SMLOUVA

„Telč – rozvoj služeb eGovernementu a Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče – část 6 – Nástroj pro analýzu a monitoring síťového provozu“
podle zákona č. 89/2012 Sb., občanského zákoníku v platném znění
(dále jen „smlouva“)

uzavřená níže uvedeného dne, měsíce, roku mezi následujícími smluvní stranami:

1. **K-net Technical International Group, s.r.o.**
   se sídlem Antonínská 20, 602 00 Brno
   zapsaný v obchodním rejstříku vedeném u Krajského soudu v Brně, sp. zn.: C 10425
   Identifikační číslo: 47916745
   DIČ: CZ699001418
   bankovní spojení: [redacted]
   jednající: Ing. Tomášem Knettigem, jednatelem
   Ing. Petrem Nepustilem, jednatelem
   (dále jen „poskytovatel“)

a

2. **Město Telč**
   se sídlem náměstí Zachariáše z Hradce 10, 588 56 Telč – Vnitřní Město
   Identifikační číslo: 00286745
   DIČ: CZ00286745
   bankovní spojení: [redacted]
   ID datové schránky: c26bg9k
   zastoupený: Mgr. Vladimírem Brtníkem, starostou města
   (dále také jako „objednatel“);

oba dále také samostatně jako „smluvní strana“ a společně jako „smluvní strany“.

Preambule, účel

Tato smlouva se uzavírá na základě výsledku 6. části zadávacího řízení na veřejnou zakázku s názvem „**Telč – rozvoj služeb eGovernementu a Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče**““ veřejného zadavatele Města Telče.

Článek 1
Předmět smlouvy, předmět plnění

Předmětem plnění smlouvy je vytvoření (dodávka a implementace) informačního systému veřejné správy **„Telč – rozvoj služeb eGovernementu a Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče – část 6 – Nástroj pro analýzu a monitoring síťového provozu“** (včetně poskytnutí licencí s neomezenou platností a pro neomezený počet uživatelů potřebných pro jeho užívání, integrace dodaného systému se stávajícím aplikačním vybavením zadavatele a s centrálními systémy a zajištění jeho provozu) vše včetně projektového řízení a zajištění podpory provozu po dobu 6 let od úplného předání a převzetí. Obsah a rozsah činností podpory provozu je určen v příloze č. 1 této smlouvy. Před úplným předáním a převzetím díla provádí poskytovatel rovněž podporu provozu příslušných již provedených částí plnění.

Podrobně je předmět plnění popsán v příloze č. 1.

Článek 2
Způsob, čas a místo dodání, odevzdání a převzetí, podmínky plnění

2.1 Plnění bude dodáno kompletní podle přílohy č. 1 této smlouvy (včetně projektového řízení a všech náležitostí nezbytných pro řádný provoz) ve lhůtě nejpozději do 4 týdnů od doručení písemné výzvy k zahájením plnění. Tuto výzvu doručí objednatel poskytovateli. Po dodání kompletního plnění proběhne částečné předání a převzetí s vypracováním protokolu o částečném předání a převzetí. Po částečném předání a převzetí objednatel provede audit kybernetické bezpečnosti. Po úspěšném provedení auditu kybernetické bezpečnosti proběhne konečné protokolární předání a převzetí. Následně poskytovatel zajistí podporu provozu po dobu 6 let od předání a převzetí díla bez vad a nedodělků.

2.2 Veškerá plnění se poskytovatel zavazuje dodat bez jakýchkoliv právních i funkčních vad; dále se zavazuje převést na objednatele veškerá práva užívání tohoto plnění (licence), a to bez časového omezení.

2.3 Místem odevzdání (dodání a poskytnutí) a převzetí plnění je sídlo objednatele. Náklady odevzdávání (dodání) a rizika s tím spojená (včetně dokladů a dokumentů vztahujících se k dodávce a dopravou do místa dodání, vykládky a manipulace na místě dodání) nese poskytovatel. Při dodání systému poskytovatel doloží certifikaci a garanci výrobce hardware (pokud je v plnění smlouvy zahrnut), že nabízené zboží je určené pro český trh, je nové, nepoužité a pochází z oficiálního distribučního kanálu v ČR.

2.4 Plnění podle odst. 2.1 smlouvy bude protokolárně odevzdáno poskytovatelem objednateli v místě dodání. Objednatelem pak bude konečně převzato v případě řádného splnění se všemi sjednanými vlastnostmi, a to formou "Protokolu o odevzdání a převzetí", který bude podepsán oběma smluvními stranami osobami oprávněnými jejich jménem jednat (dále jen „Protokol o odevzdání a převzetí“). Podmínkou konečného převzetí je pozitivní závěr auditu kybernetické bezpečnosti.

2.5 Ke konečnému převzetí v místě dodání je povinen poskytovatel vyzvat objednatele nejméně dva pracovní dny předem. Výzva poskytovatele musí být písemná, doručení výzvy provedeno pomocí prostředků elektronické pošty nebo prostřednictvím datové schránky a v příloze výzvy dodán písemný návrh "Protokolu o odevzdání a převzetí", podepsaný poskytovatelem

Protokol o odevzdání a převzetí i protokol o částečném předání a převzetí bude obsahovat nejméně tyto náležitosti:

- výkaz dodaných a zprovozněných předmětů, poskytnutého příslušenství a ostatních věcí, poskytnutých služeb a předaných dokladů a dokumentů vztahujících se k plnění;
- datum vystavení protokolu a podpis osoby oprávněné jednat za poskytovatele;
- uvedení data podpisu protokolu objednatelem.

2.6 Objednatel je oprávněn odmítnout převzít plnění poskytovatele v případě zjištění jeho vad nebo jiných nedostatků, a to bez ohledu na jejich počet a povahu nebo neobsahuje-li "Protokol o odevzdání a převzetí" náležitosti dle této smlouvy bez ohledu na počet nebo povahu chybějících náležitostí. Důvody odmítnutí budou objednatelem specifikovány v "Protokolu o odevzdání a

převzetí". V případě, že objednatel odmítne převzít plnění poskytovatele, nepřechází na něj nebezpečí škody na žádné jeho části.

2.7 Poskytovatel je povinen umožnit objednateli provést kontrolu průběhu plnění dle této smlouvy, a to po celou dobu trvání této smlouvy.

2.8 Poskytovatel se zavazuje, že bude provádět činnosti pouze za pomoci svého realizačního týmu, jehož členové jsou popsáni v příloze č. 2 smlouvy. Poskytovatel je oprávněn provést nahrazení členů realizačního týmu pouze s písemným souhlasem Objednatele. V takovém případě musí náhradníci původních členů realizačního týmu splňovat kvalifikační požadavky, které byly uvedeny v zadávací dokumentaci veřejné zakázky.

2.9 Poskytovatel se zavazuje, že poskytne součinnost ostatním poskytovatelům (vybraným dodavatelům), kterým byly zadány ostatní části veřejné zakázky „Telč – rozvoj služeb eGovernementu a Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče**“.**

2.10 Poskytovatel je povinen při plnění této smlouvy dodržovat zásady, které jsou součástí přílohy č. 4 této smlouvy.

Článek 3
Cena

3.1 Poskytovateli náleží za řádné, včasné a úplné splnění předmětu smlouvy cena ve výši 1 391 575,00 Kč + DPH ve výši 292 230,75 Kč; cena včetně příslušné výše DPH činí 1 683 805,75 Kč.

3.2 Cena jednotlivých dílčích plnění (rozpočet) dle této smlouvy je sjednána v příloze č. 3 smlouvy.

3.3 Cena dle čl. 3.1 této smlouvy byla stanovena na základě zadávacího řízení na veřejnou zakázku a obsahuje veškeré náklady nutné k plnění poskytovatele při realizaci předmětu této smlouvy po celou dobu stanovenou touto smlouvou.

3.4 Vedle případů upravených dále v čl. 8 je změna ceny dle čl. 3.1 možná pouze pokud při realizaci předmětu plnění dojde ke změnám sazeb DPH. V tomto případě se cena upraví podle výše sazby DPH platné v době vzniku zdanitelného plnění. v takovém případě nebude vyhotoven dodatek k této smlouvě a účinnost této změny nastává v návaznosti na účinnost změny příslušného obecně závazného daňového právního předpisu.

Článek 4
Platební podmínky

4.1 Objednatel uhradí cenu na základě faktury (daňového dokladu), kterou poskytovatel vystavil a prokazatelně doručil objednateli po konečném předání a převzetí celého díla bez vad a nedodělků (po úspěšném provedení auditu kybernetické bezpečnosti) Poskytovatel je rovněž oprávněn fakturovat 70 procent dílčího plnění „Dodání systému včetně dalších služeb“ (viz příloha č. 3 této smlouvy) po částečném předání a převzetí celého díla bez vad a nedodělků, v takovém případě bude zbylých 30 procent dílčího plnění „Dodání systému včetně dalších služeb“ fakturováno po konečném předání a převzetí celého díla bez vad a nedodělků (po úspěšném provedení auditu kybernetické bezpečnosti). Pokud je součástí plnění i dodání hardware, je poskytovatel oprávněn fakturovat 35 procent dílčího plnění „Dodání systému včetně dalších služeb“ (viz příloha č. 3 této smlouvy) po dovezení hardware na místo plnění, v takovém případě bude po částečném předání a převzetí celého díla bez vad a nedodělků poskytovatel fakturovat objednateli 35 procent dílčího plnění „Dodání systému včetně dalších služeb“.

4.2 Cenu dle vyúčtování fakturou (daňovým dokladem) uhradí objednatel formou bezhotovostního převodu na účet poskytovatele uvedený v záhlaví této smlouvy. Faktura (daňový doklad) musí obsahovat odkaz na tuto smlouvu a přílohu faktury (daňového dokladu) bude tvořit kopie oboustranně podepsaného "Protokolu o odevzdání a převzetí". Dále musí faktura (daňový doklad) obsahovat veškeré náležitosti stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura musí být dále označena číslem projektu, které poskytovateli sdělí objednatel.

4.3 Nebude-li faktura (daňový doklad) splňovat veškeré výše uvedené náležitosti, nebo bude-li mít jiné závady v obsahu, je objednatel oprávněn ji ve lhůtě její splatnosti poskytovateli vrátit. V

takovém případě je poskytovatel povinen vystavit a prokazatelně doručit objednateli novou opravenou či doplněnou fakturu (daňový doklad). Vrácením faktury (daňového dokladu) dle předcházející věty se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku až dnem následujícím po dni, kdy byla opravená nebo doplněná faktura (daňový doklad) splňující všechny náležitosti dle příslušných právních předpisů a této smlouvy prokazatelně doručena objednateli.

4.4 Smluvní strany se dohodly, že dnem úhrady se rozumí den odepsání fakturované částky z účtu Splatnost faktury s náležitostmi daňového dokladu se stanovuje na základě dohody obou smluvních stran do 21 dnů ode dne jejího prokazatelného doručení objednateli. Strany se dohodly, že platba bude provedena bezhotovostním převodem na číslo účtu uvedené v záhlaví této smlouvy, které je zveřejněné způsobem umožňujícím dálkový přístup podle ustanovení § 96 zák. č. 235/2004 Sb. o dani z přidané hodnoty v platném znění. Poskytovatel výslovně prohlašuje, že předmětný účet je vedený v tuzemsku.

4.5 Daň z přidané hodnoty bude účtována podle platných právních předpisů.

4.6 Přijaté plnění nebude používáno k ekonomické činnosti, a proto nebude aplikován režim přenesení daňové povinnosti dle zákona č. 235/2004 Sb. o dani z přidané hodnoty v platném znění.

4.7 Poskytovatel plnění prohlašuje, že není nespolehlivým plátcem dle zákona č. 235/2004 Sb. o dani z přidané hodnoty v platném znění a v případě, že by se jím v průběhu trvání smluvního vztahu stal, tuto informaci neprodleně sdělí příjemci plnění (objednateli).

4.8 Pokud se poskytovatel stane nespolehlivým plátcem daně dle zák. č. 235/2004 Sb. o dani z přidané hodnoty v platném znění, je poskytovatel oprávněn uhradit poskytovateli za zdanitelné plnění částku odpovídající sjednané ceně bez DPH a úhradu DPH provést přímo na příslušný účet příslušného finančního úřadu dle § 109a zák. č. 235/2004 Sb. o dani z přidané hodnoty v platném znění. Zaplacení částky ve výši daně na účet správce daně poskytovatele a zaplacení ceny bez DPH poskytovateli bude považováno za splnění závazku objednatele uhradit sjednanou cenu.

4.9 Úhrada se považuje za provedenou včas, pokud bude odepsána z účtu objednatele ve prospěch účtu poskytovatele nejpozději v poslední den dohodnuté doby splatnosti.

4.10 Poskytovatel se zavazuje do 15 kalendářních dnů po uzavření této smlouvy doručit objednateli písemné potvrzení správce daně o své registraci k dani z přidané hodnoty.

4.11 Podpora provozu bude fakturována vždy za proběhlé kalendářní čtvrtletí.

Článek 5
Práva objednatele z vadného plnění poskytovatele a servisní podpora

5.1 Práva objednatele z vadného plnění poskytovatele se podřizují dikci § 2615 až § 2619, § 2099 až § 2117 a přiměřeně rovněž § 2165 až § 2174 zákona občanského zákoníku. Objednatel je oprávněn oznámit poskytovateli vady předmětu plnění, popř. jeho částí, bez zbytečného odkladu poté, kdy byly, nejpozději však do dvou let od převzetí předmětu plnění "Protokolem o odevzdání a převzetí" bez vad a nedodělků, a zvolit si a písemně uplatnit právo z vadného plnění. V případě, že objednatel oznámí vadu Poskytovatel se zavazuje, že nastoupí k jejímu odstranění v místě dodání a odstraní ji nejpozději ve lhůtách uvedených níže. Nenastoupí-li poskytovatel k odstranění oznámené vady ani do desíti pracovních dnů po obdržení oznámení, je objednatel oprávněn pověřit odstraněním vady jiný subjekt a veškeré takto vzniklé náklady je oprávněn přeúčtovat poskytovateli.

5.2 Poskytovatel poskytuje objednateli záruku za jakost celého plnění v délce šesti let ode dne převzetí předmětu "Protokolem o odevzdání a převzetí" bez vad a nedodělků.

5.3 Poskytovatel poskytuje objednateli servisní podporu v délce šesti let ode dne převzetí předmětu "Protokolem o odevzdání a převzetí" bez vad a nedodělků. Servisní podpora bude zahrnovat:

- opravy chyb a závad systému,

- úpravy a další změny, vyplývající ze změn okolního prostředí,
- úpravy a další změny vyplývající z legislativy ČR, národních standardů a nařízení EU,
- update nové verze systému,
- obnovení systému při výpadcích systému dle dohodnutých podmínek „Service-Level Agreement“ (SLA), tak aby byly zachovány požadavky na provoz systému, viz. následující požadavky na reakční dobu a dobu řešení:
  - možnost nahlášení problému nepřetržitě v režimu 7 dní v týdnu x 24 hodin denně elektronicky přes helpdesk uchazeče nebo na emailovou adresu. Přijetí problému uchazeč obratem potvrdí,
  - zahájení řešení problému do 12 hodin od okamžiku nahlášení,
  - čas vyřešení kritického výpadku (závada bránící zadavateli poskytovat hlavní předmět jeho činnosti např. služby veřejnosti, zákonem definované povinnosti apod.) je 24 hodin,
  - čas vyřešení částečného výpadku (závada narušuje provoz systému, degraduje nebo omezuje jeho funkčnost) následující pracovní den,
  - čas vyřešení ostatních závad je 5 pracovních dnů,
  - garantovaná dostupnost systému 99,8 % v kalendářním měsíci.

V případě, že příloha č. 1 obsahuje servisní podmínky, které jsou v rozporu s tímto ustanovením, platí podmínky, které jsou pro zadavatele příznivější.

5.4 Poskytovatel je povinen být pojištěn pro případ pojistných událostí souvisejících s plněním této smlouvy po celou dobu jejího plnění, a to minimálně pojištěním odpovědnosti za škody způsobené jeho činností, včetně možných škod způsobených zaměstnanci poskytovatele. Veškeré pojištění musí být sjednáno s limitem nejméně 10 000 000 Kč.

Článek 6
Mlčenlivost

6.1 Není-li dále stanoveno jinak, poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech, které se dozví v souvislosti s plněním této smlouvy. Tento závazek se rovněž vztahuje na veškeré informace, které objednatel předá poskytovateli, a na veškeré skutečnosti, se kterými se poskytovatel seznámí při plnění této smlouvy, zejména (nikoliv výlučně) na skutečnosti tvořící předmět obchodního tajemství nebo důvěrnou informaci (dále jen „chráněné informace“).

6.2 Závazek mlčenlivosti je poskytovatel povinen zajistit mimo jiné tím, že bez předchozího písemného souhlasu objednatele nedojde k jakémukoli šíření chráněných informací, anebo jejich zpřístupnění třetím osobám. Splnění tohoto závazku nevylučuje rozmnožení chráněných informací pro potřeby objednatele a jeho poddodavatelů, které je nutné pro řádné plnění závazků objednatele vyplývajících z této smlouvy a zákona.

6.3 Závazek mlčenlivosti je poskytovatel povinen zachovávat jak po dobu plnění předmětu této smlouvy, tak po jejím dokončení; tohoto závazku jej může zprostit pouze objednatel svým písemným prohlášením.

6.4 Poskytovatel je povinen zajistit, že chráněné informace budou přístupné pouze zaměstnancům nebo jiným osobám, které se budou podílet na plnění předmětu této smlouvy (dále jen „oprávněné osoby“). Na vyžádání objednatele je poskytovatel povinen neprodleně objednateli poskytnout úplný seznam oprávněných osob (jméno a příjmení u fyzických osob a obchodní firmu a identifikační číslo u právnických osob).

6.5 Poskytovatel je povinen zajistit splnění závazku mlčenlivosti ve stejném rozsahu u oprávněných osob, a to tak, aby oprávněné osoby byly tímto závazkem vázány i po skončení pracovněprávního nebo jiného smluvního vztahu k poskytovateli.

6.6 Závazek mlčenlivosti se nevztahuje na kontroly, které mohou být v budoucnu prováděny a ve vztahu k nimž je poskytovatel povinen předložit dokumenty související s plněním dle této smlouvy ze strany objednatele orgánů oprávněných k provádění kontroly, a to zejména Ministerstva financí České republiky, Nejvyššího kontrolního úřadu případně dalších subjektů činných ve

veřejné správě nebo dalších institucích či osob, které tyto orgány touto činností pověří nebo je k ní zmocní.

Článek 7
Ujednání o smluvních pokutách

7.1. Objednatel zaplatí smluvní pokutu poskytovateli za opožděné uhrazení fakturované částky, a to ve výši 0,05 % z dlužné částky za každý i započatý den prodlení.

7.2. V případě, že poskytovatel bude v prodlení s termínem plnění specifikovaného v článku. 2.1 této smlouvy je povinen zaplatit objednateli smluvní pokutu ve výši 5.000 Kč (slovy Pěttisíc korun českých) za každý i započatý den prodlení.

7.3. V případě, že poskytovatel bude v prodlení s poskytnutím služby servisní podpory v reakční době specifikované v odstavci 5.3 této smlouvy je povinen zaplatit objednateli smluvní pokutu ve výši 5.000 Kč (slovy Pěttisíc korun českých) za každý i započatý den prodlení.

7.4. V případě porušení závazku mlčenlivosti poskytovatelem dle této smlouvy se sjednává smluvní pokuta ve výši 100.000,-- Kč (slovy Jednostotisíc korun českých) za každé jednotlivé porušení tohoto závazku.

7.5. Smluvní pokutu sjednanou touto smlouvou je poskytovatel povinen uhradit nezávisle na tom, zda a v jaké výši vznikne objednateli v této souvislosti škoda, kterou lze vymáhat samostatně.

7.6. Obě strany se vzájemnou dohodou mohou sankcí vzdát, i když na ně vznikne smluvní nárok.

7.7. V případě, že objednateli vznikne z ujednání dle této smlouvy nárok na smluvní pokutu, náhradu škody nebo jinou majetkovou sankci vůči poskytovateli, je objednatel oprávněn započíst tuto částku vůči kterékoliv faktuře, resp. více fakturám poskytovatele.

7.8. Obě strany prohlašují, že považují výši smluvních pokut dle tohoto článku za přiměřenou povaze plnění dle této smlouvy.

Článek 8
Změna závazku ze smlouvy, skončení smlouvy

8.1 Změna závazku ze smlouvy je možná, nastanou-li zákonné předpoklady dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek v platném znění (dále jen „zákon o zadávání veřejných zakázek“), pro dovolenou změnu závazku ze smlouvy jako smlouvy na veřejnou zakázku a smluvní strany se na ní dohodnou.

8.2 Smluvní vztah lze ukončit dohodou smluvních stran ke kterémukoliv datu, přičemž její součástí bude i vzájemné vyrovnání účelně vynaložených nákladů

8.3 Objednatel nebo poskytovatel jsou oprávněni odstoupit od smlouvy v intencích zákona o zadávání veřejných zakázek nebo občanského zákoníku a dále bez dalšího:

a) pokud smluvní strany shodnou vůlí dospěly k závěru, že pokračování plnění smlouvy by bylo porušením pravidel a zákonných požadavků umožňujících uzavření dovolené změny závazku ze smlouvy dle příslušného ustanovení zákona o zadávání veřejných zakázek

b) při podstatném porušení této smlouvy jednou ze smluvních stran, příp. je-li na majetek poskytovatele vyhlášeno insolvenční řízení nebo je-li tento návrh zamítnut pro nedostatek majetku. Za podstatné porušení smlouvy poskytovatelem považují smluvní strany především neplnění věcných a termínových závazků vyplývajících z této smlouvy. Za podstatné porušení smlouvy objednatelem považují smluvní strany prodlení se zaplacením finančním závazků, které z této smlouvy vyplývají, o více než 90 dní.

8.4 Jednostranné odstoupení od této smlouvy musí být učiněno písemným oznámením podepsaným oprávněným zástupcem. Právní účinky odstoupení nastávají dnem doručení druhé smluvní straně. V případě pochybností se má za to, že je odstoupení doručeno druhé smluvní straně třetí den od jeho prokazatelného odeslání.

8.5 Účinky odstoupení od smlouvy se netýkají smluvních závazků souvisejících se závazkem mlčenlivosti a závazkem hradit jednotlivé smluvní pokuty, úroku z prodlení, nároku na náhradu škody, vypořádání smluvních stran po odstoupení ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany po odstoupení.

8.6 Objednatel je oprávněn vypovědět smlouvu během poskytování podpory provozu. Výpovědní doba započne běžet doručením výpovědi poskytovateli a činí 3 měsíce. Poskytovatel není oprávněn objednatele za tento právní úkon jakkoliv postihovat.

Článek 9
Komunikace

9.1 Veškerá sdělení v souvislosti se vznikem, změnou nebo zánikem závazků plynoucích z této smlouvy musí být formulována písemně a podepsána osobou oprávněnou jednat jménem příslušné smluvní strany. Sdělení doručená v den, který není dnem pracovním, budou považována za doručená v nejbližší následující pracovní den.

9.2 Kontaktními osobami smluvních stran jsou:

Za objednatele:

- [redacted]
- [redacted]

Za poskytovatele:

- [redacted]
- [redacted]

Článek 10
Uveřejnění uzavřené smlouvy, smluvních dodatků, skutečně uhrazené ceny

10.1 Smluvní strany stanoví dohodou, že (i) žádné ustanovení této smlouvy nepodléhá obchodnímu tajemství dle ustanovení § 504 občanského zákoníku, ani neobsahuje důvěrnou informaci o poměrech smluvní strany nebo skutečnostech, které má smluvní strana potřebu ochraňovat jako důvěrnou informaci nebo předmět obchodního tajemství, a (ii) poskytovatel souhlasí se zveřejněním této smlouvy na profilu zadavatele objednatele podle zákona o zadávání veřejných zakázek nebo v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv“).

10.2 Poskytovatel bere na vědomí, že objednatel je povinen zpřístupnit obsah této smlouvy na základě aktuálně platných právních předpisů, zejména dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Článek 11
Závěrečná ustanovení

11.1 Smluvní strany se dohodly, že poskytovatel není oprávněn postoupit smlouvu, práva a závazky nebo pohledávky z této smlouvy vyplývající na třetí osobu bez předchozího výslovného písemného souhlasu objednatele

11.2 Smluvní strany podpisem této smlouvy činí rovněž prohlášení, že neexistuje žádné ujednání, smlouva či řízení, ani ústní ujednání, které by nepříznivě ovlivnilo výkon jakýchkoliv práv a závazků dle této smlouvy. Současně smluvní strany potvrzují svým podpisem, že veškerá ujištění a dokumenty, které byly poskytnuty poskytovatelem objednateli před uzavřením a po uzavření této smlouvy, jsou pravdivé, platné a právně vymahatelné.

11.3 Poskytovatel je povinen ve smyslu zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, spolupůsobit při výkonu finanční kontroly. Poskytovatel se zavazuje uchovávat veškerou dokumentaci, která souvisí

s plněním této smlouvy minimálně do roku 2035. Poskytovatel se zavazuje poskytovat řádnou součinnost ve spojitosti i s případnými dalšími kontrolami projektu.

11.4 Jestliže se ukáže jakékoliv ustanovení nebo ujednání této smlouvy jako neplatné nebo nevymahatelné nebo právně neúčinné, nedotýká se to ostatních ujednání nebo ustanovení této smlouvy. Smluvní strany se zavazují, že nahradí jakékoliv neplatné, neúčinné nebo nevymahatelné ustanovení nebo ujednání platným, účinným a vymahatelným ustanovením nebo ujednáním, které má stejný nebo obdobný smysl nebo účinek; učiní tak do patnácti pracovních dnů od doručení výzvy jedné smluvní strany druhé smluvní straně.

11.5 Tato smlouva a veškeré závazky a práva z ní vyplývající se řídí právním řádem České republiky, a to zejména občanským zákoníkem.

11.6 Smluvní strany se zavazují, že budou postupovat v souladu s oprávněnými zájmy druhé smluvní strany, a že uskuteční veškerá právní jednání, která se ukáží být nezbytná pro realizaci závazků upravených touto smlouvou. Závazek součinnosti se vztahuje pouze na takové úkony, které přispějí či mají přispět k dosažení účelu této smlouvy.

11.7 Veškeré změny a doplnění jednotlivých ujednání nebo ustanovení této smlouvy mohou být provedeny při splnění předpokladů dle odst. 8.1 této smlouvy pouze formou číslovaného písemného dodatku podepsaného oběma smluvními stranami.

11.8 Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv. Zveřejnění realizuje objednatel.

11.9 Tato smlouva je uzavřena elektronicky.

11.10 Smluvní strany prohlašují, že smlouva byla uzavřena podle jejich vážné a svobodné vůle, že nejednají v omylu či tísni, smlouvu si přečetly, považují obsah této smlouvy za určitý a srozumitelný, jsou jim známy veškeré skutečnosti, jež jsou pro uzavření této smlouvy rozhodující, a na důkaz toho připojují ke smlouvě své podpisy.

11.11 Uzavření této smlouvy bylo schváleno usnesením Rady Města Telče č. UR 937-2/59/2025 ze dne 19. února 2025.

Přílohy:

Příloha č. 1 – Specifikace předmětu plnění

Příloha č. 2 – Seznam realizačního týmu

Příloha č. 3 – Rozpočet - Cena jednotlivých dílčích plnění

Příloha č. 4 – Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele

V Brně dne	V Telči dne
za poskytovatele:	za objednatele:
---	---
Ing. Petr Nepustil, jednatel	Mgr. Vladimír Brtník, starosta města

Příloha č. 1 – Specifikace předmětu plnění

Část 6 – Nástroj pro analýzu a monitoring síťového provozu	Splňuje ANO/NE
Nástroj pro detekci kybernetických bezpečnostních událostí - Monitoring síťového toku	

Licence	
Trvalá licence	ANO

Systém pro analýzu síťového provozu	
Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	ANO
Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	ANO
Zpracování a ukládání síťových toků.	ANO
Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	ANO
Uživatelé max 120.	ANO
Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.	ANO

Uživatelské rozhraní	
Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.	ANO
Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	
Granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute).	ANO
Granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute).	ANO
Vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů.	ANO
Vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	ANO

Automatické hlášení (alerty) a reporting	
Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	ANO

Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.	ANO
Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).	ANO
Je požadováno vytváření automatizovaných reportů v českém jazyce.	ANO

Integrace systému	
Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	
Syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat).	ANO
Přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní.	ANO
Export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP.	ANO
Integrace se službami identity uživatelů v Microsoft Active Directory bez nutnosti konfigurace zasílání logů do systému.	ANO
Integrace se stávajícím firewallem Sophos XGS2300, pro automatické a manuální reakce vyvolané systémem.	ANO

Podpora EDR	
Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce.	ANO
Počet koncových zařízení je cca 250. Koncovým zařízením jsou myšleny servery, virtuální servery, pracovní stanice, notebooky, tiskárny ad.	ANO
Je požadován 1x HW datový kolektor/sensor o průměrné propustnosti minimálně 500 Mbps s monitorovacím rozhraním 2x1GE.	ANO
Na zařízení je požadována dostupná historie dat (retence alespoň 6 měsíců) uložená na rychlém úložišti o velikosti alespoň 800GB.	ANO
Požadavky na schopnost detekce bezpečnostních událostí	ANO

Monitorování zařízení, segmentů sítě a využívaných síťových služeb	
Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	
Změna IP/MAC adresy hosta.	ANO
Duplicitní IP/MAC adresa.	ANO
Změna VLAN,	ANO
Vytvoření nové podsítě.	ANO
Připojení nového zařízení.	ANO
Použití nebo vznik nové služby.	ANO
Nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení.	ANO
Přístup nového zařízení ke službě či zařízení	ANO

Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.	ANO
Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.	ANO

Samostatné učení behaviorálních aktivit a detekce anomálií	
Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.	ANO
Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	
Odchylku od modelu pro přenos dat, toků a paketů.	ANO
Odchylku od modelu pro počet komunikačních partnerů.	ANO
Odchylku od modelu entropie na komunikačních portech.	ANO
Odchylku od modelu pro počet síťových toků a využitých síťových služeb.	ANO
Odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	ANO
Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.	ANO

Identifikace neznámých hrozeb a podezřelých chování	
Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	
Průzkumné aktivity v síti.	ANO
Detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě.	ANO
Detekce repetitivních vzorců chování na síti.	ANO
Detekce botnetů a ovládání kompromitované stanice.	ANO
Detekce příznaků těžení kryptoměn.	ANO
Útoky hrubou silou a enumerace dat.	ANO
Rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	ANO

Detekce na základě databáze známých hrozeb	
Systém musí být schopen identifikovat hrozby a reportovat události na základě:	
Detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik.	ANO
Reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	ANO
Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.	ANO
Uživatel musí být schopen importovat vlastní záznamy.	ANO

Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.	ANO
Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	ANO
Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel.	ANO

Analýza šifrované komunikace	
Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.	ANO

Asistované učení	
Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	
IP adresa	ANO
MAC adresa	ANO
Hostname	ANO
Segment sítě / podsíť	ANO
Lokalita – ASN, země, apod.	ANO
Směr komunikace – určení klienta, nebo serveru	ANO
Detekovaná událost – kategorie, název apod	ANO
Použité služby, protokolu, port	ANO
Libovolné kombinaci výše popsaných	ANO
Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	ANO

Vyhledávání, filtrování a vizualizace dat	
Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	ANO
Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	
Podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	ANO
Prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.	ANO
Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	ANO
Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.	ANO

Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.	ANO
Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.	ANO
Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	ANO

Kontextuální informace	
Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:	
Jméno uživatele a další jeho parametry z doménového řadiče (MS AD), včetně její historie.	ANO
Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu.	ANO
IP geolokace.	ANO
IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá.	ANO
Historie použitých MAC adresa a výrobce zařízení.	ANO
Operační systém a jeho historie na zařízení.	ANO
Uživatelem zadané poznámky a informace k zařízení.	ANO
Automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	ANO
Seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat.	ANO
Seznam detekovaných bezpečnostních a provozních událostí daného zařízení.	ANO

Zaznamenávání, ukládání a zpětná analýza plného provozu	
Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	ANO
Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru.	ANO
Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.	ANO

Monitorování politik kybernetické bezpečnosti
Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:

monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	ANO
detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	ANO
Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí:	
uživatelem definované podsítě na základě rozsahů IP adres	ANO
uživatelsky libovolně definovaných skupin zařízení	ANO
automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	ANO

Management bezpečnostních událostí a incidentů	
Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	
Spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele.	ANO
Jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů.	ANO
Možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).	ANO
Možnost exportování dat do emailu, csv, pdf, syslogu a podobně.	ANO
Možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	ANO

Detekce úniku dat	
Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).	ANO
Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.	ANO
V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	
Název souboru.	ANO
Velikost souboru.	ANO
HASH souboru.	ANO

Monitoring cloudových služeb	
Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.	ANO
Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.	ANO

Inventarizace sítě a grafická vizualizace topologie	
Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.	ANO
Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.	ANO
Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.	ANO
Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.	ANO

Další požadavky	
Podmínkou je implementace na dedikovaný operační systém ve virtualizovaném prostředí, včetně licencí pro databázový server, šifrované spojení, grafický program na správu.	ANO
Implementační projekt, vč. požadovaných akceptačních kritérií.	ANO
Součástí nabídkové ceny je i cena rozhraní na stávající informační systém, instalace, kompletní oživení systému, administrátorské školení a základní zaškolení obsluhy pro práci s jednotlivými zařízeními a SW.	ANO
Nutné migrace pro úspěšné nasazení díla do provozu tak, aby bylo plně datově kompatibilní se stávajícím prostředím a informačními systémy.	ANO
Vytvoření kompletní a detailní provozní dokumentace dle standardů ISVS (Informační systém veřejné správy, zák. č. 365/2000 Sb.).	ANO
Dodavatel odpovídá za vady dodávky po dobu záruční lhůty, která je stanovena na 72 měsíců od doby předání.	ANO
Dodávané softwarové aplikační komponenty musí splnit požadavky zákona 365/2000 Sb. "O informačních systémech veřejné správy a o změně některých dalších zákonů" v platném znění v návaznosti na par. 5 odst. d), tj. doložit atesty na agendy, mající vazbu na jiné informační systémy státní správy (datové schránky, základní registry, JIP, apod.).	ANO
Řešení bude splňovat nařízení GDPR, eIDAS2, NIS2, případně další.	ANO
Dokumentace skutečného provedení.	ANO
Jednoduchá příručka pro uživatele.	ANO

Akceptační test
Úspěšná detekce přenosu citlivých souborů skrze: HTTP, FTP, SMTP, SMB, NFS.
Úspěšná detekce změn v síti.

Příloha č. 2 – Seznam realizačního týmu

Poř. číslo	Jméno	Pozice, působnost, zodpovědnost, vymezení podílu na realizaci zakázky, právní vztah k dodavateli
1	[redacted]	**Vedoucí projektu** Vedení zakázky, stanovení a kontrola realizace cílů implementace Zaměstnance
2		**Systémový inženýr** Implementace a konfigurace dodaných technologií, zpracování dokumentace, test funkcionality, zaškolení obsluhy Zaměstnanec

Příloha č. 3 - Rozpočet - Cena jednotlivých dílčích plnění

Položka	Počet jednotek	Cena za jednotku bez DPH	Celkem za položku bez DPH
Dodání systému včetně dalších služeb			
Servisní podpora - měsíc			
Celková cena			

Příloha č. 4 – Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele

- Bezpečnost přístupových oprávnění
    - Poskytovatel je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům poskytovatele, které umožňují přístup k informačním aktivům objednatele či umožňují jejich správu.
    - Poskytovatel 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 rok.
    - Poskytovatel 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 Poskytovatel zřizoval přístupová oprávnění třetí straně, je poskytovatel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.
- Řízení kybernetických bezpečnostních incidentů:
    - Poskytovatel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv objednatele nebo informačních aktiv poskytovatele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv objednatele.
    - Poskytovatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy objednatele.
- Řízení kontinuity činností
    - Poskytovatel se zavazuje plnit úkony definované v sestaveném a objednatelem odsouhlaseném disaster recovery plánu, který je součástí dodané provozní dokumentace.
- 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 poskytovatelem i případnými subdodavateli.
    - Poskytovatel se zavazuje všechny jím provedené změny i změny případných subdodavatelů poskytnout objednateli formou pravidelného čtvrtletního reportu.