SMLOUVA

„Telč – rozvoj služeb eGovernementu a Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče – část 7 – Logmanagement, ochrana DNS“
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 7. 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 7 – Logmanagement, ochrana DNS**“ (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 2 161 831,00 Kč + DPH ve výši 453 984,51 Kč; cena včetně příslušné výše DPH činí 2 615 815,51 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 učtu 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]
-

Za poskytovatele:

- [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 7 – Logmanagement, ochrana DNS Sběr a vyhodnocování kybernetických bezpečnostních událostí - Systém pro správu strojových dat a logů SIEM/SEM	Splňuje ANO/NE
Licence	
Trvalá licence	ANO

Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	
Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.	ANO
Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	ANO
Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli není povinná konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se skripty/makra vkládají.	ANO
Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému – Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webové rozhraní viz buňka A8. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.	ANO
Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně.	ANO
Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále zadavatel požaduje podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta.	ANO
Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definova- ných parserech.	ANO

Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	ANO
Standardizované pole dekódované z přijatých zpráv musí provádět minimálně tyto operace (pokud zdrojový log tyto informace obsahuje), názvy polí se můžou lišit, nicméně musí být v dodaném systému konzistentní - username = uživatelské jméno, src_ip = zdrojová IP adresa IPv4 nebo IPv6 včetně přeloženého DNS PTR, dst_ip = cílová IP adresa IPv4 nebo IPv6 včetně přeloženého DNS PTR, src_port = zdrojový port uložený v číselné podobě, dst_port = cílový port uložený v číselné podobě, protocol = druh přenosového protokolu, status = informace o stavu provedené akce (úspěch/neúspěch apod.), duration = kolik vteřin událost trvala uložena v číselné podobě.	ANO
Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí. Každá událost musí mít navíc unikátní identifikátor, který zůstává jedinečný po celou životnost produktu.	ANO
Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ANO
Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	ANO
Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou – administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	ANO
Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.	ANO
Systém provádí konsolidaci logů na interním storage logovacího systému.	ANO
Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu, manuální aktualizace a umožňuje používat tuto funkci jen pro vybrané IP adresné prostory.	ANO
Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.	ANO
Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	ANO
Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.	ANO

V případě krátkodobého (do cca 10 min) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován.	ANO
Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	ANO
Uchazeč musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.	ANO
Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem systému nevratně modifikovat nebo smazat.	ANO
Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.	ANO
Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO
Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.	ANO
Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.	ANO
Systém nabízí kapacitní i výkonovou škálovatelnost.	ANO
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40 TB dat.	ANO
Požadujeme, aby ze systému bylo možné za běhu vytáhnou libovolné 2 disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ANO
Pokročilá telemetrie a monitoring stavu systému. Systém musí umět zobrazovat kromě běžných telemetrických dat o svojí činnosti i data ohledně rychlosti indexování, délce fronty dat čekající na zpracování a rychlosti odezvy DNS serverů vyřizujících DNS PTR odpovědi. Dále musí umožňovat alertování při překročení prahových hodnot nebo chybě systému, s odesláním upozornění pomocí SMTP nebo Syslogu.	ANO
Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo, aby se konfigurace musela provádět mimo jednotné webové rozhraní.	ANO
Zadavatel požaduje, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému.	ANO

Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.	ANO
Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	ANO

Výkonnostní a SW parametry systému	
Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli, například není nutné editovat žádné konfigurační soubory, scripty nebo makra).	ANO
Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému.	ANO
Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce.	ANO
Systém bude přijímat logy z cca 250 zařízení. Retence dat minimálně 300 dnů.	ANO
Průměrný trvalý příjem min. 2 tisíc událostí/s Výkon musí odpovídat pro požadované množství událostí s průměrnou délkou minimálně 700 Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat, zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	ANO
Špičkový příjem minimálně 4 tisíc událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700 Byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalém příjmu událostí.	ANO
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40TB a nad to musí podporovat kompresi ukládaných dat.	ANO
Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi.	ANO
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	ANO
Systém musí podporovat doplňování zpráv o statické informace z textových tabulek. (Například k uživatelskému jménu doplnit informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes webové rozhraní.	ANO

Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů zadavatel požaduje mít možnost vložení minimálně 20 testovacích zpráv současně.	ANO
V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z Windows, zpráva byla vygenerována firewallem atd...	ANO
V centrální správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	ANO
Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	ANO
Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	ANO
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.	ANO
Podpora zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Systém umožňuje obnovit data ze záloh a během obnovy je automaticky znova indexovat tak, aby bylo možné v datech obnovených ze záloh pracovat shodně jako s aktuálním obsahem databáze. Zálohování musí jít kompletně nastavit v uživatelském rozhraní systému, nepřipouští se využívání scriptů, maker nebo textových konfiguračních souborů.	ANO

Alerty	
Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO
Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	ANO
Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO
Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby.	ANO
Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran.	ANO
V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku).	ANO

Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a výsledku testu o provedené akci.	ANO

Sběr událostí z Microsoft prostředí	
Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních Windows logů, tak monitoring textových souborových logů. . Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.	ANO
Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	ANO
Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole.	ANO
Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně Windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného aletru. Filtry musejí umožňovat okamžitě testovat jejich účinnost a zobrazit kolik z uložených dat zvolený filtr zasáhne a kolik logů by případně filtroval minimálně za posledních 24 hodin.	ANO
Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy.	ANO
Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	ANO
Komunikace Windows agenta a centrálního systému musí být šifrovaná.	ANO
Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu.	ANO
Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ANO
Počet instalací Windows agenta by neměl být licenčně a časově omezen, pokud je licenčně omezen, tak požadujeme dodání licencí na Windows agenty v množství 100 na dobu předpokládané morální životnosti produktu	ANO

Podpora pro sběr událostí z poboček	
Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.	ANO
Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.	ANO

Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	ANO
Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	ANO
Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO
Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	ANO
Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	ANO
Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO
Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO

SW Podpora	
HW - Požadované minimálně 6 letá servisní podpora na HW appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	ANO
Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	ANO
SW - Podpora výrobce na aktualizaci systému a parserů na 6 let. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	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
Odeslaný alert po splnění podmínek emailem.
Vytvoření vlastního parseru.
Analýza logů ze sítě za dobu 14 dnů.

Část 7 – Logmanagement, ochrana DNS	Splňuje ANO/NE
Nástroj pro detekci kybernetických bezpečnostních událostí - Kontrola provozu DNS	

Licence	
Trvalá licence	ANO

Obecné požadavky	
Počet uživatel 120.	ANO
Řešení s ochranou na úrovni DNS.	ANO
Zachycení malware.	ANO
Detekce nultého dne pro algoritmus generování domény.	ANO
Homografické phishingové útoky.	ANO
Komunikace C&C.	ANO
Exploit, Backdoor, Trojan, Keylogger.	ANO
Spamové domény.	ANO
Malicious coin mining.	ANO
DNS tunelování.	ANO
Cache poisoning.	ANO
DNS rebinding útok.	ANO
Detekce a upozornění na anomálie DNS.	ANO
Nevyžaduje úpravu na koncových stanicích:	ANO
Není potřeba instalovat SW na koncovou stanici.	ANO
Bez nutnosti ruční rekonfigurace musí být vše provedeno automaticky.	ANO
Není třeba instalovat certifikáty nebo resetovat zásady zabezpečení.	ANO

Administrativní interface	
Webové rozhraní pro administrátora je plně přístupné prostřednictvím webových prohlížečů bez nutnosti instalace doplňků nebo lokálního softwaru potřebného pro přístup k rozhraní.	ANO
Možnost aktivovat dvoufaktorovou autentizaci a vynutit dvoufaktorovou autentizaci pro všechny administrátory v organizaci.	ANO
Možnost omezení přístupu do administrátorského rozhraní pouze z lokální sítě nebo z definovaných rozsahů veřejných IP adres.	ANO
Pro operátory v minimálně 2 rolích jsou k dispozici různá nastavení oprávnění (pro jednotlivé skupiny):	
Správce	ANO
Uživatel s právy čtení	ANO
K dispozici je záznam DNS provozu ze všech resolverů včetně fulltextového filtrování v jednotném rozhraní.	ANO

Podrobnosti všech unikátních požadavků/odpovědí budou přístupné a exportované pro další analýzu ve formátu csv.	ANO
Administrátorské webové rozhraní poskytuje přístup do všech funkcí.	ANO
Analýza hrozeb.	ANO
Analýza provozu DNS.	ANO
Analýza filtrování obsahu.	ANO
Konfigurace bezpečnostního filtrování.	ANO
Konfigurace filtrování zabezpečení.	ANO
Konfigurace bezpečnostních politik.	ANO
Možnost vytváření vlastních whitelistů a blacklistů.	ANO
Konfigurace vizuálu blokující stránky.	ANO
Konfigurace nastavení resolveru.	ANO
Správa překladače DNS.	ANO
Přehled řešitelů.	ANO
Přiřazování zvláštních zásad konkrétním rozsahům IP adres.	ANO
Možnosti upgradu / aktualizace verze resolveru.	ANO
Pokročilé možnosti konfigurace.	ANO
Procházení změn protokolu resolveru.	ANO
Upozornění.	ANO

Funkce a komponenty	
On-premise resolver.	
Plně autonomní DNS resolver s bezpečnostní vrstvou, která provádí řešení a filtrování sama bez nutnosti komunikace s externí službou v cloudu.	ANO
V souladu se standardy RFC.	ANO
Bezpečnostní vrstva umožňuje přesměrování požadavků na problematické domény na blokovací stránku.	ANO
Podpora ověřování DNSSEC včetně negativního ukládání do mezipaměti NSEC3.	ANO
Změny konfigurace a aktualizace resolveru se provádějí za plného provozu – bez výpadku služby a bez výpadku DNS provozu, během aktualizací a rekonfigurací.	ANO
Podpora použití DNS přes TLS a DNS přes HTTPS.	ANO
Blokační stránka.	
Jedná se o webovou stránku, na kterou je uživatel přesměrován, když se jeho zařízení pokusí o přístup na problematickou webovou stránku.	ANO
Blokační stránku lze libovolně upravit dle přání zákazníka tak, aby respektovala firemní identitu a vizuál (fonty, barvy, logo, kontakty).	ANO
Funkce "ByPass" pro definované sítě - uživatel může pokračovat do cílové domény bez nutnosti součinnosti správce (např. pro sítě pro hosty).	ANO
Správa provozu DNS a firewall.	
Specifické zóny mohou být přesměrovány na vybrané IP adresy.	ANO
Požadavky na interní domény lze přesměrovat na řadiče domény nebo jiné autoritativní servery.	ANO
Prefetching DNS cache - záznamy v cache jsou před vypršením platnosti obnoveny.	ANO

DNS záznamy jsou uchovávány v paměti déle, než by měly být autoritativní jmenné servery pro danou zónu nedostupné kvůli období ttl (např. domain.com je nedostupná po dobu jedné hodiny, resolver bude moci použít poslední odpověď, kterou měl pro tuto doménu).	ANO
DNS firewall - možnost definovat přístupová pravidla pro konkrétní domény - povolení přístupu pouze k vybraným doménám v rámci IP podsítě. Příklad použití – povolení přístupu na klientské stroje pouze do domén Office365, vrácení odpovědi NXDOMAIN ostatním.	ANO
Automatická aktualizace seznamu domén Office365 a dalších služeb Microsoft Azure používaných v DNS firewallu.	ANO

Centrální správa	
Zobrazuje kompletní DNS provoz v reálném čase.	ANO
Možnost vyloučit konkrétní domény z protokolování (např. interní domény z důvodu dodržování předpisů).	ANO
Poskytuje a provádí:	
Aktualizace databáze podle bezpečnostního filtrování.	ANO
Správa resolveru a aktualizací softwaru.	ANO
Centrální úložiště protokolů a incidentů a poskytuje možnosti pro jejich vyhodnocování.	ANO
Protokol DNS Traffic včetně podrobností o všech jedinečných požadavcích / odpovědích pro další analýzu je přístupný a exportovaný ze všech překladačů ve společnosti a dostupný včetně úplných.	ANO

Security filtering engine	
Pro uživatele má nulovou latenci. Vyhodnocení zabezpečení je poskytováno v reálném čase bez požadavků přes síť.	ANO
Nasazení softwaru bez nutnosti nasazení na speciálně upravený hardware, s možností fungování ve virtuálním prostředí.	ANO
Ochrana proti útokům DNS spoofing na základě DNSSEC včetně podpory NSEC3 a negativního ukládání do mezipaměti.	ANO
Schopnost definovat různé bezpečnostní politiky a přiřazení k sítím založeným na CIDR nebo přiřazení na základě IP adresy resolveru.	ANO
Detekce Zero-day hrozeb bez nutnosti předchozí znalosti dané domény.	ANO
Detekce a upozornění na anomálie v DNS provozu.	ANO
Možnost varovat / blokovat z vnitřní sítě přístup k doménám, které vypadají podobně jako definovaná doména společnosti/organizace pro ochranu před cílenými phishingovými útoky.	ANO
Možnost blokovat přístup k doménám podle kategorie obsahu alespoň v rozsahu:	
Coin miners	ANO
P2P připojení (např. torrenty)	ANO
DNS přes HTTPS	ANO
Pornografie	ANO
Hazardní hry	ANO
Násilí	ANO
Sledování	ANO
Reklamní	ANO

Sociální sítě	ANO
Hry	ANO
Měl by zajistit ochranu před zneužitím DNS provozu pro tunelování další komunikace v technicky platných DNS paketech a komunikaci s externími servery (zabezpečení DNS tunelování).	ANO
Vrstva tunelování DNS proaktivně narušuje tunelování DNS na několika úrovních:	
Resolver.	ANO
Nervová síť.	ANO
Zásady umožňují správcům upravovat:	
Úroveň ochrany.	ANO
Úroveň detekce.	ANO
Kategorie hrozeb jsou zahrnuty ve zvláštních zásadách.	ANO
Vlastní blacklist a whitelist.	ANO
Kategorie blokovaného obsahu.	ANO
Správa DNS resolveru.	
Poskytuje vzdálenou diagnostiku.	ANO
Monitorování hardwarových problémů.	ANO
Softwarové monitorování.	ANO
Sběr logů.	ANO
Vyhodnocení latence překladu.	ANO
Aktualizace softwaru a rollbacks.	ANO
Možnost okamžitého vrácení jakékoli aktualizace do předchozího stavu.	ANO
Lokální management.	ANO
Úplný přístup k protokolům pro místní správce.	ANO
Lokální CLI.	ANO

Alerting	
Konfigurovatelné filtry pro domény, sítě a akce	ANO
Četné možnosti doručení a protokoly pro doručení výstrah, včetně:	
E-mailem	ANO
Syslog (TLS)	ANO
Slack	ANO
Webhook (REST API).	ANO
Další platformy na doručení alertů (na vyžádání).	ANO
Alerting je založen na:	
Práh událostí zabezpečení a provozu DNS.	ANO
Detekce dynamických anomálií.	ANO
Whitelist a blacklist.	ANO
	ANO
Off network protection	
Součástí řešení je i aplikace nainstalovaná lokálně na mobilních zařízeních, která zajistí stejnou úroveň ochrany zařízení, jako by byla v lokální síti pod ochranou lokálního resolve-ru.	ANO
Podporovaný operační systém:	
Windows	ANO

Android	ANO
iOS	ANO
Možnost hromadného nasazení prostřednictvím Group policy na počítačích spravovaných v doméně.	ANO
Hromadná instalace na Android / iOS možná přes MDM.	ANO
Reporting	
Zprávy jsou doručovány e-mailem na předem definované adresy.	ANO
Možnost nastavení periodicity (7/14/30 dní) a dne v týdnu.	ANO
Shrnutí průběžných zpráv.	ANO
Objem provozu.	ANO
Počet hrozeb podle jednotlivých kategorií.	ANO
Podezřelá a infikovaná klientská zařízení.	ANO
Převládající rodiny škodlivého kódu a škodlivých domén.	ANO
Ochrana identity	
Produkt podporuje ochranu vlastních doménových identit.	ANO
Hlášení e-mailových schránek, které jsou součástí veřejně potvrzených úniků dat.	ANO
Seznam historických úniků, kde byly e-mailové adresy dané domény uváděny.	ANO
Sledování nových úniků a upozornění na nové úniky.	ANO
Hlášení obsahuje seznam typů citlivých údajů, které figurovaly v úniku (hesla, telefonní čísla, osobní údaje, e-mail, pohlaví, bankovní údaje).	ANO
Produkt umožňuje správu incidentů na elementární úrovni – tedy označení incidentu jako vyřešeného/vyřešitelného.	ANO
Produkt obsahuje doporučení, jak řešit daný únik citlivých dat.	ANO
Integrační procesy.	
Dostupnost REST API pro vyhledávání informací.	ANO
Statistiky provozu DNS.	ANO
Parametr REST API pro filtrování na základě.	ANO
Zdrojová IP adresa.	ANO
Cílová doména.	ANO
Typ požadavku.	ANO
Typ hrozby.	ANO
Na IP adresu odpovědi.	ANO
Čas.	ANO
Monitorování SNMP.	ANO
Dostupné šablony pro rychlou integraci s PRTG, Zabbixem nebo jiným hostitelem SNMP.	ANO
Integrace Syslog (SIEM, správa protokolů, provozní monitorování atd.).	ANO
Konfigurovatelný datový tok přes syslog obsahující detekované hrozby.	ANO
Konfigurovatelný datový tok přes syslog obsahující provoz DNS.	ANO
Konfigurovatelná nejvyšší data přes syslog obsahující bloky z filtrování obsahu.	ANO
Konfigurovatelná nejvyšší data přes syslog obsahující metriky a systém resolveru.	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
Dvoufaktorově ověřený přístup.
Odeslání alertu na e-mail.
Reporting
Úspěšné zablokování přístupu k doménám s nevhodným obsahem.

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 poddodavatele

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.