SMLOUVA O DÍLO

„Zvýšení kybernetické bezpečnosti informačních systémů krajského úřadu“

(dále jen „smlouva“)

uzavřená ve smyslu ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, (dále jen „ObčZ“)

pod evidenčním číslem objednatele: S-4424/INF/2019

Objednatel:

Středočeský kraj

se sídlem: Zborovská 81/11, 150 21 Praha 5 - Smíchov

IČO: 70891095

ID datové schránky: keebyyf

zastoupené: Martinem Hermanem, radním pro oblast investic a veřejných zakázek

bankovní spojení: PPF, a.s.

číslo účtu: [redacted]

Zhotovitel:

O2 Czech Republic a.s.

se sídlem: Praha 4 - Michle, Za Brumlovkou 266/2, PSČ 14022

IČO: 601 93 336

DIČ: CZ60193336

za níž jedná: Petr Krutký, na základě pověření ze dne 26.6.2019

zapsaná v Obchodním rejstříku vedeném Městským soudem v Praze spisová značka B2322

tel.:[redacted] fax.: [redacted] e-mail [redacted]

bankovní spojení: KB, a.s. Praha

číslo účtu: [redacted]

dále společně jako „smluvní strany“

I.

Preambule

Tato smlouva je uzavírána na základě výsledku zadávacího řízení s názvem „**Zvýšení kybernetické bezpečnosti informačních systémů krajského úřadu (II)**“ uveřejněným ve věstníku veřejných zakázek pod evidenčním číslem Z2019-019389 a na profilu zadavatele.

II.

Předmět smlouvy

1) Předmětem smlouvy je závazek zhotovitele provést pro objednatele dílo spočívající v dodávce HW, SW a zajištění služeb souvisejících s projektem „Zvýšení kybernetické bezpečnosti informačních systémů krajského úřadu“. Cílem projektu je dodávka a implementace vybraných nástrojů kybernetické bezpečnosti do informačních systémů Krajského úřadu Středočeského kraje (dále též KÚSK) v technologických centrech Středočeského kraje (TCK) v Praze (HTCK v sídle objednatele) a Kladně (ZTCK na adrese Oblastní nemocnice Kladno, Vančurova 1548), a to v rozsahu dle zadávací dokumentace veřejné zakázky „Zvýšení kybernetické bezpečnosti informačních systémů krajského úřadu (II)“, zejména přílohy č. 6 zadávací dokumentace (Technická specifikace veřejné zakázky) a dále nabídky zhotovitele a této smlouvy (dále „dílo“). Dílo bude zahrnovat zejména:

    - Zhotovení předimplementační analýzy a prováděcí dokumentace;
    - Dodávku systému pro pokročilý provozní dohled (SW) vč. instalace, testování a uvedení do provozu a dále včetně licencí potřebných pro použití v rámci celé organizace objednatele;
    - Dodávku systému podpory pokročilé segmentace sítě (HW, SW) vč. instalace, testování a uvedení do provozu a dále včetně licencí potřebných pro použití v rámci celé organizace objednatele;
    - Dodávku komponent pro zajištění zvýšení fyzického zabezpečení HTCK (HW, SW) vč. instalace, testování a uvedení do provozu a dále včetně licencí potřebných pro použití v rámci celé organizace objednatele;
    - Zajištění sdílených služeb kybernetické bezpečnosti. Tato služba bude zahrnovat další níže uvedené služby:
        (a) Zaznamenávání a ukládání logů a detekce bezpečnostních událostí
        (b) Analýza datových toků a detekce bezpečnostních událostí
        (c) Dohledové centrum - SOC
    - Zajištění tzv. Služeb spojených s implementací IS dle kapitoly 5 Přílohy č. 1 této smlouvy
    - Integraci dodaného díla se stávajícím aplikačním (SW, IS) vybavením zadavatele;
    - Integraci dodaného díla se stávajícím HW vybavením zadavatele;
    - Implementaci IS do technologického centra Středočeského kraje (TCK);
    - Migraci dat dle pokynu objednatele;
    - Základní zaškolení obsluhy;
    - Záruční servis v délce trvání 60 měsíců garantovaný výrobcem;
    - Podpora a údržba díla v trvání 60 měsíců.

2) Podrobná specifikace technického řešení je uvedena v příloze č. 1 této smlouvy a tvoří její nedílnou součást.

3) Zhotovitel se zavazuje provést na svůj náklad a na své nebezpečí všechna související plnění a práce potřebné k včasnému a řádnému provedení díla.

4) Součástí smlouvy je i převod neomezeného vlastnického práva k tomuto dílu na objednatele. Součástí závazku zhotovitele je rovněž doprava zboží objednateli do místa plnění, jeho instalace a zprovoznění podle pokynů objednatele, a dále provádění záručních oprav díla.

5) Zhotovitel je dále povinen poskytovat podporu a údržbu v rámci druhé etapy díla (viz čl. III odst. 5) této smlouvy) a dále za podmínek uvedených v čl. III odst. 5 bodu 5.3 poskytovat práce a služby nad rámec podpory definované touto smlouvou, a to na základě samostatně objednatelem vystavených a podepsaných objednávek v cenách garantovaných touto smlouvou (viz článek IV. – platební podmínky).

III.

Doba a místo plnění, akceptace a předání díla

1) Místem plnění smlouvy je:

   a) sídlo objednatele Krajský úřad Středočeského kraje, Zborovská 81/11, 150 21 Praha 5 – Smíchov (Hlavní technologické centrum kraje – HTCK)

   b) Oblastní nemocnice Kladno, Vančurova 1548, 272 59 Kladno (Záložní technologické centrum kraje – ZTCK).

2) Zhotovitel se zavazuje, že dílo dokončí a umožní objednateli jeho převzetí nejpozději **do 3 měsíců** od účinnosti smlouvy. Dokončením díla se rozumí podpis předávacího protokolu dle tohoto článku.

3) Dílo bude realizováno ve dvou etapách, které jsou rozepsány níže.

4) **První etapa** (investiční) - zahrnuje:

   a) Zajištění tzv. Služeb spojených s implementací IS dle kapitoly 5 Přílohy č. 1 této smlouvy, zejména zajištění Základní analýzy, prováděcí dokumentace a aktualizovaného závazného harmonogramu plnění zakázky, které budou předloženy objednateli ke schválení do 10 pracovních dnů od podpisu smlouvy a které musí být v souladu s přílohou č. 1 (Technická specifikace veřejné zakázky) této smlouvy a dále s nabídkou zhotovitele. Podmínkou zahájením dodávky dle bodu níže je schválení předimplementační analýzy a prováděcí dokumentace ze strany objednatele. Objednatel je oprávněn odmítnout schválení předimplementační analýzy a prováděcí dokumentace v případě, že nejsou v souladu s přílohou č. 1 (Technická specifikace veřejné zakázky) této smlouvy a dále s nabídkou zhotovitele, přičemž konečný termín předání díla v délce 3 měsíců od účinnosti smlouvy musí být dodržen.

   b) Dodávku systému pro pokročilý provozní dohled (SW) včetně nezbytných licencí, jejich implementaci, nastavení a zprovoznění v souladu se závazným harmonogramem, který je přílohou č. 3 této smlouvy.

   c) Dodávku systému podpory pokročilé segmentace sítě (HW, SW) včetně nezbytných licencí, jejich implementaci, nastavení a zprovoznění v souladu se závazným harmonogramem, který je přílohou č. 3 této smlouvy.

   d) Dodávku komponent pro zajištění zvýšení fyzického zabezpečení HTCK (HW, SW) včetně nezbytných licencí, jejich implementaci, nastavení a zprovoznění v souladu se závazným harmonogramem, který je přílohou č. 3 této smlouvy.

   e) Poskytnutí příslušných licencí a/nebo multilicencí, integraci SW řešení a provedení základního školení uživatelů vč. předání veškeré odpovídající technické a uživatelské dokumentace.

   f) Řádné provedení implementace díla bude ověřeno v rámci testovacího provozu v délce 1 měsíce ukončeného oboustranným podpisem akceptačního protokolu testovacího provozu.

g) Po ukončení testovacího provozu bude vyvoláno **akceptační řízení**, zakončené podpisem **Akceptačního protokolu (AP),** který podepíší oprávnění zástupci obou smluvních stran. Akceptační procedura zahrnuje ověření řádné implementace díla u objednatele v souladu se specifikací stanovenou touto smlouvou a jejími přílohami. Objednatel potvrdí plnou funkčnost díla nebo díla s vadami, které nebrání jeho řádnému užívání, které je zhotoveno v souladu s touto smlouvou a v souladu se schváleným harmonogramem dle článku III., odst. 4. Přílohou AP bude i soupis veškerých předávaných komponent v editovatelné podobě. Po úspěšném ukončení akceptačního řízení dojde k předání díla přejímacím řízením.

h) V případě, že akceptační řízení prokáže nezpůsobilost dodaného řešení nasazení do produkčního prostředí, zaznamenají se tyto nedostatky do akceptačního protokolu s termíny, v nichž je zhotovitel povinen vady a nedostatky odstranit a dílo k úspěšné akceptaci připravit. Poté se akceptační řízení opakuje dle článku III., odst. 4, písm. g).

i) Nejpozději na poslední den provedení předmětu díla, resp. jeho části dle článku III., odst. 2, svolá zhotovitel **přejímací řízení**. Na přejímací řízení přizve zhotovitel objednatele, a to písemným oznámením, které musí být doručeno objednateli alespoň pět pracovních dnů předem. V případě, že nebude objednateli řádně a včas doručena výzva k účasti na přejímacím řízení, může dojít k přejímacímu řízení nejdříve po uplynutí pátého pracovního dne ode dne doručení písemné výzvy k zahájení přejímacího řízení.

j) Součástí přejímacího řízení je předání veškeré dokumentace zhotovitelem objednateli v originálech, a to jak ve formě papírových dokumentů, tak v elektronické editovatelné podobě, u SW podpory též předání přístupových hesel a uživatelských manuálů. Dále bude předána provozní dokumentace, v rozsahu odpovídajícím požadavkům zákona č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů a/nebo zákona č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů, projektová dokumentace v rozsahu odpovídajícím předmětu díla, zejména pak technická dokumentace díla, zápisy z projektových porad a další odpovídající podklady nebo dokumenty související s plněním a dodáním předmětu díla.

k) **Předání** akceptovaného díla se uskuteční fyzickým převzetím objednatelem. Předání díla bude oboustranně stvrzeno podpisem Předávacího protokolu. Předávací protokol bude podepsán oprávněnými zástupci obou smluvních stran. Dílo se považuje za převzaté a předané okamžikem podpisu Předávacího protokolu ve smyslu věty předchozí.

l) **Předávací protokol (PP)** musí obsahovat předmět a charakteristiku předmětu díla, resp. jeho částí a soupis dodaných logických technologických celků dodaného díla. Přílohami Předávacího protokolu budou i protokoly z akceptačního řízení. Dále bude obsahovat zhodnocení jakosti předmětu díla a jeho částí. V případě zjištěných vad bude obsahovat jejich soupis, lhůty pro jejich odstranění a stanovisko objednatele. V Předávacím protokolu musí být uvedeno, zda objednatel dílo přejímá či nikoli. Předávací protokol bude vyhotoven ve třech stejnopisech, z nichž jeden obdrží zhotovitel a dva objednatel. Každý stejnopis bude podepsán oprávněnými osobami obou smluvních stran a má právní sílu originálu.

m) V případě, že se při přejímání předmětu díla objednatelem prokáže, že je zhotovitelem předáván předmět díla, který nese podstatné vady bránící funkcionalitě díla či jeho části k účelu, k němuž má být využíváno, není objednatel povinen předávaný předmět díla převzít. Tato skutečnost bude uvedena v Předávacím protokolu. Po odstranění těchto podstatných vad předmětu díla či jeho části, pro které objednatel odmítl od zhotovitele předmět díla převzít, se opakuje přejímací řízení analogicky dle článku III., odst. 4, písm. i) a násl. této smlouvy. V takovém případě bude k původnímu předávacímu protokolu sepsán dodatek, ve kterém bude uvedeno převzetí předmětu díla. Dodatek obsahuje veškeré náležitosti stanovené pro předávací protokol dle článku III., odst. 4, písm. l) této smlouvy.

n) Vadou se pro účely této smlouvy rozumí odchylka v kvantitě, kvalitě, rozsahu, termínech nebo parametrech díla stanovených touto smlouvou, zadávací dokumentací a obecně závaznými předpisy.

5) **Druhá etapa** (provozní) – zahrnuje následující plnění po dobu 60 měsíců ode dne podpisu PP:

5.1) Zajištění a poskytování sdílené služby kybernetické bezpečnosti, obsahující služby:

a. zaznamenávání a ukládání logů a detekce bezpečnostních událostí
b. analýza datových toků a detekce bezpečnostních událostí
c. dohledové centrum - SOC

5.2) Podpora a údržba díla

a) Podpora a údržba systému pro pokročilý provozní dohled

b) Podpora a údržba systému podpory pokročilé segmentace sítě

c) Podpora a údržba zajištění zvýšení fyzického zabezpečení HTCK

d) Poskytnutí všech upgrade a update produktů distribuovaných po dobu účinnosti této smlouvy včetně instalace a nasazení.

e) Úpravy vyplývající ze změn legislativy tak, aby po celou dobu účinnosti této smlouvy dílo splňovalo zákonné požadavky na jeho provoz.

f) Zálohování dle harmonogramu dohodnutého s objednatelem.

g) Identifikaci příčin chybových stavů, návrh jejich fixace a fixaci chyby, opravy následků hardwarových, softwarových nebo datových chyb systému.

h) Poradní a konzultační služby po telefonu, e-mailu, HelpDesku/hot-line zhotovitele nebo osobní asistencí poskytované pracovníky zhotovitele.

i) Pravidelnou komplexní měsíční kontrolu technického stavu provozu díla.

j) Pravidelnou komplexní měsíční kontrolu konzistence dat v datové základně systému.

k) Průběžnou aktualizaci datové základny systému podle změn a vývoje databázových a aplikačních technologií a technologií ochrany a bezpečnosti dat.

l) Návrh změn konfigurace systému a implementaci změn.

m) Aktivní podporu při reklamaci závad v programovém vybavení a službách.

n) Součinnost při ladění dynamiky a nastavení parametrů systému.

o) Konzultační služby při tvorbě nebo změnách provozních standardů a technologických postupů.

p) Konzultační služby při plánování přechodu na vyšší verze softwarového vybavení nebo jiný hardware.

q) Technickou pomoc při změnách konfigurace, reinstalaci nebo upgrade podporovaného programového vybavení nebo změnách prostředí, v němž je podporované programové vybavení nainstalováno.

r) Legislativní servis, kdy aktuální verze dodaného software musí být objednateli poskytnuta nejpozději k datu nabytí účinnosti nové právní úpravy za předpokladu vydání prováděcích předpisů k této úpravě nejpozději 60 dnů před nabytím účinnosti této nové právní úpravy (v opačném případě do 60 dnů od vydání prováděcích předpisů k příslušné právní úpravě).

s) Zásahy při řešení havarijních stavů.

t) Tvorbu a ladění administračních, zálohovacích a uživatelských skriptů.

u) Dávkové zpracování dat nebo export/import dat z/do databáze.

v) Vytvoření a průběžnou aktualizaci systémové a uživatelské dokumentace k jednotlivým částem díla.

w) Archivaci a údržbu zdrojových programů a datových struktur, jejich verzování, věcnou i časovou dokumentaci změn a rozšíření.

x) Poskytování programátorského servisu k odstranění případných technických, systémových či programových problémů, které by mohly ovlivnit využití systému a které nejsou způsobeny chybou systému.

y) Práce, výkony a činnosti výslovně tímto článkem neuvedené, u nichž však zadavatel s ohledem na svoje odborné znalosti a zkušenosti věděl nebo mohl vědět či předpokládat, že jejich provedení je nutné pro řádné plnění této smlouvy.

z) Podmínky plnění druhé etapy jsou podrobněji popsány v článku VIII – Podpora a údržba

5.3) Služby poskytované nad rámec podpory a údržby po dobu 60 měsíců ode dne převzetí díla (*výkony nad rámec podpory*“)

a) služby musí být poskytovány po dobu 60 měsíců ode dne předání díla (skončení první etapy), a to v předpokládaném rozsahu až 50 člověkodní (též man-day, či MD).

b) Školení a konzultace odborných pracovníků (administrátorů) objednatele zajišťované zhotovitelem na základě výzvy objednatele zhotoviteli.

c) Průběžné úpravy díla vyžádané objednatelem nad rámec článku III, odst. 5.2

d) Do rozsahu 50 MD budou tyto služby plněny na základě výzvy objednatele zhotoviteli. Na zadávání těchto výzev se přiměřeně použijí ustanovení článku VIII. Podpora a údržba díla. Po vyčerpání limitu 50 MD budou další požadavky tohoto typu objednatelem zadávány na základě samostatně vystavených a podepsaných objednávek dle hodinové sazby specifikované v čl. IV, odst. 3 smlouvy.

e) Objednatel je oprávněn (nikoli povinen) tyto služby čerpat dle své potřeby, popřípadě nečerpat žádné z těchto služeb. Nečerpáním, nebo čerpáním v nižším rozsahu nevzniká zhotoviteli nárok na úhradu jakékoli újmy, popřípadě právo odstoupit od této (části) smlouvy. Zhotovitel bere na vědomí, že limit 50 MD nemusí být objednatelem za celou dobu trvání smlouvy vyčerpán. Objednateli budou vyúčtovány vždy jen skutečně odvedené služby a práce.

IV.

Cena a platební podmínky

1) Cena díla je stanovena na základě nabídkové ceny zhotovitele, kalkulované v rámci zadávacího řízení na předmět plnění dle této smlouvy. Celková cena díla je stanovena dohodou smluvních stran a jako cena nejvýše přípustná.

2) **Cena je určena následujícím způsobem a vychází z Podrobného položkového rozpočtu, který je přílohou č. 2 této smlouvy a byl předložen v nabídce zhotovitele:**

	Cena bez DPH	Cena s DPH
První etapa	11.904.161,51 Kč	14.404.035,43 Kč
Druhá etapa	15.945.396,08 Kč	19.293.929,25 Kč
Celková cena	**27.849.557,59 Kč**	**33.697.964,68 Kč**

3) **Zhotovitel garantuje po celou dobu trvání této smlouvy hodinovou sazbu svých výkonů nad rámec podpory, poskytovaných na základě výzvy objednatelem ve výši 1.805,56 Kč bez DPH (slovy: jeden tisíc osm set pět korun českých padesát šest haléřů) za 1 hodinu takových prací. To platí i pro objednávky zadávané po vyčerpání limitu 50 MD. DPH bude účtováno ve výši dle platných účetních zákonů.**

4) Cena díla zahrnuje i servisní podporu v rámci záruky na dodané dílo, dopravu, instalaci, implementaci a zprovoznění díla. Cena díla zahrnuje i náklady na správní poplatky, daně, cla, schvalovací řízení apod. (je-li relevantní), pojištění, přepravní náklady apod.

5) Cena díla zahrnuje také veškeré náklady spojené s rozhraními (integracemi), vzniklými na straně zhotovitele, popř. vyvolanými nutností obchodní spolupráce mezi zhotovitelem a dodavateli stávajících aplikací, na něž jsou integrace (rozhraní) požadovány. Požadavek objednatele je, aby zhotovitel uvedl a zahrnul do ceny plnění veškeré náklady spojené jak s vytvořením rozhraní, tak jejich udržováním v rámci záruční doby, zejména při změnách vyvolaných updatem aplikací zhotovitele a to jak v souvislosti se změnami legislativy, tak v souvislosti s inovacemi aplikací zhotovitele, a to vč. úprav vzniklých na straně zhotovitele, popř. vyvolaných nutností obchodní spolupráce mezi zhotovitelem a dodavateli stávajících aplikací, na něž je integrace požadována.

6) Cenu díla je možné překročit pouze v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude ke kupní ceně připočteno DPH ve výši stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o dani z přidané hodnoty). Dojde-li ke zvýšení sazby DPH, bude ke smlouvě uzavřen dodatek.

7) Cena díla bude objednatelem uhrazena v korunách českých (CZK) na základě daňového dokladu (dále jen „faktura“) doručeného zhotoviteli. **Odměna za první etapu bude hrazena po akceptaci a předání díla objednateli (tj. po podpisu Předávacího protokolu oběma stranami). Odměna za druhou etapu bude hrazena v poměrných částkách vždy za uplynulé tři kalendářní měsíce, odměna za výkony nad rámec podpory bude zhotovitelem fakturována vždy za skutečně odvedené práce a služby**.

8) Přílohou faktury za první etapu musí být kopie Předávacího protokolu podepsaného osobami oprávněnými jednat za smluvní strany ve věcech realizace díla. **Přílohou faktury za druhou etapu musí být vždy Akceptační protokol, který musí vždy obsahovat i seznam služeb a prací poskytnutých zhotovitelem za uplynulé období a přehled vyčerpaných hodin výkonů nad rámec podpory z limitu 50 MD.**

9) Akceptační protokol za druhou etapu musí být podepsán tak, aby faktura za příslušné období byla objednateli doručena nejpozději do 15. dne měsíce následujícího po skočení fakturovaného období.

10) Faktura, musí obsahovat všechny náležitosti řádného daňového dokladu ve smyslu zákona o dani z přidané hodnoty.

11) Na faktuře bude uveden název projektu „**Zvýšení kybernetické bezpečnosti IS KÚ (II)**“ a číslo smlouvy objednatele. Na fakturách za druhou etapu bude uvedeno období, k němuž se vztahuje.

12) V případě, že faktura bude obsahovat věcné či formální nesprávnosti, popřípadě nebude obsahovat všechny zákonné náležitosti nebo přílohu dle předchozího odstavce, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli k doplnění či opravě, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury objednateli.

13) Splatnost faktury se sjednává na 60 dnů ode dne doručení faktury objednateli. Faktura se považuje za splacenou odepsáním fakturované částky z účtu objednatele.

14) Faktura bude uhrazena na účet zhotovitele uvedený v záhlaví této smlouvy. Pokud by zhotovitel v období od data, kdy podepsal smlouvu, do vystavení faktury změnil číslo bankovního účtu, musí tuto skutečnost sdělit objednateli nejpozději s předloženou fakturou. Toto sdělení musí být podepsané osobou zhotovitele oprávněnou k jednání ve věcech smluvních, nebo jím zmocněnou osobou. Při splnění této podmínky není změna účtu podnětem k uzavření dodatku ke smlouvě. Kupní cena pak bude uhrazena na bankovní účet uvedený na faktuře.

15) Objednatel neposkytuje zhotoviteli zálohy na cenu díla.

16) Zhotovitel prohlašuje, že není veden v registru nespolehlivých plátců, a zavazuje se po dobu trvání této Smlouvy řádně a včas platit DPH. Pokud FÚ vyzve objednatele k placení DPH nezaplacené zhotovitelem při realizaci této smlouvy, zhotovitel se zavazuje zaplatit objednateli smluvní pokutu ve výši odpovídající nezaplacenému DPH. Pokuta je splatná ve lhůtě do 30 dnů ode dne doručení vyúčtování o smluvní pokutě.

V.

Práva a povinnosti smluvních stran

1) Zhotovitel je povinen dodat objednateli úplné a funkční dílo, v množství, jakosti, provedení a termínu dohodnutých touto smlouvou. Dílo musí být realizováno v souladu s touto smlouvu a jejími přílohami, v souladu s platnými právními předpisy a příslušnými normami, jakož i v souladu s interními předpisy objednatele díla.

2) Objednatel se zavazuje dílo řádně a včas dodané zhotovitelem převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu sjednaném touto smlouvou.

3) Zhotovitel je povinen

4) Zhotovitel je povinen spolu s dílem dodat objednateli kompletní dokumentaci nezbytnou k užívání zboží, a to zejména záruční listy a návody v českém jazyce a další dokumentaci vyplývající z platné legislativy, zejm. zákona č. 365/2000 Sb. o informačních systémech veřejné správy, ve znění pozdějších předpisů, přičemž je současně povinen provést proškolení obsluhy díla a potřebné revize.

5) Zhotovitel prohlašuje, že ke dni uzavření této Smlouvy má uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti zhotovitele za škodu způsobenou zhotovitelem do výše limitu pojistného plnění v částce minimálně 9.000.000,- Kč z jedné pojistné události ročně. Kopie pojistné smlouvy dodavatele, resp. akceptovaný návrh na uzavření pojistné smlouvy ze strany pojišťovny dle tohoto článku byl předán objednateli před podpisem této smlouvy, jako jedna z podmínek pro uzavření smlouvy dle ust. § 104 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Zhotovitel se zavazuje na žádost objednatele bezodkladně, nejpozději však ve lhůtě do 5 pracovních dnů od doručení písemné výzvy objednatele, předložit objednateli pojistný certifikát prokazující existenci a účinnost této pojistné smlouvy. Zhotovitel se zavazuje, že pojistná smlouva dle věty první tohoto článku zůstane v účinnosti v tomto rozsahu po celou dobu trvání povinností zhotovitele dle této smlouvy.

6) Objednatel nabývá vlastnického práva k dílu dnem řádného předání a převzetí díla od zhotovitele na základě podpisu předávacího protokolu oběma smluvními stranami. Stejným okamžikem přechází na objednatele také odpovědnost za nebezpečí škody na zboží a oprávnění užít dílo včetně dokumentace předané k dílu.

7) Zhotovitel je povinen neprodleně písemně vyrozumět objednatele o případném ohrožení doby plnění a o všech skutečnostech, které mohou řádné a včasné plnění předmětu této smlouvy znemožnit, a to nejpozději do 3 dnů ode dne, kdy se zhotovitel dozví o takové skutečnosti.

8) Zhotovitel není oprávněn postoupit jakákoliv práva anebo povinnosti vyplývající z této smlouvy na třetí osoby bez předchozího písemného souhlasu objednatele. Uplatní-li třetí osoba své právo k dílu nebo jeho části, zhotovitel se zavazuje bez zbytečného odkladu a na vlastní náklady učinit potřebná opatření k ochraně výkonu práv objednatele.

9) Objednatel může oprávnění plynoucí z licence poskytnout zcela nebo z části třetí osobě.

10) Práva a povinnosti uvedené v tomto článku trvají i po ukončení tohoto smluvního vztahu, a to i v případě, že by došlo k předčasnému ukončení smlouvy.

11) Každá ze stran nese odpovědnost za způsobenou škodu v rámci platných právních předpisů a této smlouvy. Obě strany se zavazují vyvíjet maximální úsilí k předcházení škodám a k minimalizaci vzniklých škod.

12) Žádná ze stran neodpovídá za škodu, která vznikla v důsledku neúplného, věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé strany. Žádná ze smluvních stran není odpovědná za nesplnění svého závazku v důsledku prodlení druhé smluvní strany nebo v důsledku nastalých okolností vylučujících odpovědnost.

13) Obě smluvní strany odpovídají za škodu, kterou způsobí druhé straně porušením svých povinností dohodnutých touto smlouvou při provádění předmětu plnění této smlouvy a za podmínek daných touto smlouvou či povinností, které vyplývají už ze samotného předmětu plnění smlouvy. Zhotovitel se zavazuje uhradit objednateli případnou škodu, která vznikne z důvodu nedodání Díla či jeho části ze strany zhotovitele a kterou bude muset objednatel vynaložit, aby Dílo bylo zrealizováno či dokončeno.

14) V případě součástí díla, které jsou předmětem ochrany práv podle autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění, zhotovitel poskytne objednateli územně, časově i množstevně neomezenou výhradní převoditelnou licenci (právo užívat) na dílo a jeho případné další verze (upgrade programového vybavení) za cenu, která je již zahrnuta ve smluvní ceně podle této smlouvy, a to okamžikem předání, převzetí a zaplacení předmětu plnění smlouvy. Ujednání tohoto odstavce neplatí pro součásti díla, které představují standardizované software, resp. produkty třetích stran, které jsou běžně dostupné na trhu, tedy které si může koupit neomezený počet osob, a jejichž užívání se řídí licenčními podmínkami výrobce.

15) Smluvní strany sjednávají, že zhotovitel není oprávněn jakékoliv jeho pohledávky za objednatelem, které vzniknou na základě této smlouvy, započítat vůči pohledávkám objednatele za zhotovitelem jednostranným právním jednáním. Zhotovitel zajistí, že k předmětu díla nevzniknou autorská práva třetích stran ani nebude zatížen právy třetích osob, ze kterých by pro objednatele plynuly jakékoliv další finanční nebo jiné nároky třetích stran. Pokud by taková práva přesto existovala či v průběhu plnění vznikla, zhotovitel je povinen zajistit jejich bezplatný převod na objednatele, a to v plném rozsahu a na vlastní náklady, respektive na vlastní náklady zajistit vypořádání nároků třetích stran.

16) Zhotovitel poskytuje objednateli v rámci licence, právo užít dílo a dokumentaci předanou objednateli spolu s dílem, tj. zejména rozmnožovat, překládat, zpracovávat, upravovat či jinak měnit nebo nechat měnit, spojovat s jiným dílem, jakož i zařazovat do díla souborného, a získaná oprávnění

postupovat zcela nebo zčásti třetí osobě, v souladu s jeho účelem a určením vč. provádění oprav vad díla objednatelem nebo prostřednictvím jiných osob, s tím, že toto oprávnění začne platit ke dni dodání a převzetí díla objednatelem. Objednatel není povinen využít poskytnutou licenci ani z části. Ujednání tohoto odstavce neplatí pro součásti díla a dokumentaci, které představují standardizované software, resp. produkty třetích stran, které jsou běžně dostupné na trhu, tedy které si může koupit neomezený počet osob, a jejichž užívání se řídí licenčními podmínkami výrobce.

17) Objednatel se dnem poskytnutí licence k předmětu smlouvy stává neomezeným výhradním uživatelem díla, vytvořeného pro něj na zakázku zhotovitelem. Licence objednatele není omezena v rozsahu výkonu aplikace ani v počtu jejich uživatelů. Ujednání tohoto odstavce neplatí pro standardizovaný software třetích stran, který je běžně dostupný na trhu, tedy který si může koupit neomezený počet osob, a jehož užívání se řídí licenčními podmínkami výrobce.

18) Zhotovitel je povinen nejpozději v okamžiku předání díla (skončení První etapy) objednateli předat zdrojový kód - software. Zdrojový kód musí být spustitelný v prostředí objednatele a zaručovat možnost ověření správnosti a kompletnosti verzí. Musí umožňovat kompilaci, instalaci, spuštění a ověření funkcionality včetně podrobné dokumentace zdrojového kódu. Zdrojový kód bude objednateli předán na nepřepisovatelném technickém nosiči dat viditelně označeném názvem „Zdrojový kód“ a informací, o který software se jedná. O předání technického nosiče dat bude sepsán písemný předávací protokol potvrzený oběma smluvními stranami.

19) Povinnost předání zdrojového kódu se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu, k nimž dojde při plnění této smlouvy nebo v rámci záručních oprav. Dokumentace takových změn zdrojového kódu musí obsahovat podrobný popis každého zásahu do zdrojového kódu.

20) Zhotovitel je povinen předat objednateli dokumentovaný zdrojový kód nebo jeho změnu nejpozději v okamžiku předání díla objednateli, nebo předání plnění dle této smlouvy, jakmile ke změně kódu dojde.

21) Zhotovitel není povinen předávat objednateli zdrojový kód software, který je běžně dostupný na trhu, tedy který si může koupit neomezený počet osob.

22) Zhotovitel je povinen udržovat v aktuálním stavu veškerá přístupová oprávnění potřebná k softwarovým a hardwarovým produktům dodaným na základě této smlouvy (přístupová jména a hesla). To platí i o přístupových oprávněních k registracím licencí a služeb prostřednictvím internetu u jednotlivých výrobců, jsou-li nezbytné pro aktualizace a údržbu daného SW a HW. Na vyžádání je zhotovitel povinen zpřístupnit tato oprávnění objednateli. V případě ukončení smluvního vztahu musí zhotovitel všechna tato oprávnění objednateli předat v aktuálním stavu.

VI.

Oprávněné osoby

1) Oprávněnými osobami při realizaci plnění jsou

- **za objednatele**

a) ve věcech smluvních: viz záhlaví této smlouvy

b) ve věcech realizace díla:

Bc. Daniel Rokos, tel.: [redacted] e-mail [redacted]
Ing. František Bláha, tel. [redacted] e-mail [redacted]
Jan Kropáček, tel. [redacted] e-mail [redacted]
Ing. Milan Dvořák, tel.: [redacted] e-mail [redacted]

c) **ve věcech technických:** Jan Kropáček, tel.: [redacted] e-mail [redacted]

❖ **za zhotovitele**

a) **ve věcech smluvních:** Petr Krutký, tel [redacted] e-mail [redacted]

b) **ve věcech realizace díla:** Ing. Radek Nejedlo, tel [redacted] e-mail: [redacted]

c) **ve věcech technických:** Marek Hercjuk, tel: [redacted] e-mail [redacted]

2) V případě změny kontaktních osob musí být o této skutečnosti druhá smluvní strana neprodleně písemně informována. Za splnění této povinnosti se považuje i e-mail potvrzený druhou smluvní stranou. Účinnost změny nastává okamžikem doručení písemného oznámení příslušné smluvní straně. Změna kontaktní osoby není důvodem k uzavření dodatku.

3) Veškerá korespondence, pokyny, oznámení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém jazyce a doručují se buď osobně, doporučenou poštou nebo prostřednictvím datové schránky, na adresu sídla či ID datové schránky objednatele, uvedené v záhlaví této smlouvy. Smluvní strany se v případě doručování zásilek formou doporučených dopisů dohodly tak, že zásilka je považována za doručenou 3. pracovní den bezprostředně následující po dni jejího odeslání prostřednictvím držitele poštovní licence na adresu příslušné smluvní strany dle záhlaví této smlouvy.

4) Zhotovitel se zavazuje zajistit, že osoby uvedené zhotovitelem v jeho nabídce (v seznamu techniků) dle čl. 7.7 zadávací dokumentace zadávacího řízení, jež předcházelo uzavření této smlouvy, se budou podílet na plnění této smlouvy a budou odpovídat za realizaci díla, a to ve funkcích, v jakých byly v seznamu uvedeny. Výměna takové osoby je možná pouze s písemným souhlasem objednatele a za předpokladu, že nová osoba bude splňovat kvalifikační předpoklady uvedené v zadávací dokumentaci.

5) Změna poddodavatelů oproti obsahu nabídky podané zhotovitelem v zadávacím řízení na uzavření této smlouvy, je možná pouze na základě písemného souhlasu objednatele. Objednatel se zavazuje, že takový souhlas nebude odpírat v případě, že nový poddodavatel bude splňovat veškeré kvalifikační požadavky a odbornost, které splňoval původní poddodavatel a z informací, kterými bude objednatel v dané situaci disponovat, nebude vyplývat obava, že nový poddodavatel by mohl provést jemu svěřenou část díla vadně nebo jiným způsobem narušit realizaci díla dle této Smlouvy. Dodavatel se zavazuje, že části díla uvedené v čl. 6 zadávací dokumentace bude realizovat vlastními kapacitami, nikoli prostřednictvím poddodavatelů.

VII.

Záruky

1) Zhotovitel se zavazuje, že předaný předmět díla bude prostý podstatných vad a bude mít vlastnosti dle obecně závazných právních předpisů, této smlouvy a zadávací dokumentace veřejné zakázky uvedené v preambuli této smlouvy, dále bude mít vlastnosti první jakosti provedení a bude proveden v souladu s ověřenou technickou praxí.

2) Zhotovitel se zavazuje, že **záruční doba činí 60 měsíců**, je poskytována na všechny části díla a **je garantovaná výrobcem**. Na vyžádání objednatele předloží zhotovitel objednateli písemný doklad, který potvrdí, že je záruka skutečně zajištěna v souladu s jeho zadáním a touto smlouvou.

3) Záruční doba začíná běžet dnem protokolárního převzetí díla objednatelem.

4) Zhotovitel odpovídá za vady, které má předmět plnění v době jeho předání objednateli a za vady, které vzniknou nebo se objeví v průběhu záruční doby dle odst. 2) a odst. 3) tohoto článku smlouvy

s výjimkou běžných opotřebení, vad způsobených nesprávnou obsluhou, vad způsobených vyšší mocí nebo třetími osobami a vad spotřebního materiálu.

5) Zhotovitel poskytne objednateli bezplatný záruční servis na dílo v souladu s přílohou č. 1 této smlouvy v režimu on-site (servis u zákazníka) s dostupností 8*5 s reakcí do 4 hodin.

6) Objednatel je oprávněn reklamovat v záruční době dle odst. 2) a odst. 3) tohoto článku smlouvy vady předmětu díla u zhotovitele, a to písemnou formou. V reklamaci musí být popsána vada předmětu díla, určen nárok objednatele z vady předmětu díla, případně požadavek na způsob odstranění vad, a to včetně termínu pro odstranění vad zhotovitelem. Za písemnou formu je považováno také nahlášení standardními prostředky technické podpory provozu, např. e-mailem nebo prostřednictvím HelpDesku/ hot-line.

7) Objednatel má právo volby způsobu odstranění důsledku vadného plnění. V případě vady zboží má objednatel nárok zejména na

   - odstranění vady dodáním nového zboží bez vad, pokud to není vzhledem k povaze vady nepřiměřené. Pokud se vada týká pouze součásti zboží, může objednatel požadovat jen výměnu součásti;
   - odstranění vady opravou, je-li vada opravou odstranitelná;
   - odstranění vady dodáním chybějícího zboží nebo její součásti;
   - přiměřenou slevu z ceny díla;
   - odstoupení od smlouvy (viz čl. X).

8) Zhotovitel se zavazuje od okamžiku oznámení vady předmětu díla či jeho části zahájit odstraňování vady či jeho části, a to i tehdy, neuznává-li zhotovitel odpovědnost za vady či příčiny, které ji vyvolaly, a vady odstranit v technicky co nejkratší lhůtě, a současně zahájit reklamační řízení v místě provádění předmětu díla. O reklamačním řízení budou objednatelem pořizovány písemné zápisy ve dvojím vyhotovení, z nichž jeden stejnopis obdrží každá ze smluvních stran. Bude-li v reklamačním řízení vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno bezúplatně.

9) U reklamovaného zboží, u kterého byla reklamace uznána a které bylo vyměněno za bezvadné či opraveno, běží nová záruční lhůta podle tohoto článku ode dne předání zboží objednateli.

10) Reklamaci uplatní objednatel u zhotovitele nejpozději poslední den záruční doby. I reklamace odeslaná objednatelem poslední den záruční doby se považuje za uplatněnou včas.

11) Uplatnění reklamačních práv objednatelem, jakož i plnění jim odpovídajících povinností zhotovitele, není podmíněno ani jinak spojeno s poskytnutím jakékoli další úplaty zhotoviteli ani jiné osobě.

12) Uplatněním práv z odpovědnosti za vady není dotčeno právo objednateli na náhradu škody.

VIII.

Podpora a údržba díla

1) Podpora a údržba je obsahem druhé etapy díla, její podrobná specifikace je uvedena v článku III této smlouvy.

Podrobná specifikace služeb (SLA)

Technologická podpora	Po-Ne 7:00 – 19:00

Zadávání požadavků HelpDesk/ hot line (e-mail, web)	24 hod. denně
Dostupnost	99,5 %
Odezva od (response time)	Dle detailu priorit v následující tabulce
Řešení do (fix time)	Dle detailu priorit v následující tabulce
Plánovaná údržba	Mimo provozní čas, souvislá délka odstávky max. 4 hodiny – servisní okno

FIX TIME = doba na vyřešení požadavku, incidentu, problému.

2) Objednatel bude své požadavky zadávat prostřednictvím HelpDesku zhotovitele, k němuž zhotovitel poskytne vybraným pracovníkům objednatele přístup, nebo (pokud zhotovitel takovou aplikací nedisponuje nebo v případě jejího výpadku) prostřednictvím kontaktního e-mailu.

3) Způsob poskytování podpory ze strany zhotovitele je následující:

- telefonicky, e-mailem na hot-line lince, osobně v sídle objednatele,
- vzdálená podpora – on line zhotovitelem

4) Kontakt na HelpDesk/ hot-line zhotovitele: e-mail [redacted] telefon [redacted]

Detail/kategorie priorit – řešení jednotlivých požadavků

Priorita	Popis	Odezva od (response time)	Řešení do (fix time)
A – kritická	• systém nefunguje vůbec nebo jeho funkčnost je omezena tak, že tento stav má významný dopad na využívání systému • prvek IT (HW, SW, IS) / služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody • dochází k narušení uživatelských dat závažným způsobem • dochází ke zhroucení systému jednou nebo několikrát za den	1 hod.	4 hod.
B – vysoká	• prvek IT (HW, SW) / služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz	4 hod.	8 hod.

	• funkce systému je narušena tak, že dochází k významnému zpomalení výkonu a využívání systému		
C – střední	• funkce systému je omezena, ale toto omezení má minimální vliv na využívání systému • závada narušuje, avšak neznemožňuje využití systému • blokuje dokončení určitých úkolů, které nejsou časově kritické • působí dílčí závadu nebo nepohodlí uživatele • procesní závada (vyřeší se změnou procesu) • Tuto závadu lze jiným náhradním dočasným způsobem (např. ruční úpravou dat) nebo dočasnou změnou pracovního postupu obejít (workround). Uživatel však musí vykonat vícepráce na obejití závady.	8 hod.	3 prac. dny.
D – nízká	• systém je funkční. Závada způsobuje jen minimální obtíže při jeho používání. Jde o situace, kdy: • vznikne malý problém nebo nepohodlí obsluhy • kosmetická chyba ve vizuálním rozhraní (chybné popisy, řazení dat, překreslování) • uživatel nemusí vykonat vícepráce na obejití závady. Způsobuje mu nepohodlí při práci (např. pohyb myší navíc, klik myší navíc, stisk několika kláves navíc atp.).	24 hod.	20 prac. dnů

5) Požadavky na HelpDesk/ hot-line jsou oprávněny zadávat výhradně osoby uvedené v článku VI. V případě, že komunikaci provádí jiná osoba, vyhrazuje si zhotovitel právo požadavek odmítnout.

6) Objednatel je povinen poskytnout zhotoviteli součinnost při řešení provozního stavu, ke kterému si vyžádal sjednanou službu, včetně zásahu na místě. Je povinen zejména:

- poskytnout zhotoviteli dodatečné informace, které si zhotovitel vyžádá,
- provést na systému akce, které zhotovitel objednateli sdělí a informovat jej neprodleně o jejich výsledku,
- zajistit součinnost pracovníků znalých potřebných hesel a disponujících oprávněními nutnými k provedení zásahu
- umožnit zhotoviteli vzdálený přístup např. přes Internet k podporovaným systémům.

7) Oprávněný zástupce objednatele je povinen podepsat „Pracovní list“ a potvrdit tak rozsah provedených prací pracovníkovi zhotovitele, který zásah prováděl. Tento pracovní list bude přílohou akceptačního protokolu k odměně za příslušný kalendářní měsíc. Má-li pracovník výhrady k jeho obsahu, uvede tyto výhrady písemně v tomto dokumentu.

8) Zhotovitel je povinen řádně a s odbornou péčí poskytovat službu v rozsahu definovaném touto smlouvou a zajistit zástupnost osob při plnění této smlouvy. Zhotovitel však může odmítnout poskytnutí služby, pokud je dílo užíváno v rozporu s touto smlouvou.

9) Zhotovitel je povinen vyvarovat se poškození nebo zničení důležitých dat, která se ve výpočetním systému nacházejí. V případě nebezpečí ztráty dat během zásahu na systému je povinen upozornit objednatele na nutnost tato data před tímto zásahem zálohovat.

IX.

Sankční ujednání

1. Pro případ prodlení zhotovitele s plněním předmětu smlouvy zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,05 % z celkové ceny díla za každý i započatý den prodlení, maximálně však do výše odpovídající ceně za první etapu.
2. Pro případ prodlení zhotovitele s odstraněním vad uvedených v předávacím protokolu dle čl. III odst. 4) písm. j) této smlouvy zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,025 % z celkové ceny díla za každý i započatý den prodlení, maximálně však do výše odpovídající polovině ceny za první etapu.
3. V případě porušení povinnosti zhotovitele uvedené v čl. VI odst. 4) a odst. 5) této smlouvy zaplatí zhotovitel objednateli smluvní pokutu ve výši 15.000,- Kč za každé jednotlivé porušení této povinnosti.
4. Smluvní strany sjednávají pro případ porušení povinnosti o ochraně informací čl. XI. této smlouvy smluvní pokutu ve výši 100.000,- Kč za každý případ.
5. V případě, že objednatel bude v prodlení se zaplacením faktury poskytovateli podle čl. IV., je objednatel povinen zaplatit zhotoviteli zákonný úrok z prodlení z fakturované částky za každý den prodlení dle aktuálně platné legislativy (nařízením vlády č. 351/2013 Sb., ze dne 16. října 2013 či následným předpisem).
6. Za porušení povinnosti uzavřít pojistnou smlouvu (čl. V. – Práva a povinnosti smluvních) zaplatí zhotovitel objednateli smluvní pokutu ve výši 0,05 % z minimální výše limitu pojistného plnění uvedené v článku V., odstavci 4 této smlouvy za každý, byť jen započatý den, v němž bude zhotovitel v prodlení.
7. Nedodržení parametrů pro služby SLA (viz článek VIII. Podpora a údržba díla) opravňuje objednatele k sankcionování zhotovitele podle následujících podmínek:

Priorita	Výše smluvní pokuty	Poznámka
A - kritická	1.500,-	Za každou (i započatou) pracovní hodinu překročení lhůty pro vyřešení.
B - vysoká	1.000,-	Za každou (i započatou) pracovní hodinu překročení lhůty pro vyřešení
C - střední	500,-	Za každý další (i započatý) pracovní den překročení lhůty pro vyřešení
D - nízká	500,-	Za každý další (i započatý) pracovní den překročení lhůty pro vyřešení

Ceny smluvní pokuty jsou uvedeny bez DPH.

8. V případě podstatného porušení smlouvy má objednatel právo od smlouvy odstoupit (viz článek X. Platnost a účinnost smlouvy).
9. Smluvní pokuty lze uložit opakovaně a za každý jednotlivý případ. Zaplacením smluvní pokuty není dotčeno právo smluvní strany na náhradu škody vzniklé porušením smluvní povinnosti, které se smluvní pokuta týká.

10. Smluvní pokuty stanovené dle tohoto článku jsou splatné do třiceti (30) dnů ode dne doručení výzvy k zaplacení smluvní pokuty povinné smluvní straně.

11. Smluvní pokuty dle této smlouvy může objednatel požadovat kumulativně, a to do maximální výše celkové ceny uvedené v článku IV. Smluvní pokutu je objednatel oprávněn započíst oproti splatným pohledávkám zhotovitele.

X.

Platnost a účinnost smlouvy

1) Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti okamžikem jejího uveřejnění v registru smluv. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv, ve znění pozdějších předpisů a s tímto uveřejněním souhlasí. Zaslání smlouvy do registru smluv se objednatel zavazuje zajistit neprodleně po podpisu smlouvy.

2) Platnost této smlouvy může být předčasně ukončena:

   a) písemnou dohodou smluvních stran;

   b) odstoupením objednatele od smlouvy v případě jejího opakovaného (tj. minimálně 2x) porušení ze strany zhotovitele nebo podstatného porušení ze strany zhotovitele;

   c) výpovědí zhotovitele, pokud bude objednatel přes písemné upozornění zhotovitele déle než 60 dnů od písemného upozornění v prodlení s plněním své platební povinnosti vůči zhotoviteli.

3) Za podstatné porušení smlouvy ze strany zhotovitele se považuje zejména prodlení zhotovitele s předáním předmětu plnění První etapy delší než 30 dnů, porušení jakékoliv povinnosti zhotovitele vyplývající ze smlouvy a její nesplnění ani v dodatečné lhůtě (alespoň 5 dnů), kterou objednatel zhotoviteli poskytl (nevylučuje-li to charakter porušené povinnosti). Odstoupení od smlouvy ze strany objednatele není spojeno s uložením jakékoliv sankce k jeho tíži.

4) Výpovědní lhůta činí jeden měsíc a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém byla písemná výpověď doručena druhé smluvní straně.

5) Odstoupení od smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně na adresu jejího sídla uvedené v záhlaví této smlouvy. Smluvní strany se dohodly, že odstoupení od smlouvy se považuje za doručené 10. dnem od jejího uložení u provozovatele poštovních služeb, resp. výslovným odmítnutím přijetí odstoupení druhou stranou.

6) Dojde-li k předčasnému ukončení smlouvy, je zhotovitel oprávněn požadovat pouze uhrazení částky za řádně ukončenou a objednatelem akceptovanou etapu plnění.

7) Odstoupením od této smlouvy zanikají všechny závazky smluvních stran z této smlouvy. V případě odstoupení od této smlouvy nezanikají nároky smluvních stran na náhradu škody a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklé před skončením účinnosti této smlouvy, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví ObčZ.

XI.

Ochrana informací

1) Zhotovitel se zavazuje, že zachová jako citlivé informace zprávy týkající se vnitřních záležitostí smluvních stran a předmětu plnění smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou

stranu. Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.

2) Smluvní strany budou považovat za citlivé informace:

   a) informace jako citlivé označené,

   b) informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o objednateli, které by mohly z povahy věci být považovány za citlivé a které se dozvědí v souvislosti s plněním této smlouvy.

3) Smluvní strany se zavazují, že neuvolní třetí osobě informace druhé strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. Závazek mlčenlivosti a ochrany citlivých informací zůstává v platnosti po dobu 5 let po ukončení platnosti smlouvy.

4) Zhotovitel je povinen zabezpečit veškeré podklady mající charakter citlivé informace poskytnuté mu objednatelem proti odcizení nebo jinému zneužití.

5) Zhotovitel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv objednatele nejméně ve stejném rozsahu, v jakém je v závazkovém vztahu zavázán sám.

6) V souvislosti s důvěrností informací bere zhotovitel na vědomí, že je zákonnou povinností objednatele uveřejnit celé znění této smlouvy včetně všech jejich případných dodatků a seznamu subdodavatelů v souladu se zákonem. Splnění této, jakož i dalších zákonných povinností objednatele, není porušením důvěrnosti informací.

7) Povinnost zachovávat mlčenlivost se nevztahuje na informace:

   a) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto odst. ze strany zhotovitele,

   b) které jsou zhotoviteli známy a byly mu volně k dispozici ještě před přijetím těchto informací od objednatele,

   c) které budou následně zhotoviteli sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána,

   d) jejichž sdělení se vyžaduje ze zákona.

8) Za prokázané porušení ustanovení v tomto čl. má druhá smluvní strana právo požadovat náhradu takto vzniklé škody.

XII.

Závěrečná ustanovení

1) Vztahy mezi smluvními stranami se řídí českým právním řádem. Ve věcech smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními ObčZ a ostatními obecně závaznými právními předpisy. Rozhodčí řízení je vyloučeno. Smluvní strany sjednávají ve smyslu příslušných ustanovení občanského soudního řádu pro spory vyplývající z této smlouvy či s touto smlouvou související místní příslušnost Obvodního soudu pro Prahu 5, případně Městského soudu v Praze.

2) Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu písemně oznámit druhé smluvní straně a vyvolat jednání objednatele a zhotovitele.

3) Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují, že bezodkladně nahradí neplatné ustanovení této smlouvy jiným platným ustanovením svým obsahem podobným neplatnému ustanovení.
4) Smlouva se vyhotovuje ve 4 stejnopisech, z nichž každý má platnost originálu, přičemž Objednateli přináleží tři stejnopisy a zhotoviteli 1 stejnopis.
5) Nedílnou součástí této smlouvy jsou následující přílohy:
   a) Příloha č. 1 – Technická specifikace předmětu zakázky (příloha č. 6 zadávací dokumentace)
   b) Příloha č. 2 – Podrobný položkový rozpočet
   c) Příloha č. 3 – Závazný harmonogram plnění

Za Objednatele:	Za Zhotovitele:
	Petr Krutký Digitally signed by Petr Krutký DN: c=CZ, 2.5.4.97=NTRCZ-60193336, o=O2 Czech Republic a.s. [IČ 60193336], ou=45814, cn=Petr Krutký, sn=Krutký, givenName=Petr, serialNumber=P357737 Date: 2019.10.22 20:07:20 +02'00'
……	……
Martin Herman	Petr Krutký
radní pro oblast investic a veřejných zakázek	Account Manager

Technická specifikace předmětu zakázky

Obsah

Předmětem veřejné zakázky je zajištění komplexního monitoringu ICT prostředků, kontrola činností všech registrovaných uživatelů na všech úrovních zpracování dat, sledování datového provozu informační infrastruktury, registrování útoků na prostředky ICT a průběžné odhalování případných interních a externích útočníků na ICT Krajského úřadu Středočeského kraje (dále také „KÚSK“). Za tím účelem budou v rámci veřejné zakázky pořízeny a v prostředí KÚSK implementovány odpovídající technologie a zajištěny vybrané služby externího dodavatele, a to v souladu se zákonem o kybernetické bezpečnosti a nařízením EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Řešení veřejné zakázky je koncipováno tak, aby naplnilo následující technická opatření dle zákona o kybernetické bezpečnosti:

- § 17 Fyzická bezpečnost
- § 18 Bezpečnost komunikačních sítí
- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
- § 23 Detekce kybernetických bezpečnostních událostí
- § 24 Sběr a vyhodnocení kybernetických bezpečnostních událostí
- § 27 Zajišťování úrovně dostupnosti informací
- Sdílené dohledové centrum kybernetické bezpečnosti (SOC)

Dodavatelé, kteří se budou podílet na rozvoji, provozu nebo zajištění bezpečnosti významných informačních systémů, musí dle § 8 Vyhlášky 82/2018 Sb., vyhláška o kybernetické bezpečnosti, splňovat bezpečnostní požadavky pro dodavatele.

Záměrem zadavatele je nakoupit dodávky a služby zařazené do 5 celků:

1. **Systém pro pokročilý provozní dohled** – Jedná se o komplexní řešení pokročilého provozního dohledu informačních technologií KÚSK tak, aby plně navazoval na stávající řešení, kdy je využíváno ASW Nagios. Součástí dodávky je návrh architektury řešení, upgrade software na nejnovější verzi a provedení jeho konfigurace podle návrhu. Dále je součástí servisní podpora zadavatele při provozu systému včetně zajištění podpory výrobce po dobu 60 měsíců.
2. **Systém podpory pokročilé segmentace sítě** – Jedná se o komplexní řešení systému podpory a řízení pokročilé segmentace síťové infrastruktury KÚSK takovým způsobem, aby navazovalo na současně využívanou technologii infrastruktury. Součástí dodávky je návrh architektury řešení včetně potřebného HW a potřebného SW a implementace tohoto řešení včetně požadované integrace do prostředí Zadavatele. Dále je součástí servisní podpora zadavatele při provozu systému včetně zajištění podpory výrobce po dobu 60 měsíců.
3. **Zvýšení fyzického zabezpečení HTCK** - Jedná se o dodávku a instalaci klimatizační jednotky a dodávku a instalaci zhášecího zařízení na bázi plynů inergenů. Dále je součástí dodávky zajištění pravidelného servisu zařízení včetně zajištění podpory výrobce po dobu 60 měsíců.
4. **Sdílené služby kybernetické bezpečnosti** – Jedná se o komplexní dodávku dílčích služeb po dobu 60 měsíců:
   4.1. *Zaznamenávání a ukládání logů a detekce bezpečnostních událostí* – Dodavatel s využitím vlastních technologií zajistí sběr, ukládání, analýzu a bezpečné dlouhodobé uchování logů z vybraných systémů IT zadavatele. Současné dodavatel zajistí detekci bezpečnostních událostí v sledovaných systémech IT dodavatele a informování o nich.
   4.2. *Analýza datových toků a detekce bezpečnostních událostí* – Dodavatel s využitím vlastních technologií zajistí sledování datových toků na výskyt anomálií a podezřelých aktivit a měření výkonových parametrů datových přenosů v síti IT zadavatele. Současně dodavatel zajistí záznam a uložení informací o sledovaných datových tocích, detekovaných událostech a stavech a o výsledcích měření sledovaných veličin.
   4.3. *Dohledové centrum – SOC* – Dodavatel s využitím vlastních zdrojů zajistí provoz Bezpečnostního dohledového centra, které pro zadavatele bude provádět bezpečnostní dohled nad sledovanými systémy IT, identifikaci, hodnocení a řešení bezpečnostních incidentů včetně poskytnutí včasných informací odpovědným pracovníkům zadavatele, pravidelné reportování stavu kybernetické bezpečnosti sledovaných systémů IT a poskytování podpory v oblasti kybernetické bezpečnosti.
5. **Služby poradenství a podpory** – Jedná se o komplexní dodávku dílčích služeb, které směřují ke koordinaci a kvalitnímu provedení dodávky ostatních služeb:
   5.1. *Předimplementační analýza* – Dodavatel zpracuje analýzu prostředí IT kraje, ve které popíše a vyhodnotí stav z hlediska zajištění kybernetické bezpečnosti podle §17, §18, §22, §23, §24 a §27 vyhlášky o kybernetické bezpečnosti, identifikuje bezpečnostní rizika a slabá místa a navrhne opatření k odstranění neshod.
   5.2. *Prováděcí dokumentace* – Dodavatel zpracuje prováděcí dokumentaci s detailním návrhem cílového stavu, s popisem aktivit potřebných pro řádnou implementaci jednotlivých služeb včetně implementace opatření navržených v předimplementační analýze a s návrhem harmonogramu implementačních prací. Součástí dokumentace bude také popis potřebných integrací do prostředí IT kraje.
   5.3. *Projektové vedení dodávky* – Dodavatel zajistí řízení, koordinaci a dokumentaci postupu dodávky včetně řízení rizik a změn dodávky a poskytování pravidelných zpráv o průběhu dodávky.

5.4. *Dokumentace skutečného provedení* – Dodavatel v průběhu celé dodávky zajistí zpracování dokumentace dodaných řešení v požadovaném rozsahu.

6. **Výkony nad rámec podpory dle čl. III odst. 5.3 Smlouvy o dílo**

1. Systém pro pokročilý provozní dohled

Realizace tohoto opatření naplní § 27 Zajišťování úrovně dostupnosti informací Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v *platném znění.*

Jedná se o komplexní řešení pokročilého provozního dohledu informačních technologií KÚSK tak, aby plně navazoval na stávající řešení, kdy je využíváno ASW Nagios. Je požadováno provést upgrade na nejnovější verzi Nagios s GUI s licencí minimálně pro 1000 hostů. V současné době je využíván Nagios 3.3 s předplacenou roční podporou. Upgrade ASW Nagios na nejnovější verzi vytvoří robustní dohledové centrum, které má zajistit nepřetržité proaktivní monitorování činností a správu všech aktivních prvků instalovaných informačních technologií na KÚSK. Je nutné zajistit zasílání automatické zprávy správcům sítě při výpadku jakéhokoliv aktivního prvku nebo dle definovaného scénáře spustit automatickou akci k obnovení provozu aktivního prvku. Systém musí umožňovat rozšíření pomocí definic uživatelských funkcí (pluginů) a být schopen pokrýt monitoring velkého množství různorodých prvků informačních technologií. Systém uchovává historii záznamů z provozu prvků, podává informace o aktuálním stavu a dostupnosti aplikací a jednotlivých prvků provozované infrastruktury. Systém bude sloužit jako centrální zdroj informací pro efektivní řízení infrastruktury KÚSK. Systém bude nakonfigurován pro poskytování automatizovaných výstupů službě SOC, na kterou bude napojen.

Požadovaný účel implementace systému:

Povýšit funkčnost služby provozního dohledu infrastruktury KÚSK s možností detekce na úrovni jednotlivých služeb nebo informačních systémů včetně vzájemných závislostí a podporou reportování (SLA).

Základní požadavky implementace systému:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
Část	**Popis**			
Upgrade stávajícího řešení, administrace				
Rozsah	▪ Řešení umožňuje připojit infrastrukturu KÚSK.			public
Upgrade Nagios 3.3	▪ Provést upgrade na nejvyšší možnou verzi stávající a stabilní verzi s GUI (komerční provedení). ▪ Provést upgrade grafického rozhraní systému Nagios. ▪ Vytvořit řešení on−premise.			public

Administrace a uživatelský přístup	▪ Realizovat výhradně přes jednotné GUI a to formou webové aplikace s podporou prohlížečů Internet Explorer verze 11 a Mozilla Firefox v. 45 příp. dalších vyšších verzí.			public
Mobilita administrace	▪ Podporovat možnosti využití verzi aplikace pro mobilní zařízení na platformách Google Android a Apple iOS v libovolném počtu.			public
Integrita	▪ Systém obsahuje všechny požadované funkcionality, není možné jej sestavit z vícero různých komponent od různých výrobců software.			public
Virtualizace	▪ Řešení se požaduje jako samostatný virtuální stroj do infrastruktury VMware (virtuální server bude zajištěn zadavatelem).			public
Podpora monitoringu				
Nativní podpora	▪ Podpora nativního monitoringu standardních technologií – Microsoft Windows, SQL Server, VMware, Linux, grafické platformy (např. Integraph technologie), FalconStor, MS Exchange, SW Symantec, Networker atd.			public
Autodiscovery	▪ Přidávat další monitorované systémy a služby s rozeznáním vyjmenovaných aktivních síťových služeb.			public
	▪ Vytvářet vlastní scripty nebo pluginy pro jednotlivé prováděné kontroly.			public
Šablony v GUI	▪ Možnost vytváření vlastních šablon zařízení, tak aby pokud je takováto šablona přiřazena ke všem vhodným prvkům v infrastruktuře, byly služby definované v této šabloně sledovány dle parametrů zadaných přímo v šabloně. Pokud je následně v šabloně provedena jakákoli změna služeb, musí se toto projevit i na prvcích, které tuto šablonu využívají bez dalších nutných kroků			public

	administrátorů. Šablony lze vytvářet nebo upravovat výhradně přes GUI.			
Monitoring služeb	▪ Návrh řešení obsahuje možnosti monitoringu služeb, které zajišťuje Odbor informatiky (OINF). Každá služba, např. email je složena z jednotlivých komponent, např. SMTP gateway, Internetová konektivita apod. Každá z těchto sub−komponent obsahuje další podřízené sub−komponenty, např. zatížení CPU, využití disku, apod. Systém umožňuje nastavení takových vazeb mezi komponentami a sub−komponentami služby, aby v případě degradace komponenty v nejnižší hierarchii byl tento stav promítnut do celé struktury služeb až po službu samotnou. Zároveň v tomto případě musí být jasně definováno, které jednotlivé části jsou tímto ovlivňovány.			public
Reporting				
Reporting SLA	▪ Řešení nabízí možnosti reportingu SLA u jednotlivých služeb poskytovaných IT, a to na základě parametrů nastavovaných pověřeným uživatelem.			public
	▪ Sledované komponenty je možné nastavit do režimu plánovaného výpadku, kdy nedochází k notifikacím a ke změně daného SLA.			public
Časové sledování služeb	▪ U jednotlivých sledovaných služeb musí být k dispozici adekvátní graf parametru služby ve zvoleném časovém úseku.			public
Topologické mapy	▪ Řešení musí obsahovat možnost vytváření interaktivních topologických map, např. mapu síťové konektivity v místě, přičemž při kliknutí na jakýkoliv interaktivní prvek uživatel			public

	uvidí detail tohoto prvku v samotném systému řešení. ▪ Zobrazení či pohled, kde se graficky znázorňuje celková mapa implementované sítě, jsou označeny spoje mezi jednotlivými body infrastruktury.			
Zobrazení	▪ Poskytovat přehled všech monitorovaných služeb, kde jejich aktuální stav je barevně odlišen; ▪ Poskytovat přehled všech monitorovaných zařízení, kde jejich aktuální stav je barevně odlišen; ▪ Poskytovat souhrnný výpis všech monitorovaných zařízení, rozdělený do jednotlivých skupin; ▪ Poskytovat souhrnný výpis všech monitorovaných služeb, rozdělený do jednotlivých skupin.			public
Dashboard, přehledy	▪ Vytvořit/revidovat základní přehled stavů (dashboard) všech monitorovaných služeb a zařízení.			public
Reporty, výčet, příklady	▪ Vytvářet reporty vybraného zařízení nebo služby a jejich problémových stavů; ▪ Vytvářet grafické reporty o stavu zařízení nebo služby v čase, kde lze stanovit časový interval; ▪ Generovat souhrnné reporty o stavu sledovaných služeb a zařízení za zvolený časový interval ▪ Zpracovávat výpis logu se zaznamenanými událostmi; ▪ Vytvářet report o dostupnosti a vyhodnocení stavu služeb a zařízeních v časovém období			public
GUI, nastavení				
Konfigurace	▪ V rámci GUI umožňovat uživatelsky měnit rozložení pracovní plochy a konfiguraci jednotlivých prvků GUI, které se týkají výstupů z monitoringu.			public

Notifikace	▪ Systém disponuje možnostmi notifikace pomocí emailů nebo SMS při určitých stavech zjištění. Samotné notifikační šablony musí být editovány prostřednictvím jednotného GUI včetně možnosti rozesílání kontaktním skupinám.			public
	▪ Součástí nabízeného řešení je možnost řízení uživatelského a administrátorského přístupu k řešení prostřednictvím LDAP/AD/IDM.			public
Autentizace	▪ Řízení autentizace bude dodán jako samostatný virtuální stroj do infrastruktury VMware. Dodávka obsahuje vlastní operační systém. Systém zajistí možnosti automatické i manuální aktualizace samotného operačního systému, tak i vlastní aplikace výhradně přes jednotné GUI.			public
Implementace monitoringu				
Dohledování HW	▪ Na HW zařízeních budou dohledovány relevantní parametry, příklady: o Síťové prvky. o Utilizace CPU. o Utilizace paměti RAM. o Teplota. o Utilizace šířky pásma rozhraní, interní. o Případně další dle typu. ▪ Servery o Utilizace RAM. o Utilizace CPU. o Utilizace síťových rozhraní. o Utilizace disků. o Služby/procesy. o Případně další dle typu.			public
Dohledování SW	▪ Pro jednotlivé monitorované SW budou definovány dle jeho účelu užití sledované parametry, které budou nakonfigurovány do řešení.			public
	▪ Definovat a rozdělit zařízení a služby do skupin tykajících			public

	se příslušných primárních aktiv; V případě aktiva, které disponuje rozdělením na produkční, testovací a případně vývojové prostředí je nutné provést seskupení dle těchto prostředí.			
	▪ Sledovat aktuální síťové stavy prostřednictvím webového rozhraní, zobrazení historií událostí, logovacích souborů atd.			public
	▪ Pro každé primární aktivum definovat relevantní služby, které budou monitorovány. Pro každou službu definovat alespoň stavy OK, Warning (HARD, SOFT) a Critical (HARD, SOFT) včetně definovaných prahových hodnot s provedením následné konfigurace.			public
	▪ Zařízení primárních aktiv budou monitorována. Pro doporučené parametry zařízení definovány stavy OK, Warning (HARD, SOFT) a Critical (HARD, SOFT) včetně definovaných prahových hodnot s provedením následné konfigurace.			public
	▪ Dále budou definovány vazby mezi jednotlivými službami (service dependency) a zařízeními (host dependency) v rámci primárního aktiva. Poté budou definovány vazby mezi jednotlivými primárními aktivy. Veškeré diagramy budou součástí dokumentace pro každé aktivum a napříč aktivy. Diagramy budou odevzdány v editovatelné podobě specifikované zadavatelem. Veškeré vazby budou nakonfigurovány.			public
	▪ Provádět monitorování síťových služeb všech systémů vystavených na internet a interních systémů/služeb, které jsou			public

	klasifikovány z míry dostupnosti vysoká a vyšší.			
	▪ Provádět monitorování hostitelských zdrojů (vytíženost procesoru, využití disku a pamětí, běžící procesy, logovací soubory atd.).			public
	▪ Disponovat schopností definovat síťovou hostitelskou hierarchii, umožňující zjištění rozdílu mezi zařízením (službou), které je vypnuté a které nedostupné.			public
	▪ Připravit vnější příkazové rozhraní, které dovoluje za provozu modifikovat monitorování a chování celého systému.			public
	▪ Uchovávat stav zařízení a služeb i po restartu Nagiosu.			public
	▪ Připravit prostředí pro potvrzení problémů přes webové rozhraní.			public
	▪ Pro specifikované události disponovat schopností definované akce na událost (např. při nedostupnosti restartuj službu apod.).			public
	▪ Provést implementaci vlastnosti Predictive Checks.			public

Obecné informace:

Zadavatel v rámci upgrade systému verze Nagios 3.3 na vyšší verzi nepožaduje přenesení naimplementovaných funkcionalit v rámci stávajícího systému na nový. V rámci dodávky bude zajištěno úvodní a průběžné školení administrátorů v rozsahu 20 MD.

Dílčí cíle implementace systému:

- Navrhnout řešení dle požadavků výše.
- Navrhnout a popsat architekturu včetně potřebného HW a potřebného SW včetně požadované integrace do prostředí Zadavatele.
- Naplnění požadavků pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
- Implementovat řešení podle návrhu schváleného Zadavatelem
- Servisní podpora v režimu 12/5/365 tj. v pracovní dny od 7-19 hodin s reakcí do 4 hodin.

Podpora výrobce:

Zadavatel požaduje zajištění upgrade a update dodaného SW po dobu 60 měsíců. Dodavatel se zavazuje, že součástí dodávky bude služba upgrade a update poskytována výrobcem Nagios na 36 měsíců, a že v průběhu plnění 5leté podpory tento dokoupí tuto službu ke své tíži na dalších 24 měsíců, jakmile to bude možné a to tak, aby byla zajištěna kontinuální podpora výrobce Nagios po dobu 60 měsíců. Dodavatel zajistí upgrade a update vždy při vydání nové verze (tzv. main release) a zajistí její implementaci do testovacího a produkčního prostředí. Testovací prostředí bude vytvořeno dodavatelem z důvodu možnosti testování před nasazením do produkčního provozu. Zadavatel si vyhrazuje právo schválit či odmítnout plánovaný upgrade.

2. Systém podpory pokročilé segmentace sítě

Realizace tohoto opatření naplní § 18 Bezpečnost komunikačních sítí Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v *platném znění.*

Jedná se o komplexní řešení systému podpory pokročilé segmentace síťové infrastruktury KÚSK takovým způsobem, aby navazovalo na současně využívanou technologii infrastruktury. Navržené řešení bude obsahovat reportovací nástroj, který bude poskytovat základní provozní informace o infrastrukturních prvcích (dodávaných firewallech, WiFi access pointech a switchích). Reportovací nástroj bude obsahovat veškeré informace o nestandardních stavech a detekovaných hrozbách v infrastruktuře, které bude zasílat automaticky oprávněným uživatelům dle pozic definovaných bezpečnostní politikou informačních technologií KÚSK.

Požadovaný účel implementace systému:

Povýšit stávající systém kontroly propojení segmentu tak, aby umožňoval pokročilou kontrolu propojení mezi jednotlivými segmenty sítě prostředí KÚSK až na aplikační úrovni. Zajistit vysoký výkon řešení firewallů s cílem využití jako tzv. interní segmentační firewally a to na 10 Gbps síti s požadavkem zajištění alespoň L2/L3 stavového firewallu v plné propustnosti sítě. Zajistit vysoký výkon v IPSEC VPN s cílem přípravy na budoucí zvyšování požadavků na šifrování provozu na vysokorychlostních sítích pro připojení podřízených organizací a složek i pro vybrané interní toky.

Základní požadavky implementace systému:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
Část	**Popis**			
Obecné				
Řešení	▪ On−premise.			public
Správa – obecné požadavky na nabízené systémy	▪ Syslog. ▪ CLI (Command Line Interface) konzole. ▪ SSHv2 konzole. ▪ SMNPv3 a vyšší. ▪ Podpora protokolu RADIUS. ▪ RBAC (Role Based Access Control). ▪ Synchronizace času prostřednictvím NTP.			public
Komponenty				
Firewally	▪ Počet komponent: 2			NDA

	▪ Hardware appliance o velikosti 1RU instalovatelné do racku 19“ s podporou duálního napájení ▪ Min 8 x 10/100/1000 Mbps 2x SFP+ 10Gb, 8x SFP 1Gb. ▪ Konzolový port RS232, management port RJ 45 ▪ Podpora IPv4 a IPv6. ▪ Minimální propustnost firewallu pro IPv4 i IPv6 provoz je 30 Gbps (měřeno na UDP komunikaci). Při měření na provozu tvořeným mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 20 Gbps ▪ Propustnost funkce IPS min. 5 Gbps (měřeno na tzv. enterprise mix provozu) ▪ Propustnost funkce SSL inspekce alespoň 5 Gbps (měřeno na tzv. enterprise mix provozu). ▪ Propustnost při zapnutí všech bezpečnostních funkcí ochrany před hrozbami (IPS, L7 analýza aplikací, ochrana proti malware) min 3,8 Gbps (měřeno na tzv. enterprise mix provozu). ▪ Latence firewallu < 4 µs. ▪ Počet souběžných spojení alespoň 5mil. ▪ Počet nových spojení alespoň 200 tis/s. ▪ SSL−VPN souběžných spojení alespoň 500. ▪ Podpora pro L2TP over IPSEC, IPSEC VPN. ▪ Propustnost IPSEC VPN alespoň 10 Gbps (při použití AES256-SHA256). ▪ Podpora NAT/PAT. ▪ Podpora HA řešení (active−active, active−passive). ▪ Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu			

	▪ Podpora bezpečnostní funkce ochrany před škodlivým kódem podle databáze vzorků škodlivého kódu pravidelně aktualizované výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora sandboxovací funkce (dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) s integrací s nabízeným řešením pro část „Ochrana neznámých hrozeb“ ▪ Podpora bezpečnostních funkcí: ochrana proti spamu, IPS/IDS, kategorizace webových stránek, IP reputační database, DNS filtering, ochrana před únikem citlivých informací data leak prevention). ▪ Podpora bezpečnostní funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 2000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace ▪ Podpora bezpečnostní funkce pro ochranu práce s populárními cloudovými aplikacemi pro sdílení a ukládání souborů na principu sledování aktivit aktivních uživatelů přes API daného provozovatele včetně funkcí monitoringu, detekce			

	compliance pravidel a bezpečnostních kontrol (DLP, antivirus včetně sandboxingu) s ohledem na minimalizaci šíření sítových hrozeb; minimálně podpora pro Google, Amazon, Microsoft Azure, Dropbox ▪ Podpora funkce SSL inspekce pro webové a poštovní protokoly s možností whitelistingu určitých domén či kategorií webových stránek ▪ Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety) s možností aplikace do bezpečnostní politiky ▪ Funkce QoS, traffic shaping ▪ Ověřování identity uživatelů (možnost napojení na MS Active Directory), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On ▪ Funkce klientská VPN (přístup do vpn v tunelovém režimu s vpn klientem a přístup do vpn přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů) ▪ Funkce site-to-site ipsec VPN s podporou statického i dynamického routování ▪ Podpora dvoufaktorové autentizace za pomoci HW tokenů i aplikace pro mobilní telefony (minimálně Android, iOS) s podporou autentizace administrátorů při přístupu k firewalu a pro 2FA autentizaci uživatelů do VPN. Funkce může být integrována do firewallu, nebo dodána jako samostatné řešení. Součástí dodávky budou 4ks HW tokenů pro přístup administrátorů. Řešení bude podporovat budoucí možné rozšíření na VPN uživatele (tj.			

	podpora pro nejméně 500 tokenů) ▪ Podpora 802.3ad ▪ Certifikace výrobce ICSA Labs minimálně pro IPSec VPN a Network Firewall, Advanced Threat Defense (ATD), Anti−virus, SSL−TLS, IPS. ▪ Umístění výrobce zařízení v NSS LABS NEXT GENERATION FIREWALL testu v roce 2017 nebo 2018 nadprůměrně v obou posuzovaných parametrech ▪ Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů. ▪ 1x Reportovací nástroj stejného výrobce jako FW – přípustná je 1ks fyzická appliance, 1 ks virtuální appliance s podporou Vmware. Minimální velikost úložiště 4 TB, min příjem 100 GB logů denně			
	▪ Dodavatel zajistí implementaci a konfiguraci nových FW tak, aby bylo možné aktuální zařízení odpojit, popř. využít k jinému účelu. V současné době je využíváno cca 500 aktivních pravidel na stávajících technologiích FortiGate a Check Point.			NDA
Ochrana neznámých hrozeb	▪ Počet komponent: 1 ▪ 4x 1 GE SFP, 4 x RJ45 10/100/1000Mbps. ▪ Úložiště 2 x 1 TB ▪ 2 x redundantní zdroj napájení ▪ Hardware appliance instalovatelná do racku 19“ maximálně 1RU ▪ Alespoň 5000 souborů za hodinu prověřených antivirem. ▪ Alespoň 150 souborů za hodinu prověřených VM sandboxingem. ▪ Technologie VM OS Sandbox nebo obdobná včetně podpory			NDA

	souběžných instancí OS MS Windows 7, 8 a vyšší. ▪ Minimální počet současně běžících VM 10 ▪ Možnost vytvořit simulovanou síť pro oddělené scanování souborů ▪ Podpora typ souborů: .7z, .ace, .apk, .arj, .bz2, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .izh, .msi, .pdf .ppsx, .ppt, .pptm, .pptx, .rar, .rtf, .tar, .tgz, .xls, .xlsb, .xlsm, .xlsx, .zip a dalších. ▪ Podpora statického směrování. ▪ Podpora HA clusteru. ▪ Možnost instalace v režimu neviditelného snífování a integrace s dodávaným firewallem. ▪ Hloubková inspekce alespoň protokolů SMTP, POP3, IMAP, HTTP, FTP, SMB ▪ Možnost SSL/TLS inspekce. ▪ Možnost white/black listingu pro kontrolní součet souboru ▪ Anti−evasion technik: alespoň sleep calls. ▪ Detekce botnetů, rootkitů atd. ▪ Dashboard s aktuálními informacemi.			
Směrovače	▪ Počet komponent: 2. ▪ Hardware appliance instalovatelné do racku 19“ max 1RU ▪ Propojení High−availability. ▪ 2 x SFP+ 10Gbe port, 24 x RJ45 10/100/1000Mbps. ▪ L2 a L3 směrovací výkon alespoň 1Gbps. ▪ IEEE 802.1Q VLAN encapsulation. ▪ Link Aggregation Control Protocol (LACP): IEEE 802.3ad. ▪ Jumbo frames na všech portech. ▪ Podpora IPv4 a IPv6. ▪ Podpora Multicast. ▪ Směrovací protokoly: Statické, Routing Information Protocol			public

	Version 2 (RIPv2), Open Shortest Path First Version 2 (OSPFv2), Border Gateway Protocol (BGP). ▪ IPv6 routing protocols: Static, OSPFv3, BGPv6. ▪ Policy−Based Routing (IPv4 and IPv6). ▪ ACL L4 včetně. ▪ Podpora MVRP dle standardu 802.1ak pro distribuci VLAN ▪ STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) ▪ Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 ▪ Podpora technologie MACsec ▪ Podpora RADIUS včetně RADIUS CoA (RFC3576) ▪ Podpora REST API pro automatizaci nastavení sítě. ▪ Podpora Zero Touch Provisioning (ZTP) ▪ Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway) ▪ Automatická konfigurace portu podle připojeného zařízení (automatické nastavení tagged a untagged VLAN, QoS a ACL) ▪ Podpora IP SLA pro měření zpoždění provozu VoIP			
Segmentace WIFI sítě pro všechny uživatele KÚSK	▪ Pokrytí všech prostor budovy KÚSK pro využití HW prostředků s Wifi připojením pro pracovníky KÚSK, zastupitelstvo, klienty úřadu v oblasti využití vazby na registrované VISy KÚSK. ▪ WiFi síť s duální frekvencí 2,4 a 5 GHz s podporou WiFi 6 (standardy 802.11n/ax), řízená controlery v HA (High Availability – režim vysoké dostupnosti). ▪ Technická specifikace bude vypracována na základě proměření budovy na prostupnost signálu v součinnosti se zadavatelem.			public

	▪ Dodávku řešení a pro implementace zabezpečení sítě dle standardu 802.1x, včetně řešení pro inteligentní správu zařízení, které standard 802.1x nepodporují (tiskárny, IP kamery apod.) + BYOD (Bring Your Own Device − ověřování zařízení, které nejsou v doméně, např. telefony, tablety včetně licence na min. 500 zařízení. Přípustné je řešení formou 2ks HW appliance v HA režimu nebo 1ks virtuální appliance s podporou Vmware. Implementace řešení musí zahrnovat kompletní implementaci ověřování 802.1x pro bezdrátovou síť mimo konfigurace klientů a přípravu řešení pro drátovou síť včetně odpovídající konfigurace dodávaných switchů. ▪ 121 x Access Point s minimálními parametry: o Určený pro instalaci na strop/podhled o Integrované všesměrové antény (v horizontální rovině) pro obě pásma o Dvě samostatná rádia pro paralelní provoz ve 2,4GHz a 5GHz pásmech o Konfigurace rádií: 4x4:4 pro 5GHz a 2x2:2 pro 2,4GHz o Přenosové rychlosti: až 4,8Gbps pro 5GHz a 575Mbps pro 2,4GHz o Podpora standardů 802.11a/b/g/n, 802.11ac wave 2 a 802.11ax o Certifikace Wi-Fi Aliance: Wifi Enhanced Open o Certifikace Wi-Fi Alliance: WiFi WPA3 Enterprise (včetně CNSA, SAE, OWE) o Záruka výrobce za dodatečnou certifikaci Wi-Fi Alliance: WiFi 6 (včetně případné výměny			

	necertifikovaných zařízení) o Minimální počet inzerovaných SSID (BSSID) per radio: 16 o Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu - Transmit Beam Forming (TxBF) o Podpora víceuživatelského vícenásobného vstup a výstupu (MU-MIMO) o Automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu, zhodnocení dostupných AP z pohledu klienta o Podpora přenosu řídících i uživatelských dat skrze controller v tzv. tunelovém režimu o Podpora operačního režimu AP umožňujícího formování clusteru AP, který se následně chová jako kontrolér – tedy synchronizuje konfiguraci AP a zajišťuje centrální funkce (např. automatické plánování kanálů, aktivní roaming, band steering atp.) AP musí být schopna formovat clustery nejméně o velikosti 100AP. o Hardwarová podpora šifrovaní řídících i uživatelských dat přenášených mezi AP a controllerem o AP uzavřené konstrukce, bez větracích otvorů a ventilátoru o Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 a IPv6 pomocí Telnet a SSH			

	○ Napájení AP pomocí 802.3at/af PoE ○ USB 2.0 port využitelný pro záložní LTE uplink zapojením LTE modemu ○ 2,5Gbps ethernet rozhraní dle standardu 802.3bz a NBase-T ○ Bluetooth rozhraní pro navigační a management účely ○ Podpora spektrální analýzy pro monitoring non-WIFI rušení ○ Podpora ověření AP do sítě pomocí 802.1x suplikanta ▪ 2 x WiFi controllery zapojené do HA clusteru s minimálními parametry: ○ Dedikované HW appliance s 2x SFP+ 10 Gbe porty ○ Je vyžadováno, aby HW appliance byly vybaveny specializovanými CPU či ASIC pro odbavování a zpracování síťového provozu, nikoliv generickými x86 procesory. ○ Podpora pro 802.11u, 802.11v, 802.11k a 802.11w ○ Podpora XML a REST API pro automatizovanou konfiguraci kontroléru ○ Klasifikace klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu ○ Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) ○ Podpora OSPF ○ Podpora rozpoznavani aplikací na 7. vrstvě (aplikace typu: Youtube,			

	Facebook, Dropbox, BitTorrent, Skype, Office365, apod.). Možnost jejich povolování, zakazování, prioritizace nebo omezování s možnosti vytvořit minimálně 20 souběžných aplikačních pravidel k ošetření provozu konkrétních aplikací. ○ Podpora Bonjour services gateway, zpracování mDNS paketů, možnost filtrování služeb mezi subnety ○ Podpora WIPS pro detekci a zamezení útoků na bezdrátovou síť ○ Podpora monitoringu IP telefonních a UCC komunikačních spojení – přehled o proběhlých hovorech a zhodnocení z hlediska jejich kvality a SLA ○ Automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI a jejich SLA monitoring ○ Podpora protokolů RADIUS a TACACS+ pro ověřování administrátorů a uživatelů do sítě včetně CoA dle RFC3576 a RadSec (Radius Over TLS) ○ Podpora tunelového režimu propojení s nabízenými AP s transportem veškerého i uživatelského provozu přes			

	controller a možností jeho šifrování ▪ 18 x L2 switch (min. 8 x 10/100/1000 Mbps + 2x SFP 1Gb) a 1 x L2 switch (min. 24 x 10/100/1000 Mbps + 2x SFP 1 Gb) s minimálními parametry: o Podpora PoE+ 802.3at na všech metalických portech a 802.1x ověřování o Podpora MVRP dle standardu 802.1ak pro distribuci VLAN o STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) o Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 o Podpora RADIUS včetně RADIUS CoA (RFC3576) o Podpora REST API pro automatizaci nastavení sítě. o Podpora Zero Touch Provisioning (ZTP) o Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway) o Automatická konfigurace portu podle připojeného zařízení (automatické nastavení tagged a untagged VLAN, QoS a ACL) ▪ 3 x PoE injektor dle 802.3af 1Gpbs. ▪ 1x Sjednocená management platforma pro dodávané WiFi řešení a switche (přípustná je 1ks fyzická appliance nebo 1 ks virtuální appliance s podporou Vmware) o Podpora upgrade firmware switchů			

	○ Podpora zálohování a zpětné nahrávání konfigurací zařízení ○ Monitorování a sběr aplikačních toků ze sítě minimálně po 30 dní ○ Monitorování a sběr historie bezdrátové sítě a připojených klientů minimálně 180 dní ○ Vizualizace fyzické topologie sítě (automatická-bez nutnosti manuálního zadávání zařízení) ○ Sledování a vyhodnocení kvality a spolehlivosti síťových služeb: DNS, DHCP, RADIUS ○ Možnost importu mapových podkladů a zakreslení rozmístění AP. Následná simulace pokrytí prostoru signálem a zobrazení připojených klientů lokalizační metodou triangulace pomocí RSSI. ▪ 1x Reportovací nástroj pro WiFi řešení a dodávané switche – přípustná je 1ks fyzická appliance nebo 1 ks virtuální appliance s podporou Vmware. Minimální velikost úložiště (pro HW appliance v RAID) 4 TB. Může být společný pro firewally, WiFi access pointy a switche. Může být sloučen se sjednocenou management platformou. ▪ Licence pro všechny části řešení po dobu udržení projektu. ▪ Instalace strukturované kabeláže z technických místností k AP tunelem pod stropem. Pro instalaci bude dle kvalifikovaného odhadu zadavatele potřeba minimálně 2800 m UTP kabelu a 50 m lišt.			

Obecné informace:

Pokud zadavatel vyžaduje jako parametr některých prvků optické SFP/SFP+, zadavatel k tomu konstatuje, že v rámci budovy má vybudovány MM optické trasy a že optické transceivery jsou vyžadovány jako součást nabídky. V rámci dodávky bude zajištěno úvodní a průběžné školení administrátorů v rozsahu 20 MD.

Dílčí cíle implementace systému:

- Navrhnout řešení dle požadavků výše.
- Navrhnout a popsat architekturu včetně potřebného HW a potřebného SW včetně požadované integrace do prostředí Zadavatele.
- Naplnit požadavky pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
- Implementovat celé řešení podle návrhu schváleného Zadavatelem včetně migrace stávajícího řešení firewallů na nové.
- Servisní podpora v režimu 12/5/365 tj. v pracovní dny od 7-19 hodin s reakcí do 4 hodin.

Záruka a podpora (maintenance) výrobce:

Minimální záruka a podpora (maintenance) garantovaná výrobcem na dodané systémy je požadována v délce 60 měsíců. Pokud výrobce neumožňuje nákup záruky a podpory na 60 měsíců dopředně, zavazuje se dodavatel, že v rámci dodávky nabídne a dodá záruku a podporu na dobu co nejbližší 60 měsícům a poté bude tyto periodicky nakupovat ke své tíži tak, aby zajistil pro zadavatele záruku a podporu poskytovanou kontinuálně na požadovaných 60 měsíců.

3. Zvýšení fyzického zabezpečení HTCK

Realizace tohoto opatření naplní § 17 Fyzická bezpečnost Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v *platném znění.*

Jedná se o pořízení klimatizační jednotky, která bude umístěna ve vyhrazených prostorách OINF v místnosti budovy KÚSK 038 a dodávku zhášecího zařízení na bázi plynů inergenů umístěného ve vyhrazeném prostoru OINF v místnosti č. 2106 budovy KÚSK. Dodávkou těchto zařízení docílíme zvýšení technické dostupnosti služeb informačních technologií nastavením standardního teplotního prostředí v prostorách UPS TCK a omezíme vzniklé škody na zařízení informačních technologií instalovaných v místnosti 2106 KÚSK v případě zahoření.

Požadovaný účel implementace technologických zařízení:

Zvýšení dostupnosti služeb informačních technologií regulací teploty a omezení škod při zahoření prostor s instalovanými HW prvky informačních technologií KÚSK.

Základní požadavky implementace systému:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
Část	**Popis**			
Klimatizační jednotka	▪ Celoroční chlazení serverovny invertní klimatizací (2 jednotky) s centrálním ovládáním. ▪ Automatická regulace teploty v závislosti zatížení tepelným výkonem. ▪ Signalizace provozu a výpadku administrátorům klimatizovaných prostor, napojení na centrální alarm budovy. ▪ Filtrace antibakteriální standardní. ▪ Chladící/topný výkon kW/hod, – stanoví výpočtem dodavatel. ▪ Vnitřní jednotka nástěnná ▪ Ovládání IR (infra) nebo kabelový ovladač			NDA

	▪ Záruka na dodané zařízení min. 60 měsíců. ▪ Čištění klimatizační jednotky nejméně 2 x ročně.			
Parametry místnosti	▪ VxŠXH: 270x260x590, sklepní místnost. ▪ Okna: nejsou; jen vývod pro vzduchotechniku pod úrovní terénu. ▪ Dveře: obyčejné plechové, nutno utěsnit – návrh na dodávku bezpečnostních dveří. ▪ Omezení instalace: venkovní klimatizační jednotky – nutno najít prostor k umístění (vchod „C“ do úřadu). ▪ Napájení: samostatný přívod el. energie jištění dieselagregátem a automatickým přiřazováním. ▪ UPS: 3x EATON 9355−30−NHS−7−2x9Ah, output: 30kVA 27 KW (stávající řešení, není součástí zadání) Výkon se bude navyšovat minimálně 2x. ▪ Nenapojeno na centrální alarm budovy. ▪ Rozměrový náčrt místnosti s umístěnými technologiemi vydá zadavatel na vyžádání.			NDA
Automatický zhášecí systém	▪ Okamžitá reakce na dým (zajištěno optickokouřovým hlásičem). ▪ Zaplavení celého prostoru pří výskytu dýmu, uhašení vzniklého požáru s následným ochlazením chráněného prostoru. ▪ Spuštění hasícího systému musí signalizovat zvukové a elektronické signalizační zařízení. ▪ Spuštěním hasícího systému musí být automaticky ukončeno větrání místnosti, aby nedošlo k úniku plynu potřebného k hašení. ▪ V případě výpadku elektrické energie musí být zařízení vybaveno záložním systémem spuštění v případě zahoření.			NDA

	▪ Použité hasivo nesmí být toxické a při určité koncentraci hašení nesmí ohrozit obsluhu zařízení. ▪ Zhášecí zařízení nesmí překročit procentní obsah ve vzduchu, který povoluje norma a nesmí obsluhu ohrozit na životě. ▪ Zhášecí zařízení musí být certifikováno pro použití v ČR. ▪ Výstup pro relé na větrání. ▪ Zajištění servisu zařízení po dobu 60 měsíců v rozsahu minimálně jednou za 12 měsíců: o Prohlídka zařízení s kontrolou jednotlivých částí. o Kontrola úniku hasiva detektorem s jeho převážením. o Kontrola vnitřního tlaku nezávislým manometrem. o Kontrola funkce hlásiče a záložního systému spouštění hasiva. o Kontrola funkce ventilu bez vypuštěného hasiva. o Vystavení protokolu o kontrole do evidence KÚSK.			
Parametry místnosti	▪ Celková VxŠxH: 350 x 280 x 680. ▪ VxŠxH: zdvojené podlahy: 26 x 280 x 360. ▪ Okno: 1 rozměr 170 x 235. ▪ Dveře: bezpečnostní dveře s těsněním. ▪ Omezení instalace: dvojitá podlaha. ▪ Napájení: samostatný přívod el. energie jištěný UPS a dieselagregátem. ▪ Napájeno na centrální alarm budovy, požární čidla. ▪ 2 centrální klimatizace, dvě náhradní a vzduchotechnika. ▪ Technicky místnost odpovídá standardu pro serverovny. ▪ Technická zdvojená podlaha.			NDA

Obecné požadavky na realizaci:

Venkovní jednotka klimatizace bude umístěna na zdi ve dvoře v 1.NP, jednotka bude přichycena konzolí na zeď, vzdálenost cca 20 m.

Stavební prostupy včetně začištění a protipožárního utěsnění budou součástí předmětu plnění ze strany vybraného dodavatele v součinnosti s hospodářskou správou Zadavatele.

Dílčí cíle implementace systému:

- Navrhnout řešení dle požadavků výše.
- Implementovat celé řešení včetně potřebných úprav stavebních prostupů.
- Servisní podpora v režimu 12/5/365 tj. v pracovní dny od 7-19 hodin s reakcí do 4 hodin.

Záruka a servis:

Minimální záruka garantovaná výrobcem a servis na dodaný systém dodavatelem je požadována v délce 60 měsíců. Pokud výrobce neumožňuje nákup záruky a servisu na 60 měsíců dopředně, zavazuje se dodavatel, že v rámci dodávky nabídne a dodá záruku a servis na dobu co nejbližší 60 měsícům a poté bude tyto periodicky nakupovat ke své tíži tak, aby zajistil pro zadavatele záruku a servis kontinuálně poskytovaný na požadovaných 60 měsíců.

4. Sdílené služby kybernetické bezpečnosti

Součástí služby jsou následující činnosti:

1. zaznamenávání a ukládání logů a detekce bezpečnostních událostí
2. analýza datových toků a detekce bezpečnostních událostí
3. dohledové centrum - SOC

4.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí

Realizace tohoto opatření naplní, dle Vyhlášky 82/2018 Sb., *§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů, § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.*

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů zajistí tzv. log management. Mimo sběru logů řeší log management i zajištění jejich uložení v nezměněné podobě minimálně po zákonem definovanou dobu.

Security Information and Event Management (dále jen „SIEM“) je jedním ze základních stavebních prvků, který zajišťuje nutné bezpečnostní informace pro plnění povinností vyplývajících ze Zákona o kybernetické bezpečnosti a příslušných vyhlášek. Bez SIEM nástroje nelze reálně splnit požadavek na vyhodnocování kybernetických bezpečnostní události a následného hlášení kybernetického bezpečnostního incidentu dle § 7 a § 8 zákona 181/2014 Sb.

Poptávané řešení bude dodáno formou rozšíření služby SOC o sběr, uložení, vyhodnocování logů a detekce kybernetických událostí, musí umožňovat efektivně reagovat na již proběhlé bezpečnostní incidenty.

Dále služba umožní dlouhodobé ukládání dat v nezpochybnitelné podobě pro potřeby shody s předpisy, požadavky pro forenzní analýzu, případné bezpečnostní audity a orgány ČR. Systém poskytuje i informace pro operační a provozní úseky, kterým bude umožněno snadnými dotazy proti uložené databázi s logy nalézat například podstatu možného bezpečnostního incidentu u aplikačního nebo infrastrukturního systému, okamžitě identifikovat podstatu identifikované hrozby, včetně rychlého dohledání událostí popisujících její příčinu. Poptávané řešení musí poskytovat vysokou dostupnost sběru a transportu logů minimálně na úrovni sběračů logů.

Navazující rozšiřující službou bude SIEM, který v reálném čase vyhodnotí bezpečnostní výjimky z uložené databáze a prezentuje data ve formě předdefinovaných reportů. Systém bude podporovat sběr všech potenciálních událostí a logů vznikajících v informačním systému KÚSK a zajistí jejich ukládání do centrálního zabezpečeného úložiště. Od systému bude požadováno, aby rychle vyhodnocoval velké množství dat, které okamžitě zpracuje.

Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC.

Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

Požadovaný účel služby:

Poskytnout komplexní službu pro zaznamenávání logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

Základní požadavky na službu:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízená služba tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve

sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnutou službu a její technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů *§24 Sběr a vyhodnocování kybernetických bezpečnostních událostí*				
1.	Řešení musí být funkčně i technicky odděleno od ostatních částí systému SIEM			public
2	Řešení nesmí nijak zasahovat do sbíraných systémů.			public
3	Řešení musí být schopno trvale zpracovávat 10000 EPS			public
4	Řešení musí umožnit uchování log záznamů (RAW formát) po dobu minimálně 13 měsíců			public
5	Řešení musí poskytnout vysokou dostupnost sběru logů (sběračů).			public
6	Řešení musí podporovat (sbírat, zpracovat a interpretovat) všechny typy logu a protokolů nezbytné pro zpracování dle vyhlášky 82/2018 Sb. Jmenovitě musí podporovat zejména následující typy logů a protokolů: TCP/UDP Syslog, WMI, SQL, FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol RAW, CEF, JSON RFC7159 a další. Windows Events Collection (WinRM/ RPC) - MS Windows Vista SP2 a vyšší, MS windows Server 2008 a vyšší, MS SQL 2008 a vyšší.			public
7	Řešení musí podporovat bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)			public
8	Řešení musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenou strukturu a význam dat.			public
9	Komponenta sbírající logy je posílá dále zašifrovaně a komprimovaně a umožňuje regulovat šířku užívaného pásma.			public
§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí.				

10	Licence pro trvalé zpracování 1000 EPS v rámci celodenního průměru, která musí být rozšířitelná na 5000 EPS v celodenním průměru.			NDA
11	Architektura produktu obsahuje realtime procesory pro sběr a analýzu událostí včetně fulltext databáze pro ukládání a analýzu dat.			public
12	Řešení zvládá krátkodobé výkonové špičky (trvání 24 hodin) o objemu 7500 EPS.			NDA
13	Řešení musí podporovat současnou práci minimálně 5 administrátorů či operátorů.			public
14	Řešení musí obsahovat možnost minimálně 1000 sběrných konektorů			public
15	Řešení nebude licenčně omezeno úložnou kapacitou.			public
16	Licence umožňuje dočasné překročení EPS limitu na dobu několika minut bez ztráty přijímaných událostí.			public
17.	Možnost definovat na základě rolí uživatelům přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům.			public
18.	Možnost uložení uživatelem vytvořených pohledů na data (dashboardů, pojmenovaných dotazů) pro budoucí zpracování.			public
19	Systém umožňuje tvorbu pravidelných reportů podporujících řízení bezpečnosti podle standardu ISO 27001 s tím, že úroveň reportování bude specifikována v průběhu provozu SOC.			public
20	Služba splňuje požadavky kladené evropskými a českými bezpečnostními normami – ISO 27001, GDPR a zákon 181/2014 Sb. - Zákon o kybernetické bezpečnosti.			public
21	Řešení Služby bude poskytovat automaticky backup/recovery procesu.			public
22	Poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému.			public
23	Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box).			public
24	Systém musí umožňovat definici vlastního parseru pro jednotlivé zdroje logů a tím, že uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka.			public
25	Požadujeme zajištění integrity nasbíraných dat, kdy data jsou kontrolována před neoprávněnou změnou nebo smazáním.			public
26	Požadujeme možnost nastavit více filtrů retenčních politik pro různé zdroje dat			public

27	Near-real-time analýza událostí			public
28	S ohledem k nastavení a provádění procesu získávání, zaznamenání a zpracování logů je přípustná detekce bezpečnostních událostí v řádu minut.			public
29	Analýza dlouhodobých trendů událostí			public
30	Pokročilé "drill-down" dohledávání v případě potřeby			public
31	Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro zadání regulárními výrazy			public
32	Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí			public
33	Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů			public
34	Korelační systém musí využívat i externí on-line reputační databázi pro vyhodnocování bezpečnostních rizik.			public
35	Systém musí být schopen využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu a snížení false-positives			public
36	Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení			public
37	Požadujeme schopnost samostatného “učení” normálního stavu. Podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií.			public
38	Vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript			public
39	Schopnost pracovat s IP geolokacemi (botnet kanály atp.)			public
40	Generování alertu při výpadku logů z konkrétního zařízení			public
41	Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs. databázový server)			public
42	Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy			public
43	Požadujeme pravidelnou, plánovanou tvorbu takových reportů minimálně ve formátech PDF a			public

	CSV + podporu alespoň jednoho běžně používaného formátu pro strojové čtení (XML či JSON)			
44	Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.			public
45	Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy.			public
46	Řešení musí uchovávat logy v normalizovaném formátu, tak i „raw“ formátu.			public
47	Řešení musí obsahovat funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru, jako jsou STIX nebo TAXII.			public
48	Řešení musí být navázáno na národní centrum kybernetické bezpečnosti CSIRT a publikovat v konzoli jím aktuálně uveřejněné hrozby.			public
49	SIEM použitý v řešení musí být zařazen do 5 posledních studií agentury Gartner (tzv. magických kvadrantů)			

Další požadavky na rozšiřující službu SOC:

- Nabízená služba detekce bezpečnostních událostí musí:
  - naplnit požadavky pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).
  - zajistit dlouhodobé uschování logů pro předložení organizacím zabývajícím se bezpečností, zejména NBÚ a orgánům činným v trestním řízení.
  - zajistit v rámci poskytování služby SIEM napojení „Primárních aktiv“, kterými jsou významné informační systémy (VIS) Krajského úřadu Středočeského kraje, pokud tato aktiva poskytují využitelné výstupy, které lze automatizovaně zpracovat:
    1. Spisová služba
    2. Ekonomický systém
  - zajistit v rámci poskytování služby SIEM napojení „Podpůrných aktiv“, kterými jsou bezpečnostní systémy a veškeré ICT prvky pro zajištění provozní dostupnosti, důvěrnosti a integrity informací:
    1. Ochrana perimetru a přístupy k perimetru sítí Internet/DMZ/LAN/WiFi
    2. Komponenty datové sítě (switch, router, hub, access point)
    3. Network Behavior Analyzer
    4. Autentizační a autorizační systémy
    5. Anti (mallware, spam, adware) systémy
    6. Vulnerability management systém
    7. Databázové systémy
    8. Provozní dohledové systémy (Servery, Storage, Datová síť, Energy infrastruktura, Zálohování dat)

9. Zálohovací systémy
10. Operační systémy serverů – Unix a Windows
11. Virtualizační infrastruktura

Záruka a podpora (maintenance) výrobce:

Poskytovatel služby zajistí, že po celou dobu poskytování služby budou veškeré využité části kryté zárukou a podporou ze strany výrobce. Z tohoto důvodu zadavatel nepřipouští open sourcové řešení.

Doba poskytování služby:

Služba bude poskytována po dobu 60 měsíců.

4.2. Analýza datových toků a detekce bezpečnostních událostí

Realizace tohoto opatření naplní § 23 Detekce kybernetických bezpečnostních událostí Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v *platném znění.*

Jedná se o komplexní službu pro monitorování sítě KÚSK na základě datových toků, kterou umožní nástroje pro sledování provozu a zabezpečení sítě. Služba bude podporovat následná řešení vyskytujících se problémů a nestandardních stavů v síti, monitoring aktivit uživatelů a provozovaných SW aplikací. Služba umožní správcům pohled na využití síťového provozu na infrastruktuře KÚSK. Služba disponuje funkcí, která umožní sledovat výkonové parametry sítě a technologií analýzy datových toků včetně vyhodnocování chování sítě v návaznosti na aktuální hrozby a nestandardní stavy.

Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC.

Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

Požadovaný účel služby:

Poskytnout komplexní službu pro zaznamenávání aplikačních logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

Základní služby:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízená služba tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnutou službu a její technické parametry.

Minimální technické požadavky, které zadavatel požaduje		**Splnění požadavků zadavatele (ANO/NE)**	**Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku**	**Public/NDA**
Část	**Popis**			
Řešení	▪ V rámci monitoringu infrastruktury KÚSK se předpokládá využití: o 1x Kolektor a detekční moduly. o 2x Modul sonda. o Dále jako zdroj budou připojeny alespoň 2x core přepínače.			NDA
Obecné				
Monitorování sítě	▪ Schopnost analyzovat provoz ze SPAN portu			public

	centrálních switchů, TAP zařízení nebo zdrojů NetFlow dat. ▪ Protokoly NetFlow v9 a IPFIX nebo ekvivaletní. ▪ Podpora pro IPv4, IPv6, VLAN, MPLS ▪ Neviditelné na L3 vrstvě (monitorovací porty nemají IP, je zcela pasivní. ▪ Zaznamenávání vybrané komunikace do formátu PCAP z celé sítě. ▪ Řešení, které významným způsobem nezatíží datové linky zadavatele (nárůst provozu o max 5%)			
Komponenty				
Modul NetFlow kolektor	▪ Záznamy dat 12 měsíců zpětně na RAID poli. ▪ Dedikovaná kapacita je alespoň 48TB dat. ▪ Zabezpečená vzdálená správa, dohled a konfigurace.			NDA
Modul NetFlow sonda	▪ 2 kusy sondy ▪ Realizováno hardware komponentami s instalaci do 19“ racku, každá sonda max. 1RU. ▪ Zabezpečená vzdálená správa, dohled a konfigurace. ▪ Podpora standardu NSEL, monitorování MAC adres. ▪ Fyzická monitorovací rozhraní minimálně 2x 10Gbps pro každou sondu ▪ Sondy poskytnou na každém monitorovacím portu monitorování v rychlosti 10 Gbps ▪ Podpora pro příjem a analýzu HTTP/HTTPS provozu. ▪ Pasivní zapojení monitorovacích portů přes TAP. ▪ Zpracování všech FLOWs – nesamplované. ▪ Monitoring zpoždění sítě a odezvy aplikace.			public

Modul detekce anomálií na síti	▪ Nástroj bude poskytován na kolektoru, kde bude dostupné grafické rozhraní a které bude i zdrojem pro reporting událostí pro rozšiřující službu SIEM. ▪ Sběr a zpracování statistik o síťovém provozu. ▪ Sbírání informací z netflow sond. ▪ Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). ▪ Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti. ▪ Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti. ▪ Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103). ▪ Integrace informací ze služeb DNS, DHCP, WHOIS, geolokační služby.			public
Modul analýzy a monitorování komunikace aplikací a systémů	▪ Pro naplnění zákona č.101/2000 Sb. v aktuálním znění má řešení detekovat a lokalizovat aktuální změny komunikace systémů, aplikací a uživatelů pracujících se zákonně klasifikovanými informacemi, tj.: o Sledování komunikace systémů o Sledování komunikace aplikací			public
Modul analýzy a monitorování výkonosti	▪ Sledování provozní výkonnosti datové sítě, minimálně Round Trip Time			public

	▪ Sledování provozní výkonnosti všech aplikací z provozu datové sítě, především reakce databází a WWW strojů.			
Správa				
Víceuživatelský přístup	▪ Možnost definovat k jakým datům má jednotlivý uživatel přístup i v jednotlivých aplikačních modulech.			public
Webové rozhraní	▪ Uživatelsky definovat dashboard. ▪ Správu provádět prostřednictvím webového rozhraní.			public
Aktualizace	▪ Zařízení pravidelně samostatně aktualizuje znalostní bázi.			public
Reporty				
Generování	▪ Vytvářet krátkodobé i dlouhodobé grafy a přehledy s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), aplikačních protokolů atp. ▪ Generování statistik a podrobných výpisů nad volitelnými časovými intervaly. ▪ Export reportů a grafů alespoň do PDF.			public
Zasílání logů do SIEM	▪ Zasílání logů o detekovaných událostech ze všech detekčních modulů s možností uživatelské konfigurace přes GUI ▪ Konfigurovatelný obsah logů			public

Dílčí cíle služby:

- Navrhnout řešení služby dle požadavků výše.
- Navrhnout a popsat architekturu, včetně potřebného HW a potřebného SW, včetně požadované integrace do prostředí Zadavatele.

- Naplnit požadavky pro významné informační systémy pro řešenou oblast ze zákona č. 181/2014 Sb. o kybernetické bezpečnosti a příslušných vyhlášek v platném znění a souvisejících část normy ČSN ISO/IEC 27001:2014 (nebo rovnocenné řešení).

Záruka a podpora (maintenance) výrobce:

Poskytovatel služby zajistí, že po celou dobu poskytování služby budou veškeré využité části kryté zárukou a podporou ze strany výrobce. Z tohoto důvodu zadavatel nepřipouští open sourcové řešení.

Doba poskytování služby:

Služba bude poskytována po dobu 60 měsíců.

4.3. Dohledové centrum - SOC

Předmětem poptávky je komplexní řešení pro centralizovanou správu, ukládání a vyhodnocování logů v nezměnitelné podobě z libovolných síťových aktivních prvků, operačních systémů a používaného aplikačního software provozované formou služby Sdíleného dohledového centra kybernetické bezpečnosti (SOC – Security Operation Centra). Implementace systému bude v provedena v souladu s § 22 a § 24 Vyhlášky č.82/2018 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti v *platném znění*.

Požadovaný účel implementace opatření:

Zajištění externě provozované / dodávané služby dohledového ICT bezpečnostního centra - SOC.

Základní požadavky implementace systému:

Požadavky zadavatele jsou uvedeny ve sloupci „Minimální technické požadavky, které zadavatel požaduje“. Dodavatel je povinen vyplnit, zda jím nabízený produkt / řešení tyto požadavky splňuje, a to v sloupci „Splnění požadavků zadavatele“ (dodavatel doplní prohlášení ANO nebo NE podle skutečnosti). Ve sloupci „Odkaz do nabídky“ dodavatel uvede odkaz na konkrétní část nabídky, ve které je možné ověřit splnění uvedeného požadavku. Následná smlouva s vybraným dodavatelem může být v této části upravena tak, aby obsahovala již pouze dodavatelem nabídnuté zařízení a jeho technické parametry.

Minimální technické požadavky, které zadavatel požaduje		Splnění požadavků zadavatele (ANO/NE)	Odkaz do nabídky dodavatele, kde je možné ověřit splnění požadavku	Public/NDA
Požadavky na SOC				
1.	Poskytovatel prokazatelně doloží, že provozuje CSIRT (CERT), který je registrovaný v databázi TF – CSIRT Trusted Introducer.			public
2.	Poskytovatel musí uvést adresu, kde jsou ukládána data SOC k prokázání zpracování dat v působnosti právních norem ČR			public
3.	Informace o provozu a potenciálních zranitelnostech informačních systémů umožní zavádění preventivních opatření a předcházení případným bezpečnostním incidentům.			public
4.	Zavedením systému zadavatel získá schopnost detekce bezpečnostních incidentů a informace pro jejich rychlejší a efektivnější řešení.			public
5.	Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace zadavatele.			public
6.	Pro případné auditní akce ze strany zadavatele systém umožní provádění tzv. NBA (Network			public

	Behavioral Analysis), tj. automatického trvalého monitorování síťového provozu nad prostředím sdíleného dohledového centra kybernetické bezpečnosti. Ze stejného důvodu bude nad významnými součástmi služby provozován nástroj pro audit a monitoring aktivit uživatelů.			
7.	Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu. Data / logy budou uskladněna v prostředí poskytnutém dodavatelem, a to minimálně na dobu požadovanou zákonem.			public
8.	Vytvoření bezpečného sdíleného uložiště pro sdílení kompletních materiálů k poskytované službě.			public
9.	Detailní analýza bude zahrnovat identifikaci zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Analýza bude podléhat schválení zadavatelem.			public
10.	Zdroje dat budou vybrány z tzv. primárních a podpůrných (technických) aktiv zadavatele (zejm. se jedná o systémy a řešení poptávané v této veřejné zakázce). K jejich určení bude využito vyhlášky č. 82/2018 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí zadavatele (zadavatel provozu celkem 4 významné informační systémy – GINIS, e-mail, elektronickou spisovou službu a Service Desk). Dále bude pro určení zdrojů dat využito vstupního osobního setkání (workshopu) se správci provozovaných informačních a komunikačních systémů v rozsahu jednoho pracovního dne.			public
11.	Předimplementační analýza bude obsahovat následující oblasti specifické pro SOC: (a) specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře, (b) klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu), (c) doporučení nastavení logování pro jednotlivé zdroje, (d) výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů, (e) návrh parserů pro zdroje, které nebudou systémem přímo podporovány,			public

	(f) návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti, (g) metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací, (h) pravidla pro vznik varováni, upozornění, incidentů včetně priority, (i) doporučenou strukturu oprávnění a řízení přístupových práv (j) proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod. (k) popis zajištění autentičnosti logů, (l) definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.), (m) návrh zálohování konfigurace a dat, (n) návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu, (o) návrh retence logů a archivů, (p) návrh způsobu napojení řešení na monitorovací systém dodavatele a definice procesů reakce, které jsou v souladu s platnou legislativou a bezpečnostní politikou ISKÚ, (q) popis monitorovaných aktivit přispívajících k naplnění požadavků dle zákona č.101/2000 Sb. v aktuálním znění a k naplnění požadavků dle nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR).			
12.	Součástí dodávky bude návrh změn konfigurací dotčených a souvisejících systémů, koordinace provedení změn s provozovateli systémů a ověření správné konfigurace.			public
13.	Součástí dodávky bude návrh a provedení funkčních testů (musí zahrnovat výkonové testy, testy archivace/obnovy logů a ověření detekce neoprávněně modifikace logů). Návrh podléhá schválení zadavatele.			public
Požadovaná podpora SOC				
14.	Průběžné monitorování IT prvků dodaných v rámci této veřejné zakázky, popř. prvků IT, které mohou ovlivnit jejich chod. Počet sledovaných parametrů nesmí být prakticky omezen (min. stovky).			public

15.	Monitoring bude probíhat minimálně dle výstupů ze služby pro zaznamenávání a ukládání logů a detekce bezpečnostních událostí (SIEM), systému analýzy datových toků a detekce bezpečnostních událostí, systému pro pokročilý provozní dohled a firewallů zadavatele.			public
16.	Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.			public
17.	Rozšířený monitoring a specifické služby provozního zajištění komodity SOC: (r) Provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb. (s) Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / tel). (t) Zahájení řešení bezpečnostního incidentu do 4 hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob. (u) Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NUKIB, CSIRT atd. (v) Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference. (w) Kontinuální skenování aktiv definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové. (x) Přístup administrátorů zadavatele ke sledovaným parametrům alespoň v režimu čtení prostřednictvím grafického rozhraní (GUI – dashboard apod.).			public
18.	Dodavatel zpracuje a poskytne zadavateli každý měsíc Report, ve kterém je popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a prevenci incidentů.			public
SLA				public
19.	Přístup k podpoře služby - HotLine/Ticket systém – 24 x 7			public

20.	Přístup k webovému portálu služby – 24 x 7			public
21.	Reakční čas na změnu konfigurace služby mimo Incident Response – 12x5 do 4 hodin			public
22.	Reakční čas na mimořádnou událost – do 15 minut			public
23.	**Služba Monitoringu a detekce - Zajištění Operátorské úrovně** Průběžné sledování provozu prostředí objednatele. Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému objednatele na analytického specialistu dodavatele.			public
24.	**Služba reakce na nestandardní situace v provozu bezpečnostních systémů – Zajištění analytické úrovně** Zpracování analytických scénářů na aktuální kybernetické hrozby. Posouzení eskalovaného problému objednatele analytickým specialistou. Detekce a vyhodnocení závažnosti identifikovaných anomálií. Posouzení a ve spolupráci se Zadavatelem případná eskalace nestandardní situace v provozu objednatele na službu včasné výstrahy a reakce na incident v rámci bezpečnostních struktur ČR. 1x za měsíc předání analytického reportu za uplynulé období do 10 pracovního dne v následném měsíci interpretující stav bezpečnosti prostředí, účinnost nápravných opatření a seznam eskalace incidentů.			public

<u>Doba poskytování služby</u>:

Dohledové centrum bude poskytováno formou služby po dobu 60 měsíců.

5. Služby poradenství a podpory, resp. „Služby spojené s implementací IS“

5.1. Předimplementační analýza

Před implementací řešení zpracuje dodavatel předimplementační analýzu, minimálně pro následující oblasti a pro oblasti specifické pro jednotlivé dodávané produkty a služby:

1. Detailní popis stávajícího stavu, identifikaci slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy TCK.
2. Způsob začlenění nabízených komodit do prostředí TCK, popis začlenění nabízených / dodávaných služeb do procesů zadavatele.
3. Síťová infrastruktura ve vztahu k plánovanému využití.
4. SAN infrastruktura ve vztahu k plánovanému využití.
5. Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.
6. Integrace nabízených softwarových systémů.
7. Rekonfigurace stávajících systémů.
8. Dopady implementace na dostupnost a funkčnost stávajících služeb.
9. Požadované součinnosti zadavatele a jejich rozsah.
10. Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva, která podléhá schválení zadavatelem.

5.2. Prováděcí dokumentace

Po schválení předimplementační analýzy zpracuje dodavatel prováděcí dokumentaci minimálně pro následující oblasti a pro oblasti specifické pro jednotlivé dodávané produkty a služby:

1. Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude vycházet ze schválené předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění veřejné zakázky do stávajícího prostředí TCK.
2. Prováděcí dokumentace musí být před zahájením prací schválena zadavatelem.
3. Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
    a. Detailní popis cílového stavu včetně funkcionalit jednotlivých částí dodávky.
    b. Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů TCK (vSphere, LAN, SAN, zálohování, monitorování atd.).
    c. Způsob zajištění potřebného HW a SW.
    d. Způsob zajištění koordinace realizace předmětu plnění s běžným provozem.
    e. Detailní návrh a popis postupu implementace předmětu plnění.
    f. Detailní popis zajištění bezpečnosti informací.
    g. Detailní harmonogram realizace včetně uvedení kritických milníků.
    h. Návrh designu síťového a bezpečnostního řešení a jeho konfigurace.
    i. Návrh designu aplikačních řešení.
    j. Vazby na stávající systémy a jejich konfigurace.

k. Návrh akceptačních kritérií a akceptačních testů.

Výstupem prováděcí dokumentace bude písemná zpráva, která podléhá schválení zadavatelem.

5.3. Projektové vedení dodávky

V průběhu celého plnění veřejné zakázky (dodávka řešení) zajistí dodavatel projektové vedení dodávky:

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu je požadováno aplikování základních principů projektového řízení ze strany dodavatele. Jedná se o následující aktivity:

1. Řízení projektových prací v souladu s uzavřenou smlouvu s ohledem na:
   a. věcné plnění dané smlouvou,
   b. řízení postupu prací s ohledem na závazný harmonogram projektu,
   c. dodržování termínů a milníků harmonogramu.
2. Zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů z konzultačních schůzek a pracovních jednání.
3. Prezenční účast odpovědné osoby dodavatele na kontrolních dnech v sídle zadavatele, případně se souhlasem obou smluvních stran formou videokonference nebo telekonference.
4. Reporting projektu na úrovni pravidelných dvoutýdenních písemných zpráv směrem k odpovědné osobě zadavatele.
5. Řízení rizik projektu.
6. Řízení změn na projektu – v případě odsouhlasení změn spolupráce při implementaci změn do projektu, komunikace s realizačním týmem.

5.4. Dokumentace

Zadavatel požaduje v rámci plnění zpracování a dodání konečné a úplné dokumentace k dodanému řešení v následující skladbě:

1. Uživatelská dokumentace – v rozsahu konkrétních nasazených funkcionalit u zadavatele.
2. Administrátorská dokumentace – správa a konfigurace v rozsahu konkrétního (nasazeného) řešení. Dokumentace musí být zpracována v takovém rozsahu, který umožní odborným IT pracovníkům zadavatele systémy spravovat a udržovat bez jakékoliv součinnosti dodavatele (s výjimkou mimořádných událostí a chyb v dodaném SW a HW).
3. Bezpečnostní dokumentace – příručka bezpečnostního správce informačních systémů.
4. Integrační dokumentace – dokumentace všech nasazených a dodaných rozhraní k informačním systémům.

5.5. Provádění prací

Zadavatel požaduje, aby v rámci plnění zakázky práce probíhaly:

1. V souladu se všemi běžnými zákonnými předpisy týkajícími se bezpečnosti práce
2. Dle zadavatelem schválené prováděcí dokumentace
3. Byly vždy řádně dokumentovány
4. A práce, které generují riziko pro technologie, infrastrukturu, či prostředí zadavatele, byly explicitně schvalovány pověřenou osobou zadavatele

6. Výkony nad rámec podpory

Jedná se o služby upravené v čl. III odst. 5.3) smlouvy o dílo.

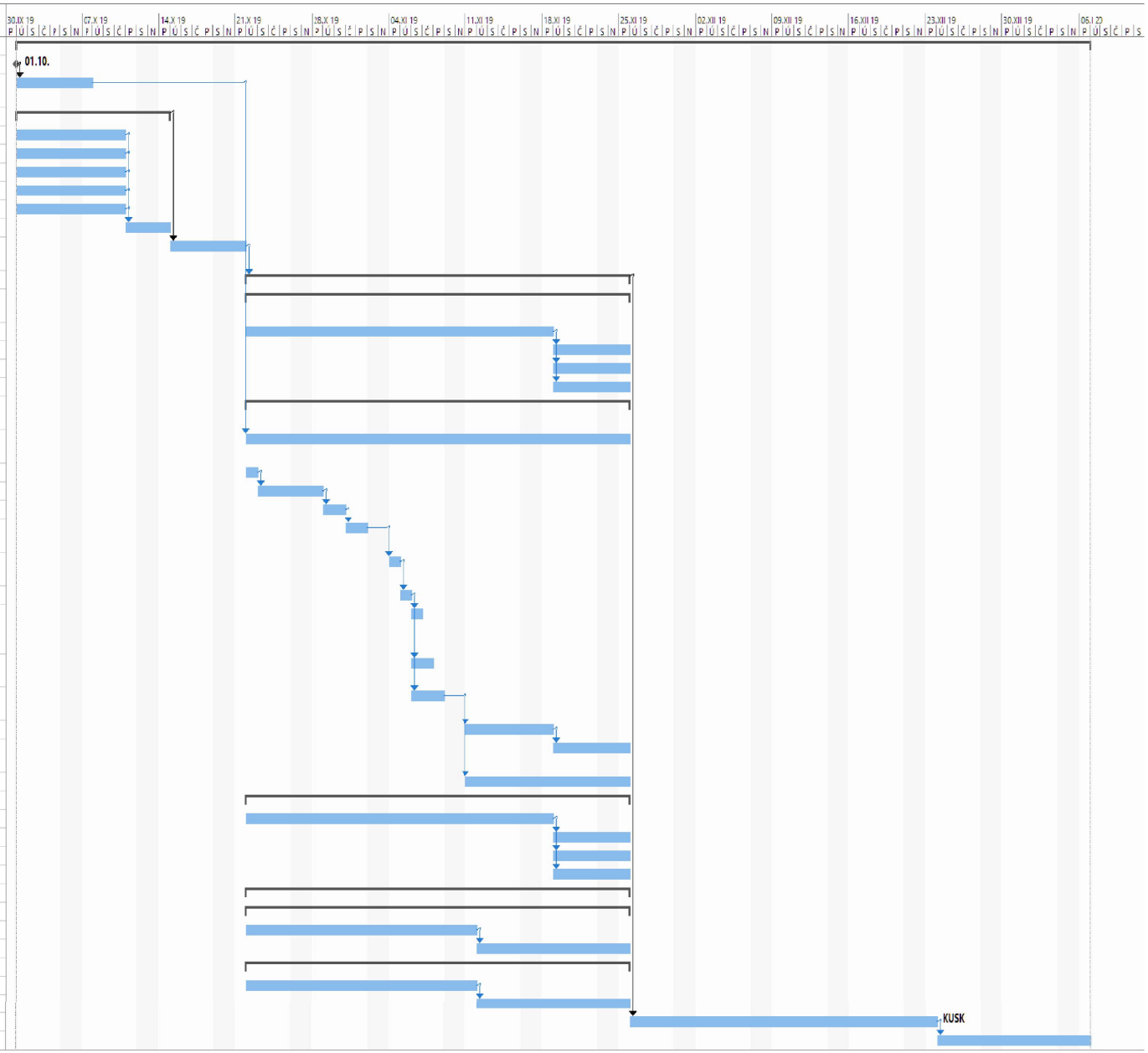
Podrobný nabídkový (položkový) rozpočet (dodávané systémy a služby)				
1. Systém pro pokročilý provozní dohled				
Název položky	**Počet kusů**	**Jednotková cena bez DPH**		**Cena celkem bez DPH**
Licence	1	2 024 796,67 Kč		2 024 796,67 Kč
Služby spojené s implementací IS (analýzy, prováděcí dokumentace, projektové vedení, instalace, testovací provoz)	1	342 261,90 Kč		342 261,90 Kč
Zaškolení administrátorů - úvodní (2 dny)	2	14 880,95 Kč		29 761,90 Kč
Školení administrátorů - průběžné (18 dnů)	18	14 880,95 Kč		267 857,14 Kč
Provozní náklady (60 měsíců)	1	428 571,43 Kč		428 571,43 Kč
Celkem	**-**		**-**	**3 093 249,05 Kč**
2. Systém podpory pokročilé segmentace sítě				
Název položky	**Počet kusů**	**Jednotková cena bez DPH**		**Cena celkem bez DPH**
Dodávka HW	1	3 752 785,56 Kč		3 752 785,56 Kč
Licence	1	3 918 642,22 Kč		3 918 642,22 Kč
Služby spojené s implementací IS (analýzy, prováděcí dokumentace, projektové vedení, instalace, testovací provoz)	1	1 107 755,95 Kč		1 107 755,95 Kč
Zaškolení administrátorů - úvodní (2 dny)	2	17 857,14 Kč		35 714,29 Kč
Školení administrátorů - průběžné (18 dnů)	18	17 857,14 Kč		321 428,57 Kč
Provozní náklady (60 měsíců)	1	3 214 285,71 Kč		3 214 285,71 Kč
Celkem	**-**		**-**	**12 350 612,30 Kč**
3. Zvýšení fyzického zabezpečení TCK				
Název položky	**Počet kusů**	**Cena bez DPH**		**Cena celkem bez DPH**
Dodávka HW	1	576 431,11 Kč		576 431,11 Kč
Licence	1	0,00 Kč		0,00 Kč
Služby spojené s implementací IS (analýzy, prováděcí dokumentace, projektové vedení, instalace, testovací provoz)	1	116 011,90 Kč		116 011,90 Kč
Provozní náklady (60 měsíců)	1	256 250,00 Kč		256 250,00 Kč
Celkem	**-**		**-**	**948 693,02 Kč**

4. Sdílené služby kybernetické bezpečnosti				
Název položky	**Počet měsíců**	**Jednotková cena bez DPH (měsíc)**		**Cena celkem bez DPH**
Zaznamenávání a ukládání logů a detekce bezpečnostních událostí (služba)	60	178 912,99 Kč		10 734 779,22 Kč
Analýza datových toků a detekce bezpečnostních událostí (služba)				
Dohledové centrum - SOC (služba)				
Celkem	**-**		**-**	**10 734 779,22 Kč**

5. Výkony poskytované nad rámec základní a rozšíření servisní podpory				
Název položky	**Počet MD**	**Jednotková cena bez DPH (1 MD)**		**Cena celkem bez DPH**
Výkony nad rámec servisní podpory	50	14 444,48 Kč		722 224,00 Kč
Celkem	**-**		**-**	**722 224,00 Kč**

Nabídková cena - První etapa	**11 904 161,51 Kč**	součet modrých polí	investice
Nabídková cena - Druhá etapa	**15 945 396,08 Kč**	součet zelených polí	služby
NABÍDKOVÁ CENA CELKEM	**27 849 557,59 Kč**		

ID	Režim úkolu	Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci
1		**Posílení bezpečnosti**	**70 dny**	**01.10. 19**	**06.01. 20**	
2		Zveřejnění smlouvy	0 dny	01.10. 19	01.10. 19	
3		Zahájení projektu, sestavení projektového týmu	5 dny	01.10. 19	07.10. 19	2
4		**Předimplementační analýza**	**10 dny**	**01.10. 19**	**14.10. 19**	
5		Předimplementační analýza Solutia	8 dny	01.10. 19	10.10. 19	
6		Předimplementační analýza Compu	8 dny	01.10. 19	10.10. 19	
7		Předimplementační analýza AiT	8 dny	01.10. 19	10.10. 19	
8		Předimplementační analýza hasič	8 dny	01.10. 19	10.10. 19	
9		Předimplementační analýza Axenta	8 dny	01.10. 19	10.10. 19	
10		Kompletace Analýzy	2 dny	11.10. 19	14.10. 19	5;6;7;8;9
11		Schválení předimplementační analýzy	5 dny	15.10. 19	21.10. 19	4
12		**Dodávka celkového řešení**	**25 dny**	**22.10. 19**	**25.11. 19**	11
13		**Systém pro pokročilý provozní dohled (Nagios)**	**25 dny**	**22.10. 19**	**25.11. 19**	
14		Implementace	20 dny	22.10. 19	18.11. 19	
15		Zkušební provoz	5 dny	19.11. 19	25.11. 19	14
16		Dokumetace	5 dny	19.11. 19	25.11. 19	14
17		Školení	5 dny	19.11. 19	25.11. 19	14
18		**Systém pokročilé segmentace sítě (Fortinet, Aruba)**	**25 dny**	**22.10. 19**	**25.11. 19**	
19		Instalace Kabeláže a jednotlivých AP	25 dny	22.10. 19	25.11. 19	3
20		Instalace a konfigurace ClearPassu	1 den	22.10. 19	22.10. 19	
21		Konfigurace AD, GP, CA, NPS	4 dny	23.10. 19	28.10. 19	20
22		Sběr MAC adres	2 dny	29.10. 19	30.10. 19	21
23		Aplikování nové Group Policy na koncové stanice	2 dny	31.10. 19	01.11. 19	22
24		Otestování funkčnosti ověřování 802.1x a MAC	1 den	04.11. 19	04.11. 19	23
25		Revize segmentace sítě VLAN	1 den	05.11. 19	05.11. 19	24
26		Montáž, propojení kabelů a oživení nově dodaných FW, WiFi, LAN switchů atd.	1 den	06.11. 19	06.11. 19	25
27		Upgrade SW a základní konfigurace nově dodaného HW	2 dny	06.11. 19	07.11. 19	25
28		Konfigurace přepínačů a bezdrátových kontrolerů	3 dny	06.11. 19	08.11. 19	25
29		Konfigurace FW a Sandboxu	6 dny	11.11. 19	18.11. 19	28
30		Spuštění ověřování 802.1x – postupné spouštění	5 dny	19.11. 19	25.11. 19	29
31		Dokumentace skutečného stavu	11 dny	11.11. 19	25.11. 19	28
		SEC	**25 dny**	**22.10. 19**	**25.11. 19**	
		Implementace	20 dny	22.10. 19	18.11. 19	
		Zkušební provoz	5 dny	19.11. 19	25.11. 19	33
		Dokumetace	5 dny	19.11. 19	25.11. 19	33
		Školení	5 dny	19.11. 19	25.11. 19	33
		yšení fyzického zabezpečení HTCI	**25 dny**	**22.10. 19**	**25.11. 19**	
		Chlazení	**25 dny**	**22.10. 19**	**25.11. 19**	
		Dodávka zařízení	15 dny	22.10. 19	11.11. 19	
		Instalace	10 dny	12.11. 19	25.11. 19	39
		Zhášení	**25 dny**	**22.10. 19**	**25.11. 19**	
		Dodávka zařízení	15 dny	22.10. 19	11.11. 19	
		Instalace	10 dny	12.11. 19	25.11. 19	42
		ovací provoz	20 dny	26.11. 19	23.12. 19	12
		eptace investiční části	10 dny	24.12. 19	06.01. 20	44



Dokument je podepsán elektronickým podpisem

Podepisující: **Martin Herman**
Organizace, OJ: Středočeský kraj - krajský úřad
Sériové č. cert.: 4074522
Vydavatel cert.: PostSignum Qualified CA 2
Datum a čas: 24.10.2019 08:08:10
Důvod:
Místo: Praha

310