍ MONITORING

7.1 Poskytovatel nebo externí provozovatel IS pro účel pravidelného monitorování a vyhodnocování kybernetických bezpečnostních událostí a identifikace kybernetických bezpečnostních incidentů zajistí poskytování hlášení a záznamů o detekovaných kybernetických a bezpečnostních událostech pro určené bezpečnostní/provozní role Objednatele.

7.2 Poskytovatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události a incidenty v souladu se ZoKB:

1. Odpovědné osobě Objednatele (osoba stanovená pro tyto účely ve smlouvě);
2. V termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události/incidentu;
3. Způsobem předání e-mailem, telefonicky, nebo osobně;
4. S popisem
    a) data a času zjištění;
    b) povahy události;
    c) zdroje události;
    d) cíle/oběti události;
    e) potencionálního dopadu.

7.3 Poskytovatel je povinen průběžně sledovat zveřejnění výskytu bezpečnostních chyb, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webových komponentách atd., a tyto případné chyby bez prodlení odstranit v rámci své vlastní ICT infrastruktury, a informovat odpovědnou osobu Objednatele o dané situaci a přijatých nápravných opatřeních.

8. AUDIT

8.1 Poskytovatel v souladu s Vyhláškou 82/2018, příloha 7, odstavem d) zajistí aktivní spolupráci a součinnost při auditu, včetně ad-hoc auditů Objednatele pro vybrané a určené oblasti,

procesy a ICT infrastrukturu, ověření, provedení bezpečnostních testů a provedení analýzy rizik prostředí Poskytovatele. Objednatel si vyhrazuje právo provádět audity Poskytovatele:

8.2 Objednatel s dostatečným předstihem alespoň 5 pracovních dnů oznámí Poskytovateli záměr na provedení auditu. Obě strany se dohodnou na obsahu, potřebné součinnosti a časovém plánu auditu s tím, že Objednatel se zavazuje postupovat tak, aby nenarušilo provozní potřeby Poskytovatele.

8.3 Objednatel si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování Poskytovatele) v souvislosti s plněním této smlouvy provést neohlášený audit u Posktyovatele s přihlédnutím k provozní situaci Poskytovatele.

8.4 Dokumentace auditů prováděných Objednatelem je vedena v útvaru odpovědném za provádění auditů. Záznamy týkající se určitého auditu jsou vždy označovány stejným identifikátorem. Jednotlivé záznamy auditů tvoří:

i. plán auditu;
ii. oznámení o auditu;
iii. dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
iv. zpráva z auditu;
v. písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů);
vi. záznam o zjištění (nápravných opatřeních a následné kontrole).

8.5 Auditovaná strana (Poskytovatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění:

i. Poskytovatel navrhne na základě zjištění uvedených v závěrečné auditní zprávě návrh opatření a termíny řešení, a předá jejich seznam Objednateli k odsouhlasení;
ii. Objednatel potvrdí souhlas s navrženými opatřeními.

8.6 Auditovaná strana (Poskytovatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření. Zprávu o realizovaných opatřeních Poskytovatel oznamuje a předává organizaci. Poskytovatel, jeho systémy a ICT infrastruktura budou rovněž přehodnoceny v případě změn smlouvy Poskytovatele, které mají vliv na jejich přístup k informačním aktivům. Požadavek na pravidelné hodnocení Poskytovatele, jeho procesů, systémů/ infrastruktury a rizikového profilu.

Příloha číslo 3 - Kontrolní přehled plnění bezpečnosti na straně Poskytovatele

Poskytovatel před prováděním služeb a následně minimálně 1x ročně přehodnotí níže uvedený přehled zajištění bezpečnosti ve vztahu ke své organizaci. Přehled bude přikládám formou přílohy ke smlouvě a na základě níže uvedených skutečností bude Objednatel provádět vyhodnocení rizikovosti Poskytovatele.

STANDARDY A NEJLEPŠÍ PRAKTIKY		
1	Aplikuje Poskytovatel služeb níže uvedený standard na své informační a komunikační systémy (i bez platné certifikace)?	
a.	ISO/IEC 27001	Ano, platná certifikace ISO 27001 podléhající pravidelným interním a nezávislým kontrolám, vydán a řízen platný certifikát shody s normou ISO27001 aktuální verze
ZÁKLADNÍ OPATŘENÍ		
2	Má Poskytovatel služeb manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností?	Manažerka bezpečnosti informací a představitel vedení pro bezpečnost informací
3	Byl u Poskytovatele služeb v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti?	Analýza požadavků dle ZoKB je součást zjištění interního auditu ISO 27001 a ISO 37301; řízené riziko v rámci analýzy CMS, stanoven plán opatření k dosažení shody
4	Bylo u Poskytovatele služeb v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti?	V ročním intervalu je prováděna analýza rizik dle požadavků ISO 27001, 37301 a analýza dopadu podle ISO 22301
5	Které oblasti pokrývá dokument bezpečnostní politiky, pokud takový dokument u Poskytovatele služeb existuje?	
a.	Procesy řízení rizik	Příručka IMS, kap.9, metodika pro analýzu rizik v záznamu analýzy rizik;je vytvářen a řízen plán ošetření rizik
b.	Klasifikace aktiv	Příručka IMS, kap.9, metodika pro analýzu rizik, vlastní hodnocení aktiv je provedena v analýze rizik bezpečnosti informací, klasifikace informačních aktiv je stanovena v rámci dokumentovaných informací
c.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti	Nástroje A11 a A12 prohlášení o aplikovatelnosti, interní postupy a směrnice, pracovní řád
d.	Ochrana osobních dat	Postupy GDPR, pracovní řád, smlouvy s dotčenými subjekty
e.	Identifikace a autentizace uživatelů	Projektová a provozní dokumentace, nástroje A9.4 prohlášení o aplikovatelnosti, záznamy v helpdesku, záznamy v nástrojích pro řízení přístupu
f.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	Projektová a provozní dokumentace, nástroje A9.4 prohlášení o aplikovatelnosti, záznamy v helpdesku
g.	Řízení privilegovaných přístupů	Nástroj A9.2.3, postupy a odpovědnosti administrátorů, záznamy o řízení privilegovaných přístupů
h.	Ochrana koncových stanic	Nástroje A11 fyzická bezpečnost a bezpečnost prostředí, pracovní řád, smlouvy, zavedené postupy a směrnice
i.	Ochrana mobilních zařízení a vzdáleného přístupu	Nástroje A6.2 práce s mobilními zařízeními a práce na dálku, technická dokumentace, nastavení infrastruktury
j.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	Aplikace antivirů, antispamu, pravidla komunikace, pracovní řád

k.	Ochrana přístupu do internetu	Aplikace firewallů, technická dokumentace
l.	Ochrana výměnných médií	Nástroje skupiny A8.3, vlastní směrnice řešící zacházení s médii včetně jejich vyřazení
m.	Procesy řízení změn	Vlastní směrnice pro řízení změn odpovídající požadavkům norem ISO 20000-1, 22301 a ISO 27001
n.	Ochrana bezdrátových sítí a komunikace	Ano (Externí dodavatele neřešíme, pouze upozorníme)
o.	Fyzická bezpečnost informačních aktiv	Zavedené prostřednictvím skupiny nástrojů A11
p.	Bezpečnostní školení koncových uživatelů a administrátorů	Ano u vlastních zaměstnanců.
q.	Ochrana proti škodlivému softwaru	Aplikovány nástroje skupiny A12.2 ochrana před škodlivým software, technická dokumentace, vlastní směrnice
r.	Ochrana při výměně dat	Řízení komunikací, obsaženo v uzavřených smlouvách
s.	Procesy zvládání kybernetických incidentů	Zatím nasazen proces řízení událostí, incidentů v oblasti bezpečnosti informací
t.	Procesy řízení rizik dodavatelů	Probíhá průběžně
u.	Bezpečnost lidských zdrojů	Probíhá průběžně
v.	Bezpečnostní audity a analýzy	Zaveden plán auditů bezpečnosti informací externí a interní
w.	Řízení kontinuity činností a havarijní plánování	Zavedena v rámci systému BCMS dle ISO 22301, 27001 a 20000-1
BEZPEČNOSTNÍ TECHNOLOGIE		
6	Které níže uvedené bezpečnostní technologie Poskytovatel služeb provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?	
a.	Antivirový software na pracovních stanicích	Zavedeno
b.	Antivirový software na mobilních zařízeních	NE
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)	ANO
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)	NE
e.	Více-faktorová autentizace	Zavedena u vybraných aktiv
f.	Automatizovaný nástroj pro řízení technologických zranitelností	Zaveden nástroj nessus, není pro řízení, ale pro detekci
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	NE
h.	Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)	ANO
i.	Šifrovací nástroje a techniky	Pouze u vybraných systémů
j.	Firewall	Ano, zavedené
k.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)	Ano, zaveden
7	Byly interní systémy Poskytovatele služeb v posledních 12ti měsících podrobeny penetračnímu testování?	ANO, internímu
PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ		
8	Má Poskytovatel služeb zaveden proces zvládání kybernetických incidentů?	Aktuálně zaveden proces zvládání událostí a incidentů bezpečnosti informací

9	Jsou všichni pracovníci Poskytovatele služeb pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?	Prozatím ne
KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ		
10	Má Poskytovatel služeb zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro pracovníky?	Ano
11	Jsou noví zaměstnanci Poskytovatele služeb vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	Částečně, zajištěno pro oblast ISO 27001, 22301, 20000-1 a 37301
12	Dokumentuje Poskytovatel služeb účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	Ano
13	Vyžaduje Poskytovatel služeb po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	Řešeno pracovní smlouvou a pracovním řádem
14	Vyžaduje Poskytovatel služeb po zaměstnancích podepsání etického kodexu?	Řešeno pracovní smlouvou a pracovním řádem

NEPOVINNÉ OTÁZKY (účastník odpovědi nemusí vyplňovat, otázky jsou pouze informativní a nejsou součástí hodnocení)		
15	Je Poskytovatel služeb orgánem nebo osobou povinnou dle §3 zákona 181/2014 o kybernetické bezpečnosti?	Významný dodavatel ve smyslu výkladu platné verze ZoKB
16	Má Poskytovatel služeb zaveden certifikovaný systém řízení dle ISO/IEC 27001?	Ano, každoročně podléhá kontrolám interních a externích auditů, každé 3 roky je prováděna recertifikace, aktuálně je soulad s ISO 27001:2017, plánován přechod na 27001:2022
17	Jsou pracovníci dodavatelů Poskytovatele služeb vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	Ano, pravidelná školení
18	Vyžaduje Poskytovatel služeb po pracovnících svých dodavatelů s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	Vždy řešeno s dodavatelem, nikoliv s jednotlivými pracovníky dodavatelů. Kontroly smluv probíhají pravidelně včetně ověření stavu NDA
19	Jaké negativní dopady pocítil Poskytovatel služeb v souvislosti s kybernetickým incidentem, pokud v minulosti nastal:	
a.	Výpadek sítě	Existují krizové scénáře a postup řešení nenadálých výpadků, probíhá pravidelná testování
b.	Nedostupnost emailu a kancelářských aplikací	Existují krizové scénáře a postup řešení nenadálých výpadků, probíhá pravidelná testování
c.	Neoprávněné zneužití identity	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
d.	Prozrazení chráněných dat	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
e.	Ztráta nebo zničení dat	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
f.	Finanční ztráta	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko

g.	Ztráta duševního vlastnictví	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
h.	Poškození pověsti organizace účastníka	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
i.	Negativní publicita v médiích	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
j.	Ztráta hodnoty organizace účastníka	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko
k.	Trestní stíhání organizace účastníka	Indikováno přes řízení incidentů, řešeno v rámci analýz rizik, jde o řízené riziko

Příloha číslo 4 - Fyzická a virtuální zařízení ve správě SITMP

- **Servery**
  - fyzický server až 14ks
  - fyzický datastore až 5ks
  - virtuální server až 80ks
  - databázový server až 29ks
  - aplikační server až 69ks
- **Notebooky**
  - až 155ks
- **PC stanice**
  - až 132ks
- **Tiskárny**
  - až 25ks
- **Plottery**
  - až 6ks
- **Aktivní prvky**
  - bezpečnostní prvek až 6ks
  - síťový prvky enterprice až 12ks
  - síťový prvek přístupový až 20ks
  - Wi-Fi AP až 18ks
- **Mobilní zařízení**
  - Tablety až 93ks