Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

SMLOUVA O DODÁVCE HW A SW A O POSKYTOVÁNÍ SOUVISEJÍCÍCH SLUŽEB

uzavřená § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

Evidenční číslo smlouvy: OR/22/24254

Pardubický kraj

Sídlo: Komenského nám. 125, 532 11 Pardubice
IČO: 70892822
zastoupený: JUDr. Martinem Netolickým Ph.D., hejtmanem Pardubického kraje
Bankovní spojení: ČSOB, a.s., Pardubice
číslo účtu: 239602855/0300
Kontaktní osoba ve věcech technických: Ing. David Rezler:
tel. kontaktní osoby: [redacted]
e-mail:
Kontaktní osoba ve věcech projektu: Ing. Miroslava Oravcová
tel. kontaktní osoby: [redacted]
e-mail:

(na straně jedné, dále jen „**objednatel**“)

a

AUTOCONT a.s.

Sídlo: Hornopolní 3322/34, 702 00 Ostrava
Korespondenční adresa: Hornopolní 3322/34, 702 00 Ostrava
IČO: 04308697
DIČ: CZ04308697
zapsaný v obchodním rejstříku u Krajského soudu v Ostravě sp. zn. B 11012
zastoupený: Ondřejem Matuštíkem, členem představenstva
Bankovní spojení: Česká spořitelna a.s.
Číslo účtu: 6563752/0800
Kontaktní osoba: [redacted]
tel. kontaktní osoby:
e-mail:

(na straně druhé, dále jen „**poskytovatel**“)

(objednatel a poskytovatel dále společně také jako „**smluvní strany**“ a každá jednotlivě jako „**smluvní strana**“)

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu o servisu dodávce HW a SW a o poskytování souvisejících služeb (dále jen „**smlouva**“).

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Preambule

1. Tato smlouva se uzavírá v souvislosti s realizací projektu „Modernizace infrastruktury pro sdílení informací a dat s obcemi Pardubického kraje“ (dále jen „**projekt**“). Pardubický kraj je v rámci tohoto projektu příjemcem finanční podpory z Integrovaného regionálního operačního programu, č. výzvy 28 (dále jen „**Výzva 28 IROP**“), registrační číslo projektu CZ.06.3.05/0.0/0.0/16_044/0006323. Služby a dodávky, které jsou předmětem této smlouvy, jsou spolufinancovány z Výzvy 28 IROP a z rozpočtu Pardubického kraje. Smluvní strany této smlouvy jsou seznámeny s podmínkami stanovenými Výzvou 28 IROP, podmínkami pro účast v projektu a jsou rovněž obeznámeny s koncepcí projektu.
2. Poskytovatel je vybraným dodavatelem veřejné zakázky s názvem **„RDS 2.0 – Bezpečnostní modul“** (dále jen „**Veřejná zakázka**“) uveřejněné na profilu objednatele, jakožto zadavatele, ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), zadávané v otevřeném nadlimitním řízení. Služby, které jsou předmětem této smlouvy, navazují na dodávku prvků komunikační infrastruktury dle Smlouvy o dodávce.
3. Poskytovatel prohlašuje, že je držitelem potřebného živnostenského oprávnění a má řádné vybavení, zkušenosti a schopnosti, aby služby dle této smlouvy poskytoval ve stanovené době a ve sjednané kvalitě a že si je vědom skutečnosti, že objednatel má značný zájem na plnění předmětu této smlouvy, v čase a kvalitě stanovené touto smlouvou.

I.
Účel smlouvy

1. Účelem této smlouvy je zajištění realizace předmětu Veřejné zakázky dle zadávací dokumentace Veřejné zakázky (dále jen „**Zadávací dokumentace**“), tj. dodávky HW, dodávky SW včetně licencí, implementace do stávajícího prostředí objednatele, včetně využití stávajících produktů, licencí a smluvních vztahů objednatele, záruky a servisní podpory, a to v souladu s požadavky objednatele definovanými touto Smlouvou.
2. Poskytovatel touto smlouvou garantuje objednateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle Zadávací dokumentace. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:
   a) v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel a předmět plnění Veřejné zakázky vyjádřený Zadávací dokumentací;
   b) v případě chybějících ustanovení této smlouvy budou použita dostatečně konkrétní ustanovení Zadávací dokumentace;
   c) poskytovatel je vázán svou nabídkou předloženou objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

II.
Předmět smlouvy

1. Poskytovatel se zavazuje poskytnout objednateli plnění podrobně specifikované v příloze č. 1 této Smlouvy spočívající v dodávce, instalaci a implementaci HW a SW komponent včetně licencí, jakož i vzájemné funkční provázání těchto komponent s ostatní infrastrukturou Zadavatele a poskytnutí požadované servisní podpory, včetně dalších činností (dále jen „**Dodávka**“). Poskytovatel odevzdá věci, které jsou předmětem Dodávky, a umožní objednateli nabýt vlastnické právo k nim.
2. Poskytovatel se zavazuje poskytnout objednateli Dodávku řádně a včas za podmínek dle této smlouvy.
3. Objednatel se zavazuje zaplatit poskytovateli dohodnutou cenu za řádně a včas poskytnutou Dodávku a poskytnout poskytovateli součinnost nezbytnou k řádnému poskytnutí Dodávky, a to za podmínek touto smlouvou dále stanovených.
4. Poskytovatel se zavazuje Dodávku poskytovat sám, nebo s využitím poddodavatelů, které uvedl v příloze č. 6 Zadávací dokumentace a prostřednictvím osob – členů realizačního týmu, které uvedl v příloze č. 4 Zadávací dokumentace. Jakákoliv dodatečná změna osoby člena realizačního týmu, poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval poskytovatel sám. Nový člen realizačního týmu musí odpovídat požadavkům stanoveným objednatelem v Zadávací dokumentaci.
5. Smluvní strany výslovně uvádějí, že při poskytování Dodávky prostřednictvím poddodavatele má poskytovatel odpovědnost, jako by Dodávku poskytoval sám. Objednatel bude jednat vždy výhradně s poskytovatelem.

III.
Termíny a místo plnění

1. Nevyplývá-li z této Smlouvy výslovně jinak, je poskytovatel povinen provést Dodávku nejpozději do 8 měsíců nebo do 30. 5. 2023 od nabytí účinnosti této Smlouvy a poskytovat záruku a servisní podporu po dobu 5 let od předání HW, SW a jeho implementace do prostředí objednatele. Tím není dotčeno ustanovení čl. V. odst. 11 a 12 smlouvy.
2. Místem plnění této veřejné zakázky je sídlo objednatele. Pokud to povaha plnění dle smlouvy umožňuje, je poskytovatel oprávněn poskytovat plnění dle smlouvy také vzdáleným přístupem.

IV.
Způsob provedení dodávky

1. V rámci Dodávky je poskytovatel povinen provést instalaci a zprovoznění jednotlivých HW a SW komponent tvořících Dodávku, jakož i vzájemné funkční provázání těchto komponent se stávající infrastrukturou Zadavatele a poskytnutí požadované servisní podpory, včetně dalších činností, a to v souladu s **Přílohou č. 1** této Smlouvy.

2. V rámci provedení Dodávky a v rámci poskytnutí Licencí k autorským dílům tvořícím součást Dodávky je poskytovatel povinen předat objednateli veškerou dokumentaci, doklady, záruční listy, technické a uživatelské manuály a jiné dokumenty, které jsou nezbytné k řádnému užívání komponent tvořících Dodávku, jakož i k užívání Dodávky jako celku. Předáním dokumentace je myšleno zejména dodání následujících dokumentů uvedených v příloze č. 1 smlouvy (dále jen „**Dokumentace**“).

3. Objednatel akceptuje provedení Dodávky na základě provedené akceptační procedury dle ustanovení čl. V. této smlouvy.

4. Dodávka HW a SW včetně licencí je řádně provedena okamžikem podpisu akceptačního protokolu dle čl. V. odst. 4 smlouvy ze strany objednatele s výrokem „Akceptováno“. Tímto okamžikem přechází na objednatele vlastnické právo a nebezpečí škody způsobené na věcech tvořících součást Dodávky.

5. Pokud je součástí Dodávky poskytovatele poskytnutí doplňkového programového vybavení (software, systémové komponenty) nebo jiného předmětu (např. Dokumentace), který naplňuje znaky díla dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorské dílo**“), zavazuje se poskytovatel objednateli poskytnout nebo zajistit pro objednatele oprávnění užít veškerá takováto autorská díla všemi v úvahu přicházejícími způsoby užití nezbytnými k řádnému užívání Dodávky objednatelem po dobu trvání majetkových práv autorských autora k autorskému dílu, bez jakýchkoliv množstevních nebo územních omezení (dále jen „**Licence**“). V případě, že autorské dílo je standardním komerčním softwarovým produktem poskytovatele nebo třetí strany, objednatel připouští omezení Licence v nezbytném rozsahu z této skutečnosti vyplývajícího, umožňujícího naplnění předmětu a účelu této smlouvy. Smluvní strany se výslovně dohodly, že veškeré předmětné Licence budou objednateli poskytnuty bez nároku na dodatečnou odměnu nad rámec ceny Dodávky sjednané v této smlouvě a náklady na pořízení příslušné Licence jsou součástí ceny Dodávky dle této smlouvy.

6. Poskytovatel se zavazuje zajistit platnost Licencí k autorským dílům třetích stran a možnost objednatele užít veškerá takováto autorská díla v souladu s předmětem této smlouvy a k účelům vyplývajícím z této smlouvy.

7. Poskytovatel prohlašuje, že veškeré jeho plnění dodané podle této smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním poskytovatele podle této smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu (či obdobnému) zákazu či omezení užívání Dodávky či jeho části ze strany objednatele, zavazuje se poskytovatel zajistit náhradní řešení a minimalizovat dopady takovéto situace na objednatele, a to bez dopadu na cenu Dodávky sjednanou podle této smlouvy, přičemž současně nebudou dotčeny ani nároky objednatele na náhradu škody.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

V.
Akceptace

1. Část Dodávky, tvořící logický a funkční celek způsobilý být předmětem přejímky (dále jen „**dílčí plnění**“), bude objednatelem akceptována na základě akceptační procedury. Akceptační procedura zahrnuje ověření, zda poskytovatelem poskytnuté dílčí plnění splňuje podmínky, k jejichž splnění se poskytovatel zavázal, a to porovnáním skutečných vlastností jednotlivých dílčích plnění poskytovatele s jejich závaznou specifikací uvedenou v této smlouvě; specifikací se rozumí i akceptační kritéria, jsou-li stanovena dohodou Smluvních stran.
2. Předání a převzetí poskytovatelem řádně provedené Dodávky, která je samostatným dílčím plněním, proběhne na základě níže popsané akceptační procedury, a to v termínu dle čl. III. odst. 1 této smlouvy.
3. Poskytovatel písemně vyzve objednatele k účasti na akceptační proceduře nejméně 7 pracovních dnů před jejím zahájením. Pokud se objednatel nedostaví v termínu určeném pro provedení akceptačních testů, přestože byl poskytovatelem k účasti řádně vyzván, je poskytovatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti. O průběhu akceptačních testů vyhotoví poskytovatel písemný záznam, v němž zejména uvede, zda testy prokázaly chyby. Objednateli budou poskytnuty originály veškerých dokumentů vypracovaných v souvislosti s provedením akceptačních testů.
4. Jestliže jednotlivé dílčí plnění splní akceptační kritéria akceptačních testů, poskytovatel se zavazuje nejpozději v pracovní den následující po ukončení akceptačních testů umožnit objednateli toto dílčí plnění převzít a objednatel se zavazuje k jeho převzetí nejpozději do 5 pracovních dnů. Smluvní strany se zavazují o tomto převzetí sepsat akceptační protokol, jehož vzor je přílohou č. 2 této smlouvy.
5. Nestanoví-li specifikace akceptačních testů jinak, má se za to, že dílčí plnění splňuje stanovená akceptační kritéria za předpokladu, že toto plnění nemá žádnou vadu kategorie A ve smyslu odst. 6 tohoto článku smlouvy, a současně nemá více než 2 vady kategorie B ve smyslu odst. 7 tohoto článku smlouvy – v takovém případě objednatel může podepsat akceptační protokol s výrokem „Akceptováno s výhradami“. V případech, kdy počet a/nebo druh vad překračuje maximální počet stanovený pro splnění akceptačních kritérií s výrokem „Akceptováno s výhradami“, objednatel uvede do akceptačního protokolu výrok „Neakceptováno“ a není povinen Dodávku či dílčí plnění převzít.
6. Vadou kategorie A je vada, která zcela nebo podstatným způsobem znemožňuje použití dílčího plnění pro potřeby objednatele v souladu s touto smlouvou.
7. Vadou kategorie B je vada, která umožňuje použití dílčího plnění pro potřeby objednatele v souladu s touto smlouvou, ovšem dílčí plnění neodpovídá jeho specifikaci dle této smlouvy.
8. Za úspěšnou se akceptační procedura považuje v okamžiku, kdy je oběma stranami podepsán akceptační protokol s výrokem „Akceptováno bez výhrad“.
9. Pokud kterékoliv z jednotlivých dílčích plnění nesplňuje stanovená akceptační kritéria nebo je splňuje s vadami, které jsou přípustné, sdělí objednatel své připomínky písemně

poskytovateli; pokud objednatel takové dílčí plnění současně akceptuje, uvede své připomínky v akceptačním protokolu.

10. Poskytovatel je povinen vypořádat připomínky objednatele bez zbytečného odkladu a neprodleně předložit příslušné dílčí plnění k opakované akceptaci dle této smlouvy, za přiměřeného použití ostatních ustanovení tohoto článku smlouvy. Akceptační procedura se bude opakovat, dokud příslušné dílčí plnění nesplní akceptační kritéria a nebude možné zakončit akceptaci s výrokem „Akceptováno bez výhrad“. V případě, že se jedná o vypořádání připomínek k dílčímu plnění, které již bylo akceptováno, namísto akceptačního protokolu strany potvrdí písemně, že připomínky byly vypořádány.
11. Dohodnuté termíny pro akceptaci dílčího plnění nejsou dotčeny trváním akceptační procedury ani jakýmkoli jejím prodloužením z důvodu vad bránících akceptaci, tj. pokud akceptační procedura z důvodů na straně poskytovatele či z důvodů jejího nutného opakování ve smyslu odst. 9 tohoto článku smlouvy či jiných vad bránících akceptaci překročí termín uvedený v čl. III. odst. 1 této smlouvy, bude se jednat o prodlení poskytovatele s plněním Dodávky.
12. V souladu s čl. IV. odst. 5 smlouvy je poskytovatel povinen poskytnout objednateli veškeré Licence k autorským dílům tvořícím součást Dodávky (či s touto Dodávkou souvisejících) nejpozději v den podpisu akceptačního protokolu Dodávky. Přede dnem podpisu akceptačního protokolu Dodávky je objednatel oprávněn užívat autorská díla dle předešlé věty v rozsahu nezbytně nutném k provedení akceptační procedury dle tohoto článku smlouvy a k ověření kvality plnění poskytovatele.
13. Není-li touto smlouvou stanoveno jinak, je poskytovatel nejpozději v den podpisu akceptačního protokolu jednotlivého dílčího plnění povinen předat objednateli Dokumentaci, včetně provozní, uživatelské a administrátorské dokumentace k dílčímu plnění.

VI.
Cena a platební podmínky

1. Cena za Dodávku dle této smlouvy je cenou smluvní, nejvýše přípustnou, nepřekročitelnou a činí 15.090.000,- Kč bez DPH, samostatně DPH ve výši 3.168.900,- Kč, tj. celkem 18.258.900,- Kč včetně DPH (dále jen „**cena za Dodávku**“).
2. Cena za Dodávku zahrnuje veškeré náklady poskytovatele spojené s Dodávkou a zahrnují zejména veškeré Licence vztahující se k či související s příslušnou částí Dodávky, základní záruku, a dále veškeré služby, které budou poskytovatelem k Dodávce či v souvislosti s Dodávkou poskytovány. Cenu je možné změnit pouze v případě změny sazby DPH. Poskytovatel prohlašuje, že všechny technické, finanční, věcné a ostatní podmínky pro splnění závazků z této smlouvy zahrnul do kalkulace ceny. Poskytovatel výslovně prohlašuje, že součástí ceny jsou i veškeré náklady spojené se splněním podmínek pro splnění závazků z této smlouvy dle obecně závazných právních předpisů.
3. Cena za servisní podporu dle přílohy č. 1 této smlouvy, je cenou smluvní, nejvýše přípustnou, nepřekročitelnou a činí 15.000,- Kč bez DPH za 1 měsíc, samostatně DPH ve výši 3.150,- Kč, tj. celkem 18.150,- Kč včetně DPH (dále jen „**cena za servisní podporu**“). Cena za servisní podporu zahrnuje veškeré náklady poskytovatele spojené se splněním jeho závazku z této smlouvy, zejména přílohy č. 1. Cenu je možné změnit (s

výjimkou odst. 4 tohoto článku smlouvy) pouze v případě změny sazby DPH. Poskytovatel prohlašuje, že všechny technické, finanční, věcné a ostatní podmínky pro splnění závazků z této smlouvy zahrnul do kalkulace ceny. Poskytovatel výslovně prohlašuje, že součástí ceny jsou i veškeré náklady spojené se splněním podmínek pro splnění závazků z této smlouvy dle obecně závazných právních předpisů.

4. Vícepráce i vícenáklady, které vzniknou poskytovateli z důvodu poskytnutí nekvalitních služeb či služeb poskytnutých v rozporu se smlouvou či jejími přílohami, nejsou součástí ceny a hradí je poskytovatel v plné výši.
5. Cena zahrnuje veškeré činnosti poskytovatele a požadavky objednatele, uvedené v příloze č. 1 smlouvy.
6. Objednatel nebude poskytovat žádné zálohové platby.
7. Úhrada ceny bude provedena po poskytnutí služeb v české měně nebo v měně platné v České republice na základě řádného daňového dokladu (dále jen jako „**faktura**“), kterou je poskytovatel povinen vystavit nejpozději do 10. kalendářního dne následujícího měsíce. Poslední den uplynulého kalendářního měsíce je datem uskutečnění zdanitelného plnění. Splatnost faktury je smluvními stranami dohodnuta na 30 (třicet) kalendářních dnů ode dne řádného doručení faktury objednateli.
8. Podkladem a podmínkou pro vystavení řádné faktury za Dodávku dle odst. 1 tohoto článku smlouvy bude objednatelem podepsaný akceptační protokol s výrokem „Akceptováno bez výhrad“; podkladem a podmínkou pro vystavení řádné faktury za servisní podporu dle odst. 2 tohoto článku smlouvy bude objednatelem potvrzený report příslušného kalendářního pololetí, který bude ze strany poskytovatele předáván 1x za pololetí, vždy za celé ukončené kalendářní pololetí zpětně, a musí obsahovat minimálně název projektu, registrační číslo projektu, číslo reportu, období, datum činnosti, konkrétní popis činnosti, identifikační údaje poskytovatele a dále výpis všech záznamů Hotline a Helpdesk z dotčeného pololetí a jejich stav vyřízení poskytovatelem, souhrnné informace ohledně dodržování garance provozu (SLA) za dotčené pololetí. Tento report bude přílohou faktury.
9. V případě, že budou služby poskytovány jen po část kalendářního pololetí, bude poměrně zkrácena příslušná fakturace za poskytování služeb.
10. Stane-li se v průběhu trvání smlouvy Česká republika členem Evropské měnové unie a bude-li v závazně stanoven koeficient pro přepočet CZK na EUR, budou ceny sjednané v CZK přepočteny do EUR na základě odpovídajícího koeficientu sjednaného v mezinárodních úmluvách, kterými bude Česká republika vázána, jakož i v souladu s případnou tomu odpovídající vnitrostátní právní úpravou České republiky.
11. Faktury vystavené poskytovatelem musí obsahovat všechny náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“), a dle § 435 občanského zákoníku vč. označení smlouvy, ke které se vztahuje. Faktura bude dále obsahovat náležitosti vyplývající z režimu spolufinancování Projektu ze strukturálních fondů Evropské unie, zejména registrační číslo projektu CZ.06.3.05/0.0/0.0/16_044/0006323, název projektu „Modernizace infrastruktury pro sdílení informací a dat s obcemi Pardubického kraje“ a informaci o tom, že Projekt je spolufinancován z Evropského fondu pro regionální rozvoj, Integrovaného operačního

programu (IROP)včetně povinných parametrů publicity, dále cenu bez DPH, sazbu DPH a cenu vč. DPH.

12. Nebude-li faktura obsahovat veškeré náležitosti podle zákona o DPH, občanského zákoníku nebo podle jiných obecně platných právních předpisů nebo bude-li v rozporu s podmínkami stanovenými smlouvou, nebo bude-li chybně vyúčtována cena nebo DPH, je objednatel oprávněn fakturu poskytovateli vrátit s pokyny k její opravě. V takovém případě splatnost faktury nezačala běžet a splatnost nové opravné faktury počne běžet od samého počátku až prvním dnem po jejím doručení objednateli.
13. Povinnost uhradit cenu za poskytnuté služby je splněna dnem odepsání příslušné částky z účtu objednatele ve prospěch účtu poskytovatele. Všechny poukazované částky vzájemně stranami na základě smlouvy musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů spojených s převodem na jejich účty.
14. Objednatel uhradí přijatou fakturu pouze na bankovní účty poskytovatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH. V případě, že poskytovatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí objednatel poskytovateli pouze základ daně, přičemž DPH uhradí poskytovateli až po zveřejnění příslušného účtu poskytovatele v registru plátců a identifikovaných osob poskytovatelem.
15. Poskytovatel prohlašuje, že správce daně před uzavřením smlouvy nerozhodl, že poskytovatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „nespolehlivý plátce“). V případě, že správce daně rozhodne o tom, že poskytovatel je nespolehlivým plátcem, zavazuje se poskytovatel o tomto informovat objednatele do 2 (slovy: dvou) pracovních dní. Stane-li se poskytovatel nespolehlivým plátcem nebo dojde k některé ze skutečností předvídaných v § 109 zákona o DPH, uhradí objednatel poskytovateli pouze základ daně, přičemž DPH je objednatel oprávněn uhradit přímo příslušnému správci daně, přičemž tato úhrada se považuje za řádné splnění povinnosti zaplatit cenu dle smlouvy. O úhradě DPH přímo příslušnému správci daně je objednatel povinen poskytovatele písemně informovat.

VII.
Práva a povinnosti stran, prohlášení stran

1. Poskytovatel se zavazuje:
   a) poskytovat Dodávku podle této smlouvy a služby servisní podpory vlastním jménem, na vlastní odpovědnost a v souladu s pokyny objednatele řádně a včas, zejména se zohledněním délky trvání akceptační procedury;
   b) poskytovat Dodávku dle této smlouvy výhradně s využitím nového, nerepasovaného zboží, které pochází z oficiálního distribučního kanálu výrobce dodávaného zařízení a je určeno pro trh v České republice;
   c) poskytovat Dodávku dle této smlouvy spočívající v instalaci a veškeré konzultační, servisní či obdobné činnost vztahující se k dodanému HW či SW členy realizačního týmu, které uvedl v příloze č. 4 Zadávací dokumentace;

d) poskytovat plnění podle této smlouvy s péčí řádného hospodáře odpovídající podmínkám sjednaným v této smlouvě a s procesy „best practice“, za dodržování obecně závazných právních předpisů;
e) upozorňovat objednatel včas na všechny hrozící vady či výpadky svého plnění, jakož i poskytovat objednateli veškeré informace, které jsou pro plnění smlouvy nezbytné;
f) neprodleně oznámit písemnou formou objednateli překážky, které mu brání v plnění předmětu smlouvy a výkonu dalších činností souvisejících s plněním předmětu smlouvy;
g) upozornit objednatele na potenciální rizika vzniku škod a včas a řádně dle svých možností provést taková opatření, která riziko vzniku škod zcela vyloučí nebo sníží;
h) informovat objednatele o plnění svých povinností podle této smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností smluvních stran;
i) zajistit, aby všechny osoby podílející se na plnění jeho závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci a veškeré interní předpisy objednatele, s nimiž objednatel poskytovatele obeznámil;
j) chránit osobní údaje, data a duševní vlastnictví objednatele a třetích osob;
k) upozorňovat objednatele v odůvodněných případech na případnou nevhodnost pokynů objednatele.

2. Poskytovatel se v oblasti služby servisní podpory zavazuje:

a) Služby servisní podpory budou poskytovány v lokalitách, na dodaném zařízení a v rozsahu a dle specifikace uvedené v této Smlouvě a v příloze č. 1 této Smlouvy.

b) Poskytovatel se zavazuje udržovat po celou dobu poskytování služeb dostupnost dodaného zboží v parametrech SLA, které je specifikováno v Příloze č. 1 této Smlouvy, a v takovém stavu, aby její garantované i standardní parametry odpovídali Akceptačnímu protokolu Dodávky, a objednatel se zavazuje poskytnout k tomu veškerou potřebnou součinnost.

c) Poskytovatel zaručuje a zajišťuje objednateli nepřetržité poskytování služby (nepřetržitý provoz předmětu Dodávky a dostupnost této služby 24 hodin denně, sedm dní v týdnu po celý kalendářní rok), s maximální dobou nedostupnosti stanovenou v tomto článku a v příloze č. 1 této smlouvy.

d) Pro určení dostupnosti se použije následující vzorec:

Měsíční dostupnost (v %) = [(počet hodin v měsíci) – (součet trvání všech poruch v měsíci)] x 100 (počet hodin v měsíci)

(Přičemž počet hodin v měsíci se stanoví podle skutečného počtu dní v měsíci vynásobeného číslovkou 24 např. 30 dnů x 24 = 720 hodin)

Za nedostupnost, tedy poruchu, se považuje i poskytování služby s horšími než garantovanými parametry, dohodnutými v Akceptačním protokolu Dodávky a dále v Příloze č. 1 této Smlouvy.

e) Plánované výpadky se nezapočítávají do doby dostupnosti podle odst. c) a d) tohoto článku smlouvy. Poskytovatel se zavazuje, že celková doba plánovaných výpadků v každém kalendářním měsíci nepřesáhne procentuální hodnotu uvedenou v příloze č. 1 smlouvy, smluvní strany se mohou v konkrétním případě písemně dohodnout jinak. Poskytovatel se dále zavazuje, že bude plánované práce na trase, které si vyžádají nedostupnost, provádět pokud možno v době mimo pracovní špičku, tedy zejména v nočních hodinách (0:00-6:00h) a ve dnech pracovního volna a klidu.

f) Poskytovatel je povinen plánované výpadky písemně oznámit objednateli nejméně 5 pracovních dnů předem. Pokud tuto povinnost nedodrží, počítá se doba plánovaného výpadku do doby nedostupnosti, pokud se smluvní strany nedohodnou v konkrétním případě jinak.

g) Do doby nedostupnosti se dále nezapočítává doba, kdy nedostupnost bude prokazatelně způsobena důvody ležícími na straně objednatele (např. poruchy na zařízení objednatele, neposkytnutí nezbytné součinnosti, kterou poskytovatel sám nemůže zajistit, apod.) a z důvodů, které poskytovatel objektivně nemohl ovlivnit, včetně událostí vyšší moci. Za začátek nedostupnosti se pro určení doby jejího trvání považuje čas jejího ohlášení objednatelem (nebo jím určenou třetí osobou) způsobem podle odst. h) tohoto článku smlouvy nebo zjištěním nedostupnosti poskytovatelem a zavedením požadavku do servicedesku za objednatele.

h) Služby servisní podpory budou dle jejich parametrů uvedených v Příloze č. 1 této Smlouvy poskytovány buď samostatně na základě pravidelné činnosti (tj. bez výslovného pokynu či objednávky ze strany objednatele), nebo na základě požadavku objednatele, který objednatel uplatní prostřednictvím aplikace helpdesk / servicedesk dostupné na adrese https://acservicedesk.autocont.cz nebo telefonicky na telefonním čísle + 420 251 022 552, záložní mobilní telefon + 420 606 026 248. Poskytovatel potvrdí přijetí ohlášení Objednatele do času dle nahlášené kategorie incidentu (viz Příloha č. 3 této Smlouvy) od přijetí incidentu/vady a to prostřednictvím aplikace helpdesk / servicedesk nebo e-mailem na adresu sd_vc@autocont.cz . Minimální obsah nahlašovaného incidentu/vady bude součástí Provozní a bezpečnostní dokumentace.

i) Objednatel nebo jím pověřená třetí strana proveden první identifikaci příčiny incidentu a nejčastěji i prvotní zásah k jejímu odstranění. V negativním případě je pak Objednatel nebo jím určená třetí strana povinna vyplnit hlášení minimálně v požadované struktuře (určené Provozní a bezpečnostní dokumentací) a uvést v něm telefonické spojení na jeho oprávněného zástupce pro možnost vyžádání doplňujících informací ze strany poskytovatele.

j) Služba Telefonická podpora (hot-line) je poskytována poskytovatelem na tel. č.: + 420 251 022 552, záložní mobilní telefon + 420 606 026 248.

k) Poskytovatel určuje a plně zodpovídá za stanovení způsobu odstranění incidentu/vady, za stanovení posloupnosti jednotlivých činností a za stanovení doby, kdy tyto činnosti budou prováděny. K tomu je Objednatel povinen poskytnout potřebnou součinnost. V případě, kdy Objednatel nezabezpečí poskytovatelem požadovanou součinnost (zpřístupnění servisovaných zařízení, poskytnutí potřebných informací, provozních dat, konfigurací apod.) a Poskytovatel si nemůže tuto součinnost zařídit jinak, je Poskytovatel povinen zaznamenat k záznamu poruchy čas nesoučinnosti a posléze jejího obnovení. Doba prodlení do obnovení součinnosti se tak do doby trvání poruchy (a tím i výpočtu doby nedostupnosti) nepočítá. Musel-li však poskytoval neprodleně a nutně zasáhnout a nemohl-li vyčkat součinnosti Objednatele (např. ohrožení majetku či života), je Objednatel povinen uhradit poskytovateli zvýšené náklady spojené s takovýmto odstraněním poruchy.

l) Poskytovatel má právo použít k plnění předmětu smlouvy třetích subjektů, odpovídá však, jako by plnil sám.

m) Po provedení servisní činnosti bude pověřenými zástupci Poskytovatele sepsán a Objednatelem potvrzen „Protokol o provedení servisní činnosti“ jako součást nahlášeného incidentu v ServiceDesku Poskytovatele, jehož vzor je přílohou č. 4 této smlouvy.

n) K omezení nebo rozšíření rozsahu servisní činnosti v důsledku omezení nebo rozšíření rozsahu servisovaného zařízení může dojít pouze dohodou smluvních stran a musí být v souladu s podmínkami stanovenými v ZZVZ. Dohoda musí být písemná a bude mít formu dodatku k této smlouvě.

o) Pokud dojde k druhé a další poruše služby/prvku za kalendářní rok v důsledku prokázaného úmyslného nebo nedbalostního porušení nebo nedodržení provozních či záručních podmínek ze strany Objednatele, jeho zaměstnanců nebo třetích osob (zaviněná porucha) nebo v důsledku vnějších událostí, které nezpůsobil Poskytovatel (např. vandalství, terorismus, válka, občanské nepokoje, požáry, povodně a jiné živelné události, výbuchy, úniky chemických a radioaktivních materiálů a podobně), je Objednatel povinen uhradit Poskytovateli vedle ceny uvedené v čl. VI. odst. 3 této Smlouvy i náklady na práci servisního technika, cenu spotřebovaného materiálu a náhradních dílů, jakož i všechny ostatní účelně vynaložené náklady spojené s provedením servisní činnosti, a to podle aktuálního ceníku poskytovatele ke dni vyúčtování. Bezplatné vyřešení prvního výskytu poruchy v roce každého typu zavinění (objednatel, třetí strana, vyšší moc) je součástí předmětu plnění.

p) Poskytovatel je povinen postupovat při plnění této smlouvy s odbornou péčí; zavazuje se při plnění předmětu smlouvy a poskytování služeb postupovat poctivě, pečlivě a s odbornou péčí, jak je vymezena v § 5 odst. 1 občanského zákoníku s použitím každého

prostředku, kterého vyžaduje povaha služeb, podle pokynů objednatele a v souladu s jeho zájmy, které jsou poskytovateli známy nebo je musí znát či předpokládat.

3. Poskytovatel prohlašuje, že:

   a) není jako právnická osoba v likvidaci;

   b) není proti němu vedeno konkursní řízení ani vyrovnací řízení ve smyslu zákona č. 328/1991 Sb., o konkursu a vyrovnání, ve znění pozdějších předpisů, popř. zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů a takové řízení nebylo zastaveno či zrušeno z důvodu nedostatku majetku poskytovatele a dále není předlužen či neschopen plnit své splatné závazky vůči svým věřitelům;

   c) uzavření/m této smlouvy:

   - neporuší správní rozhodnutí orgánu státní správy České republiky či rozhodnutí soudů České republiky;
   - neporuší ustanovení žádné dohody, smlouvy či jiného ujednání, které uzavřel se třetí osobou;
   - neučinil nic, ať již sám anebo za spolupráce či prostřednictvím třetí osoby, co by omezilo či znemožnilo dosažení účelu této smlouvy.

4. Poskytovatel se zavazuje, že objednateli bezodkladně po vzniku takové skutečnosti písemně oznámí:

   a) podání návrhu na prohlášení konkursu na majetek poskytovatele dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů; nebo
   b) podání návrhu na vyrovnání na majetek poskytovatele dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů; nebo
   c) vstup poskytovatele do likvidace; nebo
   d) splnění podmínek prohlášení konkursu na majetek poskytovatele, tj. zejména že poskytovatel je předlužen anebo insolventní; nebo
   e) rozhodnutí o provedení přeměny poskytovatele, zejména fúzí, převodem jmění na společníka či rozdělením, provedení změny právní formy poskytovatele či provedení jiných organizačních změn; nebo
   f) omezení či ukončení činnosti poskytovatele, která bezprostředně souvisí s předmětem této smlouvy; nebo
   g) všechny skutečnosti, které by mohly mít vliv na přechod či vypořádání závazků poskytovatele vůči objednateli vyplývajících z této smlouvy či s touto smlouvou souvisejících; nebo
   h) rozhodnutí o zrušení poskytovatele.

5. Poskytovatel prohlašuje, že před podpisem této smlouvy řádně překontroloval veškeré podklady a dokumentaci a řádně prověřil místní podmínky a všechny nejasné podmínky pro poskytování služeb si vyjasnil s objednatelem nebo místním šetřením.

6. Poskytovatel se zavazuje mít po celou dobu trvání smluvního vztahu sjednané pojištění odpovědnosti za škodu způsobenou třetí osobě s limitním plněním na jednu škodnou událost v minimální výši 8.000.000 Kč.

7. Poskytovatel je povinen spolupůsobit při výkonu finanční kontroly ve smyslu § 2 písm. e) a § 13 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonu (dále jen „zákon o finanční kontrole“), ve znění pozdějších předpisů, tj. poskytnout kontrolnímu orgánu doklady o dodávkách zboží a služeb hrazených z veřejných výdajů nebo z veřejné finanční podpory v rozsahu nezbytném pro ověření příslušné operace. Tutéž povinnost bude poskytovatel povinen požadovat po svých dodavatelích.
8. Poskytovatel je povinen archivovat originální vyhotovení smlouvy včetně jejích dodatků, originály účetních dokladů (a jejich příloh) a dalších dokladů vztahujících se k realizaci předmětu této smlouvy po dobu 10 let od ukončení projektu, minimálně však do 31. 12. 2030. Po tuto dobu je poskytovatel povinen umožnit osobám oprávněným k výkonu kontroly projektů provést kontrolu dokladů souvisejících s plněním této smlouvy.
9. Veškeré materiály vztahující se k projektu (dokumenty, smlouvy, prezenční listiny, publikace, prezentace atd.), nebo vzniklé v rámci projektu musí být označeny v souladu s Obecnými a/nebo Specifickými pravidly IROP. Vedle toho objednatel požaduje, aby povinná publicita všech materiálů, které vzniknou v rámci plnění projektu, byla vždy předem odsouhlasena určeným zaměstnancem objednatele jako realizátora projektu.

VIII.
Ochrana informací, osobních údajů a bezpečnost informací

1. Smluvní strany jsou si vědomy toho, že v rámci plnění této smlouvy:
   a) si mohou vzájemně úmyslně nebo i opominutím poskytnout informace, které budou považovány za důvěrné (dále „**důvěrné informace**“),
   b) mohou jejich zaměstnanci získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.
2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou plnění této smlouvy se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění této smlouvy.
3. Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. např. popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu.

4. Pokud jsou důvěrné informace poskytovány v písemné podobě nebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.
5. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:
   a) se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,
   b) měla přijímající strana legálně k dispozici před uzavřením této smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
   c) jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
   d) po podpisu této smlouvy poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.
6. Poskytovatel je povinen při poskytování plnění podle této smlouvy dodržovat zásady bezpečnosti informací a dat včetně osobních údajů (dále v tomto odstavci jen „bezpečnost informací“), jakož i zásady ochrany osobních údajů stanovených GDPR, přičemž bezpečností informací se rozumí zajišťování důvěrnosti, integrity a dostupnosti informací, které jsou uchovávány, vytvářeny nebo zpracovávány prostřednictvím prvků Dodávky, a to v přiměřeném rozsahu.
7. Poskytovatel je povinen při plnění svých povinností podle této smlouvy s odbornou péčí poskytovat objednateli veškerou součinnost nezbytnou k tomu, aby objednatel řádně naplňoval právní povinnosti stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZoKB“), a jeho prováděcími předpisy. Poskytovatel je zejména povinen poskytovat objednateli součinnost k zavádění, provádění, revidování a aktualizaci odpovídajících bezpečnostních opatření stanovených objednatelem za účelem zajištění souladu se ZoKB a jeho prováděcími předpisy. Jestliže vznikne v souvislosti s povinnostmi podle tohoto odstavce potřeba uzavřít dodatek k této smlouvě nebo zvláštní smlouvu, zavazuje se poskytovatel poskytnout objednateli veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy v souladu se ZZVZ.
8. Ustanovení tohoto článku není dotčeno ukončením této smlouvy z jakéhokoliv důvodu po dobu dalších 5 let.

IX.
Součinnost a vzájemná komunikace

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

3. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob, které si smluvní strany za tímto účelem sdělí, statutárních orgánů smluvních stran, popř. jimi písemně pověřených pracovníků.

X.
Záruka

1. Poskytovatel poskytuje záruku (včetně záruky výrobce na dodaný HW), že každá část Dodávky má ke dni její akceptace funkční vlastnosti stanovené touto smlouvou, a je způsobilá k použití pro účely stanovené v této smlouvě nebo v souladu s touto smlouvou.
2. Poskytovatel poskytuje záruku každé jednotlivé části Dodávky od okamžiku její akceptace s výrokem „Akceptováno bez výhrad“ po dobu 60 měsíců.
3. Objednatel, případně jím zmocněná třetí strana, je oprávněn vady Dodávky nahlásit poskytovateli kdykoli v průběhu záruční doby (základní či rozšířené) bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.
4. Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.
5. Podrobnosti požadované záruky jsou uvedeny v příloze č. 1 této smlouvy.

XI.
Sankce

1. V případě prodlení poskytovatele s předáním Dodávky a s poskytnutím Licencí v termínu dle čl. III. odst. 1 smlouvy vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 50.000,- Kč za každý i započatý den prodlení.
2. V případě prodlení poskytovatele s dodržením garantovaných reakčních dob (dob opravy) dle SLA k jednotlivým službám servisní podpory dle Přílohy č. 1 této smlouvy vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 2.000,- Kč za každou i započatou hodinu prodlení s takovým plněním, je-li garantovaná reakční doba (doba opravy) stanovena v hodinách.
3. V případě, že byla porušena touto smlouvou garantovaná dostupnost funkcí předmětu plnění dle SLA uvedené v přílohách této Smlouvy a vypočítaná za fakturované období, vzniká objednateli nárok na zaplacení smluvní pokuty 10.000Kč za každých i započatých 0,1% hodnoty dostupnosti pod smluvně stanovenou hodnotu.
4. V případě, že poskytovatel bude k poskytování Dodávky využívat členy realizačního týmu nebo poddodavatele v rozporu s ustanoveními čl. II. odst. 4 této smlouvy, vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 50.000,- Kč za každý jednotlivý případ takového porušení smlouvy.
5. V případě, že poskytovatel poruší svou povinnost čl. VII. odst. 1 písm. b) smlouvy poskytovat Dodávku dle této Smlouvy výhradně s využitím nového, nerepasovaného zboží, které pochází z oficiálního distribučního kanálu výrobce dodávaného zařízení a je určeno pro trh v České republice, vzniká objednateli nárok na zaplacení smluvní pokuty ve výši 10.000,- Kč za každý komponent tvořící součást Dodávky, který nesplňuje uvedené podmínky.

7. V případě, že objednatel je v prodlení s úhradou ceny za Dodávku nebo ceny za servisní podporu, je povinen uhradit poskytovateli úrok z prodlení v zákonné výši, a to z dlužné částky.
8. Smluvní pokuty a úrok z prodlení jsou splatné do 30 dnů od doručení jejich vyúčtování oprávněnou smluvní stranou straně povinné. Platby budou provedeny bezhotovostním bankovním převodem na účet oprávněné smluvní strany.
9. Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši. Pokud není v ostatních ustanoveních smlouvy uvedeno jinak, zaplacení smluvní pokuty poskytovatelem objednateli nezbavuje poskytovatele závazku splnit povinnosti dané mu smlouvou.
10. Každá ze stran smlouvy nese odpovědnost za prodlení, za vady a způsobenou škodu plynoucí z porušení smlouvy a obecně závazných právních předpisů, zejména občanského zákoníku. Žádná ze stran smlouvy nebude odpovědná za škodu způsobenou v důsledku okolností vylučujících odpovědnost ve smyslu občanského zákoníku. Smluvní strany se zavazují upozornit druhou stranu bez zbytečného odkladu na jakékoliv okolnosti bránící řádnému plnění smlouvy a zavazují se k maximálnímu úsilí k jejich odvrácení a překonání.

XII.
Platnost a účinnost smlouvy, její ukončení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího vložení do registru smluv a uzavírá se na dobu určitou potřebnou pro splnění všech povinností dle této smlouvy. Ukončením účinnosti této smlouvy nejsou dotčena ustanovení smlouvy týkající se převodu vlastnického práva, nároků z odpovědnosti za vady, nároků plynoucích ze záruky, nároků z odpovědnosti za škodu a nároků ze smluvních pokut, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této smlouvy.
2. Objednatel je oprávněn od smlouvy odstoupit zejména v případě podstatného porušení smluvní nebo zákonné povinnosti poskytovatelem.
3. Za podstatné porušení povinnosti se považuje zejména:
   a) prodlení poskytovatele s předáním jakéhokoliv dílčího plnění po dobu delší než 10 dnů oproti termínu plnění stanovenému ve smlouvě nebo na základě této smlouvy;
   b) opakované nedodržení alespoň jednoho ze sledovaných parametrů SLA u Služeb, přičemž nedodržení se považuje za opakované, pokud za posledních 6 měsíců nastalo alespoň dvakrát;
   c) opakované případy využívání členů realizačního týmu nebo poddodavatelů poskytovatelem v rozporu s ustanovením čl. II. odst. 4 smlouvy, přičemž za opakované se považuje, pokud za posledních 3 měsíce nastalo alespoň dvakrát;
   d) vyjde najevo, že poskytovatel není z jakéhokoliv důvodu neležícího na straně objednatele schopen plnit dál své závazky z této smlouvy.;
   e) jestliže bude poskytovatelem podán návrh na prohlášení konkursu na vlastní majetek ve smyslu ustanovení zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve

znění pozdějších předpisů nebo bude prohlášen konkurs na majetek poskytovatele na základě návrhu věřitele poskytovatele či bude na základě rozhodnutí soudu ustanoven předběžný správce konkursní podstaty pro poskytovatele ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších právních předpisů nebo bude poskytovatelem podán návrh na vyrovnání ve smyslu ustanovení zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů,

f) případ, kdy se prohlášení poskytovatele uvedené v příloze č. 5 zadávací dokumentace na veřejnou zakázku uvedenou v odst. 2 preambule smlouvy ukáže jako nepravdivé, a to kdykoliv po dobu trvání této smlouvy, nebo

g) poskytovatel vstoupil do likvidace.

4. Každá smluvní strana je oprávněna odstoupit od smlouvy též v případě prodlení druhé strany s plněním závazků podle této smlouvy po dobu delší než třicet (30) dnů, pokud druhá smluvní strana nezjedná nápravu ani v dodatečné přiměřené lhůtě, která jí byla smluvní stranou poskytnuta na základě písemné výzvy ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než patnáct (15) dnů od doručení takovéto výzvy.

5. Účinky odstoupení od smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

6. V případě odstoupení od smlouvy má objednatel právo rozhodnout, zda si rozpracované plnění ponechá. Rozpracovaným plněním se myslí Dodávka jako celek až do okamžiku jejího řádného převzetí objednatelem. V případě, že si objednatel rozpracované plnění ponechá, náleží poskytovateli cena, na kterou má nárok podle smlouvy, ponížená o to, co poskytovatel ušetřil neprovedením Dodávky v plném rozsahu. V případě, že objednatel nebude mít zájem ponechat si rozpracované plnění, má poskytovatel nárok na náhradu účelně vynaložených nákladů na provedení Dodávky do doby doručení odstoupení od smlouvy.

XIII.
Doručování

1. Smluvní strany této smlouvy se dohodly následujícím způsobem na adrese pro doručování písemné korespondence, pokud není smlouvou stanoveno jinak:

   a) adresa pro doručování objednateli je: Pardubický kraj Komenského nám. 125; 532 11 Pardubice, IDDS: z28bwu9.

   b) adresa pro doručování poskytovateli je: AUTOCONT a.s., Hornopolní 3322/34, 702 00 Ostrava, IDDS: ctb7phe

2. Veškerá podání a jiná oznámení, která se doručují smluvním stranám, je třeba doručit datovou schránkou, osobně, nebo doporučenou listovní zásilkou s doručenkou, pokud není ve smlouvě stanoveno jinak.

3. Aniž by tím byly dotčeny další prostředky, kterými lze prokázat doručení, má se za to, že oznámení bylo řádně doručené třetím dnem po jeho odeslání v případě, že bylo odesláno prostřednictvím držitele poštovní licence.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

XIV.
Závěrečná ustanovení

1. Smluvní strany prohlašují, že žádná část smlouvy nenaplňuje znaky obchodního tajemství ve smyslu § 504 občanského zákoníku.
2. Smluvní strany berou na vědomí, že nebude-li smlouva zveřejněna ani do tří měsíců od jejího uzavření, je následujícím dnem zrušena od počátku.
3. Smluvní strany této smlouvy se dohodly, že právní vztahy založené touto smlouvou se budou řídit právním řádem České republiky. Tato smlouva jakož i právní vztahy touto smlouvou neupravené se řídí občanským zákoníkem.
4. Případné spory vzniklé z této smlouvy budou řešeny dohodou smluvních stran a nebude-li dohody, pak podle platné právní úpravy věcně a místně příslušnými soudy České republiky.
5. V případě neplatnosti nebo neúčinnosti některého ustanovení této smlouvy nebudou dotčena ostatní ustanovení této smlouvy.
6. Smluvní strany se dohodly, že v případě zániku právního vztahu založeného touto smlouvou zůstávají v platnosti a účinnosti i nadále ustanovení, z jejichž povahy vyplývá, že mají zůstat nedotčena zánikem právního vztahu založeného touto smlouvou.
7. Právní jednání bylo schváleno dne 26. 9. 2022 Radou Pardubického kraje usnesením R/1246/22.
8. Tuto smlouvu lze měnit, doplňovat a upřesňovat pouze oboustranně odsouhlasenými, písemnými a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou smluvních stran.
9. Tato smlouva je v souladu § 211 odst. 3 zákona č. 134/2016 Sb. o zadávání veřejných zakázek ve znění pozdějších předpisů ve spojení se zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, uzavřena elektronicky.
10. Obě smluvní strany potvrzují autentičnost této smlouvy a prohlašují, že si smlouvu včetně příloh přečetly, s jejím obsahem (včetně příloh) souhlasí, že smlouva byla sepsána na základě pravdivých údajů, z jejich pravé a svobodné vůle a nebyla uzavřena v tísni ani za jinak jednostranně nevýhodných podmínek, což stvrzují svým podpisem, resp. podpisem svého oprávněného zástupce.
11. Nedílnou součást této smlouvy tvoří:
    - Příloha č. 1 – Specifikace předmětu plnění
    - Příloha č. 2 – Vzor akceptačního protokolu
    - Příloha č. 3 – Vzor hlášení poruchy
    - Příloha č. 4 – Protokol o provedení servisní činnosti

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

V Pardubicích

JUDr. Martin Netolický Ph.D.
hejtman Pardubického kraje

V Praze: dle elektronického podpisu

[redacted]

Ondřej Matuštík
člen představenstva AUTOCONT a.s.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Příloha č. 1 smlouvy

Specifikace předmětu plnění

MODERNIZACE INFRASTRUKTURY PRO SDÍLENÍ INFORMACÍ A DAT S OBCEMI PARDUBICKÉHO KRAJE

Technická specifikace pro veřejnou zakázku - Bezpečnostní modul a jeho služby

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

1. Obsah

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

2. Pojmy

Lokalita – území obce/města

Uzel – zájmový bod Pardubického kraje, aktivní prvek (PE či CPE) nebo optické zakončení v majetku nebo pronájmu Pardubického kraje poskytující své služby v daném místě

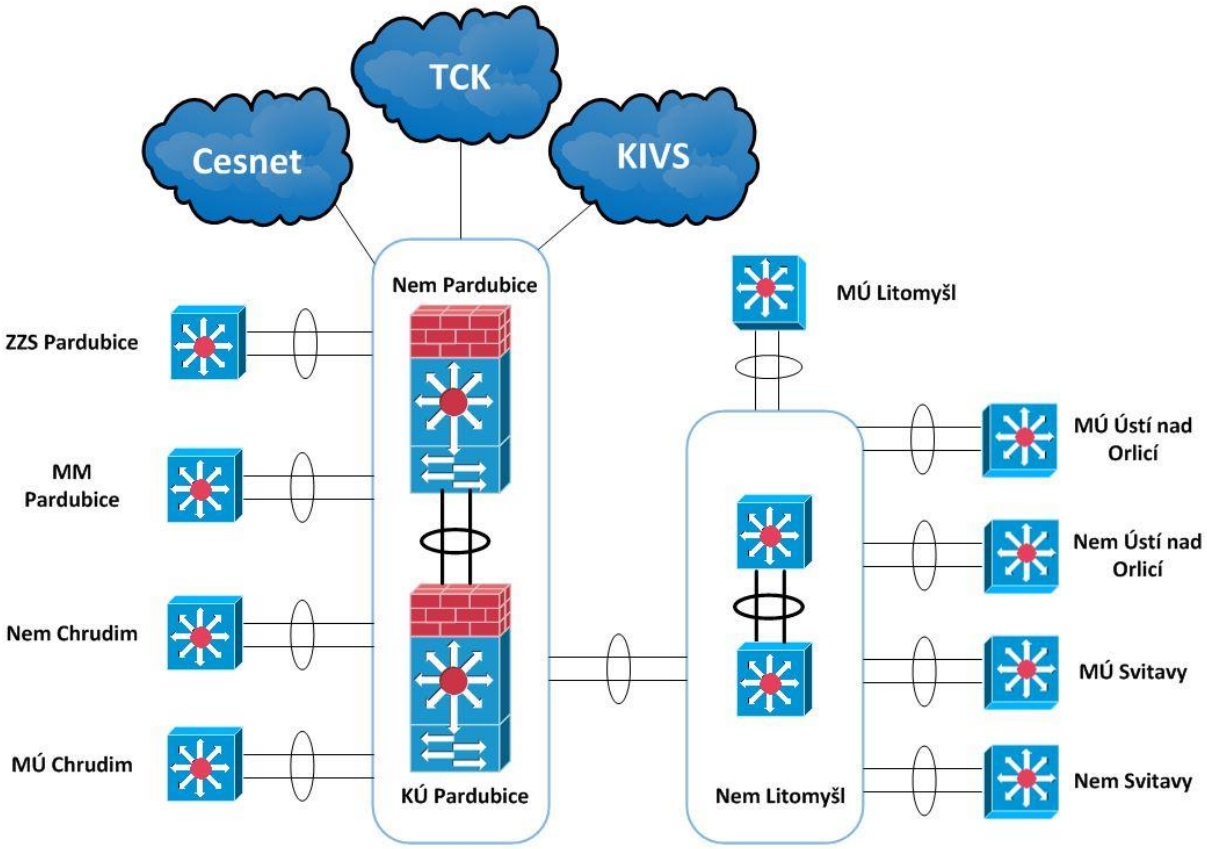
SLA – service level agreement – úroveň servisní podpory, případně v procentech požadovaná dostupnost u dodavatelem spravované části

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

3. Výchozí situace – popis aktuálního stavu

Výchozí stav sítě včetně jeho služeb podporující eGovernment a eHealth na území Pardubického kraje vznikl v rámci IOP projektu „Regionální datová síť Pardubického kraje“.



Obrázek č. 1 – Současná topologie Regionální datové sítě

Vzniklá síť, spuštěná v září 2015, propojila celkově 12 uzlů v 5 lokalitách obcí s rozšířenou působností a v současnosti se svými napojením na Technologické centrum kraje, na krajské konektory sítě ITS-NGN a akademickou síť CESNET tvoří páteř Regionální datové sítě LabeNET.

Jádro sítě tvoří tři fyzické uzly propojené mezi sebou jako dva logické celky, jeden logický uzel centrální v datových centrech Nemocnice a Krajského úřadu v Pardubicích a druhý agregační v Nemocnici Litomyšl, které jsou propojeny optickou linkou o celkové instalované kapacitě 6x1Gbps. Centrální i agregační uzly jsou osazeny dvojicí zařízení, propojovací linka mezi nimi je optický pár, rozdělený na dva svazky pouze logicky technologií CWDM. Uzly v ostatních lokalitách jsou připojeny k oběma prvkům v centrálním nebo agregačním uzlu nezálohovanou optickou

linkou, která je pomocí WDM rozdělena na dvě logické linky 1 Gbps – logicky jde o topologii dvojité rozvětvené hvězdy. Celá síť je tak z hlediska topologie uzlově neredundantní, logicky jsou linky redundantní, fyzicky však ne.

Některé služby provozované sítí LabeNET, jsou využívány také v režimu 24x7.

Tabulka č. 1 - Uzly Regionální datové sítě 1.0

Typ lokality	Adresa
Datové centrum	Pardubická krajská nemocnice, a.s. Kyjevská 44, 532 03 Pardubice
Agregační lokalita	Litomyšlská nemocnice, a.s. J. E. Purkyně 652, 570 14 Litomyšl
Koncová lokalita	Chrudimská nemocnice, a.s. Václavská 570, 537 27 Chrudim
Koncová lokalita	Orlickoústecká nemocnice, a.s. Čs. armády 1076, 562 18
Koncová lokalita	Svitavská nemocnice, a.s., Kolárova 7, 568 02 Svitavy
Koncová lokalita	Zdravotnická záchranná služba Pardubického kraje, Průmyslová 450, 530 03 Pardubice
Datové centrum	Krajský úřad Pardubického kraje, Komenského náměstí 125, 532 11 Pardubice
Koncová lokalita	Městský úřad Chrudim, Resselovo náměstí 77, 537 16 Chrudim
Koncová lokalita	Městský úřad Litomyšl, Bří Šťastných 1000, 570 20 Litomyšl
Koncová lokalita	Magistrát města Pardubice, Pernštýnské náměstí 1, 530 21 Pardubice
Koncová lokalita	Městský úřad Svitavy, T. G. Masaryka 40/25, 568 02 Svitavy
Koncová lokalita	Městský úřad, Ústí nad Orlicí Sychrova 16, 562 24 Ústí nad Orlicí

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

4. Účel projektu

1) Celková modernizace sítě RDS 1.0
2) Propojení co největšího počtu zájmových lokalit dedikovaným připojením splňujícím výkonové i bezpečnostní parametry
3) Zakruhovat minimálně lokality s nemocnicemi
4) Výkonové navýšení jednotlivých propojení
5) Visibilita a vyšší bezpečnost sítě
6) Možnost připojení i dalších uzlů sdíleným datovým médiem (internetem)
7) Kvalitní přenosové médium minimálně pro informační systém sdílení dat a informací s obcemi (ISKO)

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

5. Obecné požadavky na implementaci

1) Projektové vedení projektu i jednotlivých částí – zadavatel požaduje projektové vedení projektu i každé jeho části, která je implementována samostatně. Minimálně 1x měsíčně bude provedeno dodavatelem jednání v místě sídla objednatele, kde osobně vedoucí realizačního týmu a hlavní architekt seznámí zástupce zadavatele o stavu projektu či jeho části. Zadavatel může dle rozsahu části projektu projektové povinnosti v zadávací dokumentaci zmírnit.
2) Proškolené osoby zadavatele musí mít přístup ke všem informačním i troubleshootovacím funkcionalitám dodávaného řešení. O každém jejich postupu však musí být proveden automaticky záznam. Proškolení těchto osob je povinností dodavatele.
3) Proškolené osoby zadavatele musí mít možnost přebrat kontrolu nad celou sítí. O každé změně v síti však musí být proveden automaticky záznam.
4) Součástí přípravných prací je i předimplementační analýza
5) Součástí přípravných prací je i vypracování prováděcího projektu akceptujícího již dříve implementované části sítě nebo jiné části projektu
6) Dodávka a vlastní implementace nesmí až na plánované, oznámené a schválené výpadky ohrozit provoz datové sítě.
7) Součástí implementace je i testovací provoz, kdy dodavatel poskytuje zvýšený dozor nad provozem testované části projektu a je připraven řešit vady ve zvýšené SLA 99,9%.
8) Akceptační testy reflektují jak běžný provoz, tak i jeho zatížení.
9) Všechny dodávané části jsou vyžadovány včetně zaškolení, které odpovídá rozsahu a důležitosti jednotlivých částí.
10) Zaškolování osob zadavatele pro práci v síti provádí dodavatel na své náklady a musí být pravidelné.
11) Podmínkou spuštění ostrého provozu jednotlivých částí jsou i dodané dokumentace dle požadavků zadavatele.
12) Realizace projektu musí mít vždy možnost navázat. Navržené řešení dodavatele musí mít vždy možnost pokračovat jiným projektem či jeho částí.
13) Zadavatel může určit jinou osobu („třetí stranu“), která bude v daném rozsahu spravovat Regionální datovou síť se zadavatelem a bude za zadavatele jednat při předávce dílčích částí projektu a ve věci servisní a technické podpory. Všechny podmínky implementace a provozu jsou tak platná i pro tuto osobu.

14) Všechny částí dodávky a předmětu implementace musí být určeny pro český trh, musí být nové, ne repasované.

15) Je-li součástí požadavku podpora dané funkčnosti, dodavatel očekává i případné licence pokrývající tuto podporu jako součást dodávky.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

6. Obecné požadavky na obsah provozní podpory

1) Zadavatel požaduje služby servisního manažera u těch částí projektu, kde to bude v parametrech zadávací dokumentace požadováno.
2) Zadavatel požaduje po dodavateli řádně implementovanou dodávku a její předání do užití zadavateli
3) Zadavatel určí „třetí stranu“ jako spolusprávce celé sítě, která se většinově podílí na zajištění provozu a dostupnosti služeb sítě. Tato strana má při řešení a hlášení incidentů stejnou pravomoc komunikace s dodavatelem, jako zadavatel.

7. Projektem plánované uzly regionální datové sítě LabeNET

Tabulka 2 - Zájmové body projektu RDS 2.0 nejvyšší priority

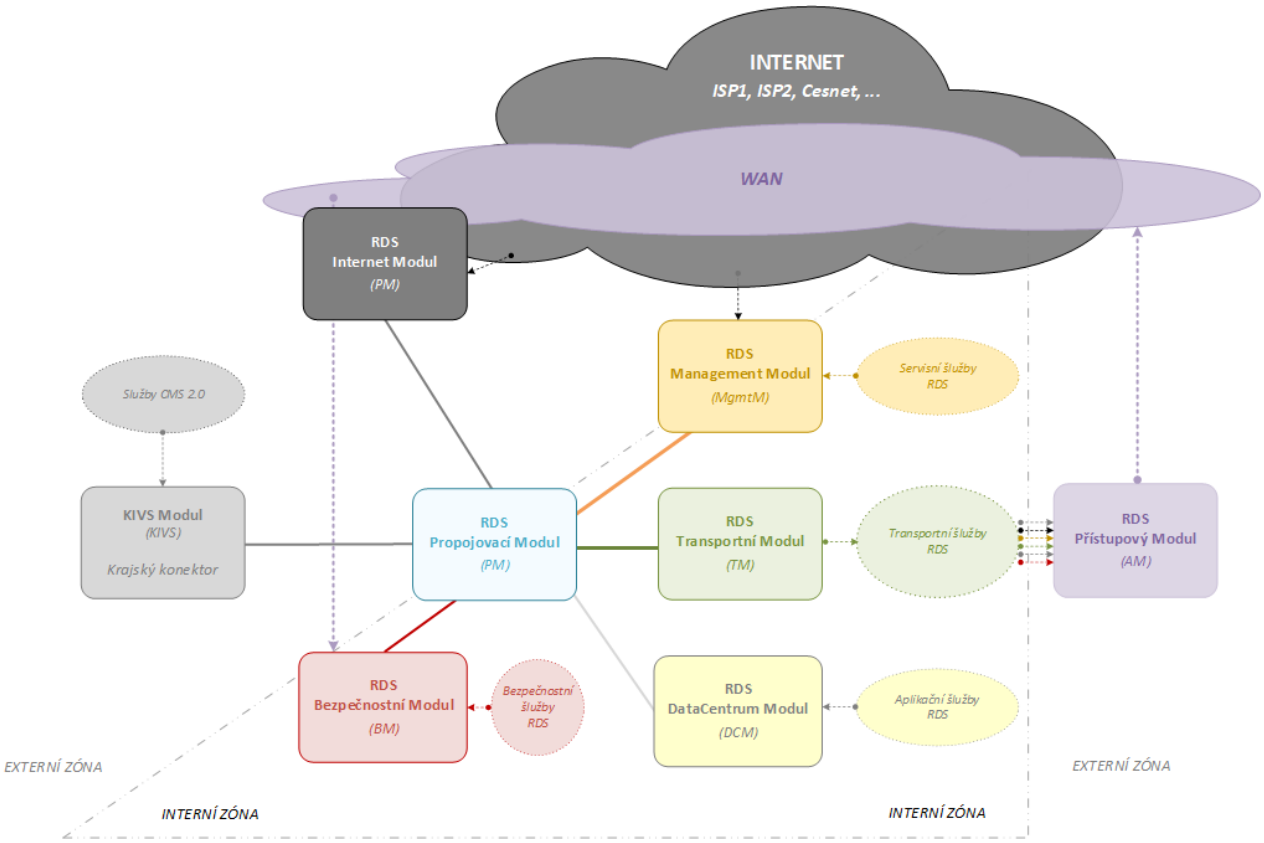
Název ORP / lokality	Název úřadu / uzlu	Adresa rozvaděčové místnosti, kde bude RDS zakončena
Litomyšl	Připojení CESNET Fakulta restaurování UPCE	Jiráskova 3, 570 01 Litomyšl
Česká Třebová	Městský úřad Česká Třebová	Staré náměstí 78, 560 02 Česká Třebová
Hlinsko	Městský úřad Hlinsko	Adámkova 554, Hlinsko
Holice	Městský úřad Holice	Holubova 1, Holice
Králíky	Městský úřad Králíky	Velké náměstí 5, 561 69 Králíky
Lanškroun	Městský úřad Lanškroun	nám. J. M. Marků 5, 563 01 Lanškroun
Moravská Třebová	Městský úřad Moravská Třebová	Olomoucká 178/2 571 01 Moravská Třebová
Polička	Městský úřad Polička	Palackého nám. 160, 57201 Polička
Přelouč	Městský úřad Přelouč	Československé armády 1665
Vysoké Mýto	Městský úřad Vysoké Mýto	B. Smetany 92, 566 32 Vysoké Mýto
Žamberk	Městský úřad Žamberk	Masarykovo nám. 166, 564 01 Žamberk

8. RDS 2.0 – obecné informace

Vzhledem ke stále rostoucím požadavkům na komunikační infrastrukturu a bezpečnost služeb a celé RDS je třeba v rámci rozšíření zásadně modernizovat celý projekt na RDS 2.0 a zajistit tak fungování stávajících i nových služeb.

8.1. High-Level architektura

Základním stavebním prvkem budou jednotlivé moduly, poskytující do celkového informačního systému definované služby, které jsou pak různorodě využívány připojenými organizacemi. Řízené propojení a směrování služeb je pak v prostředí RDS 2.0 zajišťováno pomocí Propojovacího Modulu (PM). Ten je také jediným vstupním a výstupním bodem služeb, které poskytují moduly Externí zóny. Výjimku tvoří zajištění propojení Přístupového Modulu (AM) s VPN koncentrátorem Bezpečnostního Modulu (BM), který nejprve zakončí IPSec Site-to-Site (případně Client-to-Site) tunel a teprve potom pošle komunikaci směrem do Propojovacího Modulu (PM)



Obrázek 3 High-Level adrchitektura RDS 2.0

8.2. Architektonické moduly

Jednotlivé moduly jsou podle kontroly nad jejich konfigurací, správou a provozem rozděleny do Interní a Externím zóny.

RDS 2.0 bude ihned po rozšíření primárně infrastrukturou transportního charakteru, tzn., že její využití bude spočívat převážně v distribuci služeb externí zóny k jednotlivým připojovaným organizacím pomocí Bezpečnostního, Propojovacího a Transportního Modulu.

Zóna	Modul	Priorita výstavby
INTERNÍ	Management Modul (MgmtM)	ihned při rozšíření
	Propojovací Modul (PM)	ihned při rozšíření
	Transportní Modul (TM)	ihned při rozšíření
	Přístupový Modul (AM)	řeší připojované organizace
	DataCentrum Modul (DCM)	ihned při rozšíření
	Bezpečnostní Modul (BM)	ihned při rozšíření
EXTERNÍ	Internet Modul (IM)	ihned při rozšíření
	KIVS Modul	ihned při rozšíření

Tabulka 3 Architektonické moduly RDS 2.0

8.3. Bezpečnostní modul

Jako samostatný modul je v architektuře RDS 2.0 použit Bezpečnostní Modul (…dále jen RDS-BM). Tato část bude přes Propojovací modul (RDS-PM) logicky propojena do všech ostatních modulů „Interní zóny“. Úkolem RDS-BM je zajištění „bezpečnostní části servisních služeb“. Na pomezí s provozními Servisními službami se řadí Síťová analýza provozu, která je v této poptávce a budoucí veřejné zakázce řazena k bezpečnostním prvkům, ale věcně k provozním.

8.4. Servisní služby

V rámci prvního kroku rozšíření RDS se nepředpokládá vznik a provoz všech služeb najednou, ale z pohledu dimenzace HW a SW zdrojů pro jejich provoz, je nutné vědět o záměru spuštění některých služeb v dalších krocích viz. Tabulka č. 4.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Servisní služby RDS 2.0

Oblast	Servisní služby Management Modulu	Priorita spuštění
Provoz	Log Management	ihned při rozšíření
	Network Management a správa konfigurací	ihned při rozšíření
	Network Monitoring	ihned při rozšíření
	Zálohování (Backup)	ihned při rozšíření
	Out of Band Management (OOB)	ihned při rozšíření
Bezpečnost	Next Generation Firewall pro nezávislý přístup MGMT	ihned při rozšíření
	Remote VPN (R-VPN) pro nezávislý přístup MGMT	ihned při rozšíření
	Bezpečnostní analýza služeb	ihned při rozšíření
	Síťová analýza provozu	ihned při rozšíření
	Adresářové služby LDAP (LDAP)	ihned při rozšíření
	Služba bezpečného ověření identity (RADIUS)	ihned při rozšíření
	Anti-X ochrana serverů (AntiX-SRV)	*v budoucnu*
	Anti-X ochrana koncových zařízení (AntiX-EndP)	*v budoucnu*
	Bezpečná přístupová stanice (SAW)	*v budoucnu*
	Multifaktorová authentizace (MFA)	*v budoucnu*
	Bezpečnostní Monitoring (SIEM)	*v budoucnu*

Tabulka 4 Servisní služby RDS 2.0 a jejich priorita spuštění

Servisní služby mají za úkol zajistit základní potřeby chodu vlastní infrastruktury modulů v interní zóně RDS 2.0. Vazba využití jednotlivých Servisních služeb konkrétními moduly architektury je upřesněna v Tabulce č. 3.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Vazba Servisních služeb na architekturu Interní zony RDS 2.0

Oblast	Servisní služby Management Modulu	Službou zajištěná část architektury				
		Management Modul	Propojovací Modul	Transportní Modul	DataCentrum Modul	Bezpečnostní Modul
Provoz	Log Management	●	●	●	●	●
	Network Management a správa konfigurací	●	●	●	●	●
	Network Monitoring	●	●	●	●	●
	Zálohování (Backup)	●	●	●	●	●
	Out of Band Management (OOB)	●				
Bezpečnost	Next Generation Firewall pro nezávislý přístup MGMT	●				
	Remote VPN (R-VPN) pro nezávislý přístup MGMT	●				
	Bezpečnostní analýza služeb	●			●	●
	Síťová analýza provozu	●	●	●	●	●
	Adresářové služby LDAP (LDAP)	●	●	●	●	●
	Služba bezpečného ověření identity (RADIUS)	●	●	●	●	●
	Anti-X ochrana serverů (AntiX-SRV)	●				
	Anti-X ochrana koncových zařízení (AntiX-EndP)	●				
	Bezpečná přístupová stanice (SAW)	●	●	●	●	●
	Multifaktorová authentizace (MFA)	●	●	●	●	●
	Bezpečnostní Monitoring (SIEM)	●	●	●	●	●

Tabulka 5 Vazba Servisních služeb Bezpečnostního modulu na architekturu Interní zóny RDS 2.0

Pro potřeby poptávky a veřejné zakázky nás zajímají ty služby modulu Bezpečnosti, které jsou označeny červeně.

8.5. Předpokládaná forma zajištění Servisních služeb RDS-BM

S ohledem na snahu zajistit vysokou dostupnost (HA) prostředí RDS 2.0 je vyžadováno řešení redundantní co do lokality, připojení, tak do použití jednotlivých technologií. Nosné prostředí Management modulu RDS 2.0. je proto rozvrženo do 2 lokalit. Předpokládá se tedy zajištění dostupnosti HW komponent umístěním minimálně do obou lokalit. Na aplikační úrovni není vždy možné zajistit aspekty HA pouhým zdvojením instalace aplikace. Také ekonomika takového designu může být v některých případech neadekvátní velikosti a účelu řešení. Předpokládáme proto využití virtualizační platformy VMWare, která řeší požadavek na HA prostředí serverů a aplikací pomocí vlastního mechanismu a to nejen na úrovni komponent zajišťujících výkon platformy (vCPU, RAM, LAN) ale také na straně společného datového úložiště v podobě Software Defined Storage (SDS). Některé Servisní služby jsou pak provozovány pomocí Virtuálních serverů (VM) a Virtuálních Appliancí (VA) na kterých běží jejich aplikace. Virtualizační platforma není předmětem poptávky ani následující veřejné zakázky. Je řešena jinou VZ (jako součást VZ na MGMT modul)

Předpokládaná forma zajištění jednotlivých Servisních služeb RDS 2.0 vyplývá z Tabulky č.6.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Předpokládaná forma zajištění Servisních služeb RDS 2.0

Oblast	Servisní služby Management Modulu	Předpokládaná forma zajištění	Stávající, využitelné licence	Předpokládané zajištění HA prostředí
Provoz	Log Management	Hardware (HW)		pomocí HW prvků
	Network Management a správa konfigurací	Virtuální Server (VM)	Ansible	pomocí virtualizační platformy
	Network Monitoring	VM	Zabix 5.0	pomocí virtualizační platformy
	Zálohování (Backup)	VM	Veeam Backup & Replication Community Edition	pomocí virtualizační platformy
	Out of Band Management (OOB)	HW		pomocí HW prvků (*např. virtualní chassi, HW cluster apod.*)
Bezpečnost	Next Generation Firewall pro nezávislý přístup MGMT	HW		
	Remote VPN (R-VPN) pro nezávislý přístup MGMT	HW		
	Bezpečnostní analýza služeb	HW		pomocí HW prvků
	Síťová analýza provozu	HW		pomocí HW prvků
	Adresářové služby LDAP (LDAP)	VM	Linux Debian 9 Server s OpenLDAP	min. 2x VM na různých nodech hypervisorů, HA zajištěno vlastní konfigurací aplikace (*např. aplikační cluster, synchronizace databáze apod.*)
	Služba bezpečného ověření identity (RADIUS)	VM	Linux Debian 9 s FreeRadius	
	Anti-X ochrana serverů (AntiX-SRV)	*VM*	-	*pomocí virtualizační platformy*
	Anti-X ochrana koncových zařízení (AntiX-EndP)	*VM*	-	*pomocí virtualizační platformy*
	Bezpečná přístupová stanice (SAW)	*VA*	-	*pomocí virtualizační platformy*
	Multifaktorová authentizace (MFA)	*VM*	-	*pomocí virtualizační platformy*
	Bezpečnostní Monitoring (SIEM)	*HW+VA*	-	*samostatné HW řešení*

Tabulka 6 Předpokládaná forma zajištění Servisních služeb Bezpečnostního modulu

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

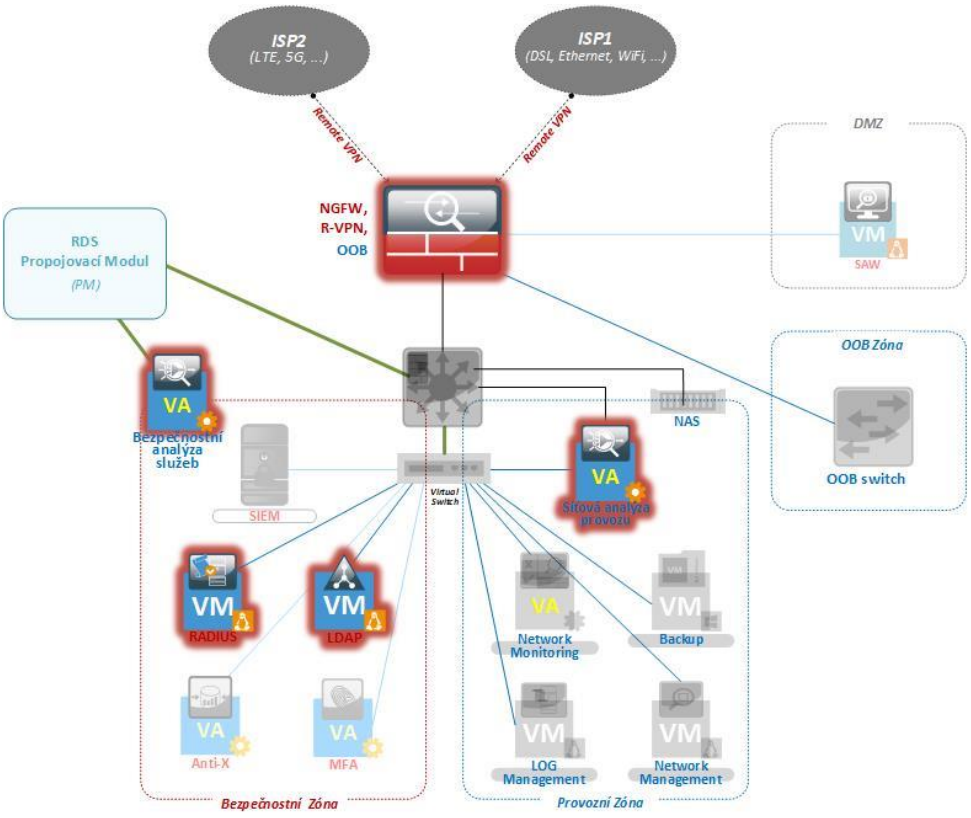
9. Bezpečnostní modul – PŘEDMĚT DODÁVKY

9.1. Předměty plnění

1) NGFW + Remote VPN pro nezávislý přístup MGMT
2) Site-to-site VPN
3) NG segmentační FW
4) Síťová analýza provozu
5) Bezpečnostní analýza plného služeb
6) Služba bezpečného ověření identity
7) Adresářová služba

9.2. Aplikační architektura

Očekávaná aplikační architektura řešení se bude skládat z označených logických komponent dle Obrázku č. 4.



Obrázek 4 Základní logická architektura řešení Servisních služeb RDS 2.0 – zvýrazněné se týkají poptávky na Bezpečnostní modul

Serverová infrastruktura virtualizačního prostředí včetně SDS úložiště

Management modul RDS 2.0 bude vytvořen servery přes dvě lokality - KrÚ 120 a KrÚ 125. V obou jsou stávající datová centra. Datová centra budou pro zajištění HA prostředí modulu vystavěna v režimu „Active-Active“. V případě havárie jednoho datového centra musí být druhé datové centrum schopné poskytovat všechny Servisní služby Management modulu. V lokalitě KrÚ 125 bude z pohledu RDS 2.0. umístěno DC1.

Fyzická topologie

Popis řešení

Virtualizační platforma bude dodána z jiné veřejné zakázky jako hyperkonvergovaný systém nodů s interní diskovou kapacitou rozšiřitelný jak metodou scale-out, tak scale-up s vysokým stupněm redundance pro přežití výpadku až 50% nodů. V lokalitě DC1 a DC2 bude umístěn vždy minimálně jeden HW nod. Kromě virtualizace výkonu tedy bude řešení disponovat i virtualizací diskové kapacity tzv. Software Defined Storacge (SDS). V těchto případech je nutné zajistit dostatečnou kapacitu datových spojů mezi nody clusteru. Proto bude požadované řešení disponovat minimálně 4x10Gbps spoji, které budou dedikované pouze pro SDS řešení.

Výkonnostní nároky

Očekávané výkonnostní požadavky Bezpečnostních služeb jednotlivých logických komponent aplikační architektury RDS 2.0. udává Tabulka č. 7.

Oblast	Servisní služba	vCPU	RAM (GB)	HDD (TB)	Dedikované HW LAN adaptéry
	Network Management a správa konfigurací	6	48	1	
	Network Monitoring	4	16	3	1x 1GB Base-T
	Zálohování (Backup)	4	48	0,5	
Bezpečnost	Adresářové služby LDAP (LDAP)	2	8	0,5	
	Služba bezpečného ověření identity (RADIUS)	2	8	0,5	
	Anti-X ochrana serverů (AntiX-SRV)	*4*	*24*	*1*	
	Anti-X ochrana koncových zařízení (AntiX-EndP)				
	Bezpečná přístupová stanice (SAW)	*2*	*16*	*0,5*	
	Multifaktorová authentizace (MFA)	*2*	*16*	*0,5*	

Tabulka 7 Minimální výkonnostní nároky Servisních služeb RDS 2.0

Next Generation Firewall pro nezávislý přístup MGMT

Komponenta zajišťující služby, především bezpečnostního charakteru. Úkolem je zajistit bezpečný přístup na Internet pouze pro zdroje umístěné ve vlastním Management modulu. Důvodem je potřeba automatických update, aktualizací bezpečnostních oprav a on-line přístup k tzv. Threath

Inteligenci výrobců dalších komponent architektury. Protože se jedná a prvek umístěný na hranici vnitřní a vnější zóny RDS 2.0. bude chod těchto aplikací zajištěn vlastním, pro tyto účely specializovaným, výkonným HW. Ten může být společným i pro komponentu Remote VPN pro nezávislý přístup MGMT. Díky požadovaným vlastnostem a funkcím bude zároveň s dalšími aktivními prvky tvořit základ pro segmentaci prostředí a bezpečné oddělení provozu jednotlivých oblastí sítě.

Konkrétní rozsah implementace, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Remote VPN pro nezávislý přístup MGMT

Další z komponent zajišťující službu bezpečnostního charakteru. Jejím hlavním úkolem je zajistit bezpečný, vzdálený přístup administrátorů, případně externích subjektů, k prostředí Management modulu RDS 2.0. Klíčovým, pro přístup VIP účtů k prostředí Management modulu, je jednoznačné prokázání identity. Proto je jedním z požadavků také podpora a zajištění licencí MFA (multifaktorové authentizace). Vlastní chod aplikace bude zajištěn novým HW, který může být společný i pro komponentu NGFW management modulu pro nezávislý přístup MGMT.

Konkrétní rozsah implementace, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Site-to-Site VPN

Propojení lokalit bez optické infrastruktury bude směrem do RDS 2.0 zajišťovat komponenta Site-to-Site VPN. Provoz z těchto lokalit ve formě IPSec kryptovaného tunelu zde bude zakončen, dekryptován a přes Propojovací modul RDS 2.0 začleněn do celkové koncepce sítě. Definované toky pak mohou být dále zaslány do segmentačního FW, který zajistí jejich vyžadované směrování.

9.2.1. Segmentační Firewall

Primární úlohou segmentačního FW je řízení přístupu mezi jednotlivými sítěmi účastníků provozu RDS 2.0 a jejich kontrola z pohledu detekce bezpečnostních hrozeb především formou IPS a Aplikační inspekce. Na výkon a dostupnost této komponenty bude kladen veliký důraz.

Síťová analýza provozu

Komponenta zajišťující komplexní bezpečnostní monitoring datových toků (např. NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších) pro celé prostředí RDS 2.0.

Technologie představuje moderní a ověřený, způsob pro bezpečnostní monitorování sítě a nabízí výhody možnosti zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu a škálovatelnost. Nabízená technologie musí být určená pro český trh. Podpora na

licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může Zadavatel přímo kontaktovat.

Vlastní aplikace bude řešena jako Flow kolektor. Kolektory jsou zařízení/prostředky (datová úložiště) s diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných dat.

Aplikace nemusí ihned při rozšíření RDS umožňovat provoz v režimu HA. V rámci rozšíření RDS je požadována dodávka 1ks HW datového kolektoru pro zpracování a analýzu pouze dat typu NetFlow a dále implementace, která zajistí poskytování Servisní služby „Síťová analýza provozu“. Konkrétní rozsah implementace, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Budoucí rozšíření na HA a o sondu není předmětem této zakázky, pouze bude s tímto rozšířením počítáno v rámci předimplementační analýzy a dokumentace.

Bezpečnostní analýza služeb

Služba bezpečnostního charakteru. Jejím hlavním úkolem je zajistit detekci případných bezpečnostních událostí formou analýzy plného síťového provozu s využitím vlastního sensoru na základě zrcadleného kompletního provozu (nikoliv jen na základě statistických protokolů typu NetFlow). Zajištění takovéto viditelnosti je při rozšíření RDS vyžadováno pouze pro prostředí vybraných modulů.

Nabízená technologie musí být určená pro český trh. Podpora na licence ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může Zadavatel přímo kontaktovat.

Aplikace nemusí ihned při rozšíření RDS umožňovat provoz v režimu HA. V rámci rozšíření RDS je požadována dodávka 1ks HW datového kolektoru a senzoru pro zpracování kompletní síťové komunikace a dále implementace, která zajistí poskytování Servisní služby „Bezpečnostní analýza plného síťového provozu“. Konkrétní rozsah implementace, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Adresářové služby (LDAP) – popis služby

Komponenta zajišťující centrální adresářové služby, především jako úložiště identit pro přístup k ostatním Servisním službám RDS 2.0.

Nasazení bude v podobě minimálně 2ks virtuálních serveru ve formě VM, instalovaných na na minimálně dvou nodech virtualizační platformy, kdy každý bude umístěn v jiné lokalitě a každý VM bude v aktivním stavu. Na VM bude implementován OS Linux Debian 11 Server s démonem OpenLDAP. Licence zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Adresářové služby LDAP“ pro dotčené moduly, viz. Tabulka č. 5.

Pro chod aplikací bude využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 2x vCPU, 8GB RAM a diskový prostor s kapacitou 0,5TB.

Konkrétní rozsah implementace, včetně definice členění do OU, zařazení uživatelů a jejich členství v OU, bude upřesněna na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Služba bezpečného ověření identity (RADIUS) – popis služby

Komponenta zajišťující bezpečné ověření identity a následné přiřazení práv a konfigurace v závislosti na výsledku ověření i na aktivních prvcích sítě, jako jsou switche, routery, firewally apod.

Nasazení bude v podobě minimálně 2ks virtuálních serveru ve formě VM, instalovaných na na minimálně dvou nodech virtualizační platformy, kdy každý bude umístěn v jiné lokalitě a každý VM bude v aktivním stavu. Na VM bude implementován OS Linux Debian 11 Server s démonem FreeRADIUS. Licence zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Služba bezpečného ověření identity“ pro dotčené moduly, viz. Tabulka č. 5.

Pro chod aplikací bude využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 2x vCPU, 8GB RAM a diskový prostor s kapacitou 0,5TB.

Konkrétní rozsah implementace, včetně definice prvků, které mohou RADIUS Server využívat bude upřesněna na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Ostatní budoucí a plánované služby

V budoucnu se očekává nasazení ještě těchto, především bezpečnostních aplikací:

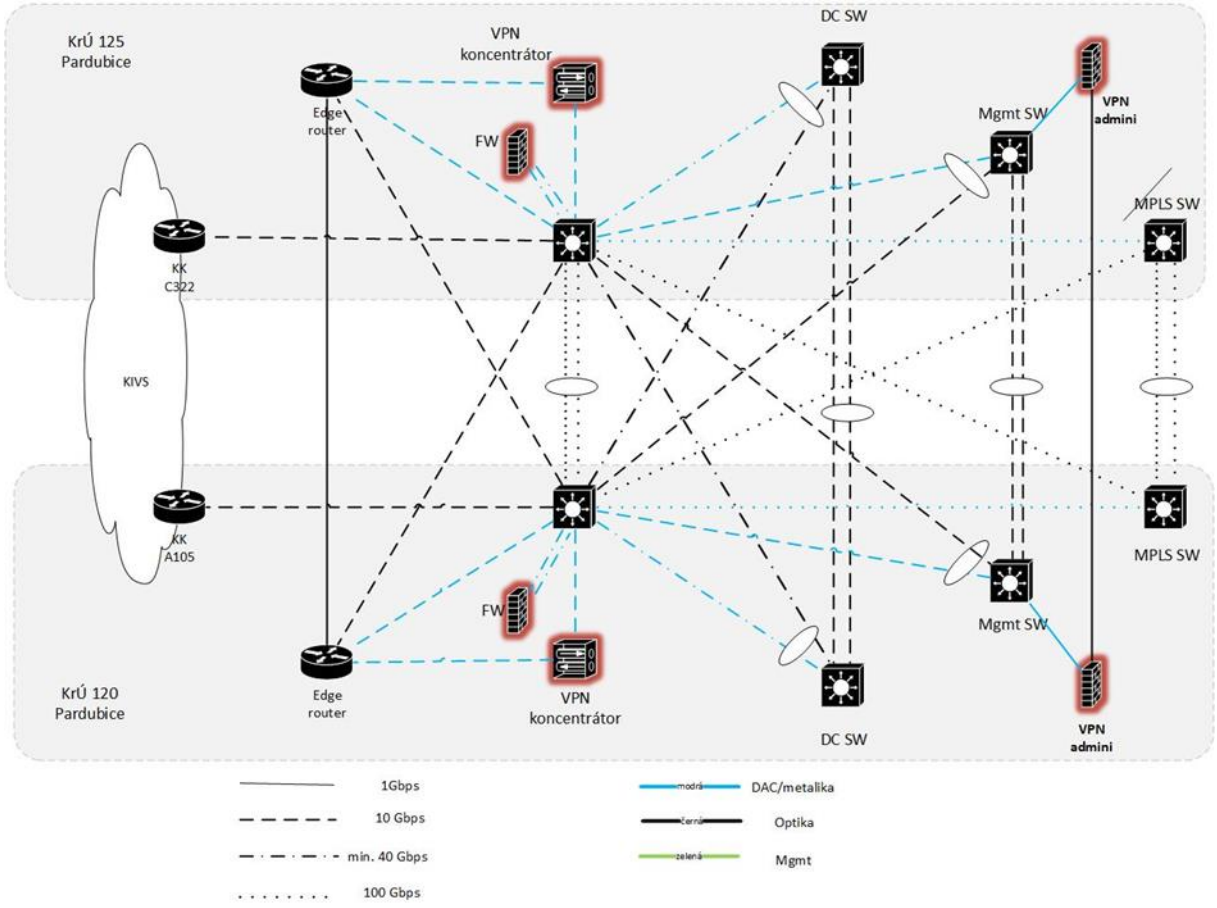
1) Anti-X ochrana serverů (AntiX-EndP)
2) Bezpečná přístupová stanice (SAW)
3) Multifaktorová authentizace (MFA)
4) Bezpečnostní Monitoring (SIEM)

Architektura i Prováděcí dokumentace musí s těmito službami počítat, minimálně z hlediska sizingu.

9.3. Bližší parametry poptávky

9.3.1. Firewally

Umístění firewallů, které jsou dále požadovány budou připojeny dle následujícího obrázku.



Součástí dodávky bude i plné osazení DAC kabelů nebo transceiverů pro SM 9/125 na vzdálenost v rackové skříni a na vzdálenost 200-500m (mezi datacentry) včetně kabelů optických i metalických.

Obecné požadavky na všechna zařízení firewall:

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Splněno ANO/NE
Vlastnosti hardware		
Instalace	Rack, racková skříň	ANO
Velikost	Max. 2U/zařízení	ANO
Stejný výrobce všech zařízení	ano	ANO

Stejné ovládání přes CLI i GUI u všech zařízení	ano	ANO
Umístění výrobce zařízení mezi Leadery Network Firewalls v Gartner Magic Quadrant nebo obdobné	Min. 2x za poslední 4 roky	ANO

Všechny firewally budou mít jednotný management a další stejné parametry zde uvedené:

Správa		
Požadavky na VM		**Splněno ANO/NE**
Centrální management řešen jako VM na Vmwarer ESXi 6.7+	Ano	ANO, Fortimanager VM licence + 5 let support / Fortianalyzer VM licence + 5 let support
Podpora vysoké dostupnosti managementu formou dvou strojů	Ano	ANO
požadavky na vCPUs	Né více než 16 CPU	ANO
požadavky na RAM	Né více než 32GB RAM	ANO
požadavky na úložiště/disk space	Né více než 1T	ANO

Funkcionality		**Splněno ANO/NE**
Vzdálené správa přes grafické rozhraní	Ano	ANO
Centrální správa pro všechny nabízené NGFW platformy včetně všech oddělených virtuálních kontextů	Ano	ANO
Management by měl poskytovat informace o "zdraví firewallu" (vytížení CPU/RAM/disk a pod.)	Ano	ANO
Centrální správa bezpečnostních politik	Ano	ANO
Centrální správa NAT politik/konfigurace fw	Ano	ANO
Centrální správa při nasazení více firewallů	Ano	ANO
Možnost sdílených bezpečnostních politik	Ano	ANO
Při použití ve vysoké dostupnosti se spravuje pouze jeden logický prvek	Ano	ANO
Možnost upgrade/update software firewallu, bezpečnostních update (IPS signatury, geolokační databáze, apod.), konfigurací atd. z grafického rozhraní managementu	Ano	ANO
Zobrazení všech logů a událostí (provozní i bezpečnostní), alespoň za posledních 14 dní(50GB/denně) nebo v objemu min. 700GB v grafickém rozhraní správy. Žádný log nesmí být v tomto čase nebo objemu smazán, kapacitně musí zařízení umět uložit všechny konfigurovatelné logy.	Ano	ANO
Centrální mgmt konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	ANO
Centrální mgmt konzole by měla být schopna vytvářet reporty automaticky nebo manuálně a podle časového harmonogramu	Ano	ANO
Centrální mgmt konzole musí být schopna exportovat reporty alespoň ve formátech PDF a CSV	Ano	ANO
Centrální mgmt konzole musí být schopna integrace s Microsoft AD/Cisco ISE pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	ANO
Podpora posílání vybraných logů formou syslog (SYSLOG as per RFC 5424)	Ano	ANO
Podpora posílání vybraných událostí formou emailu nebo SNMP na externí platformy (možnost konfigurace pro každou platformu)	Ano	ANO
Podpora pro sdílení informací s externími systémy SIEM		
Možnost zasílat předdefinované reporty emailem. (podpora také autentizovaného SMTP pro komunikaci s mail relay)		
Podpora API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	ANO
Podpora řízeného přístupu podle rolí administrátorů	Ano	ANO
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	ANO
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Ano	ANO
• Čas	Ano	ANO
• Akce (allow, deny,..)		
• Důvod případného blokování		
• Zdroj. a cíl. adresa		
• Zdroj. a cíl. port		
• v případě NATu i přeloženou src nebo dst IP		
• Aplikační protokol		
• IPS událost, pokud vznikne		
• Použitá síťová aplikace		
Možnost zobrazit si logy pouze pro funkcionalitu, která může provoz blokovat (IPS, Antivir/Antimalware, Anti-bot apod.)	Ano	ANO

Požadovaná funkcionalita/činnost	Způsob splnění požadované funkcionality/činnosti	Splněno ANO/NE
zaškolení administrátorů	2x 3MD pro 3 osoby	ANO
Implementace/Instalace managementu	ano	ANO
základní konfigurace FW	ano	ANO
Zapojení do infrastruktury zadavatele	ano	ANO
Zahoření	ano	ANO
Testovací provoz	v rozsahu 3 týdnů	ANO
pilotní konfigurace aplikační kontroly FW (L7)	ano - minimálně 1 týden před koncem testovacího provozu	ANO
pilotní konfigurace IPS v "detect" módu	ano - minimálně 1 týden před koncem testovacího provozu	ANO
pilotní konfigurace antivir/antimalware funkcionality	ano - minimálně 1 týden před koncem testovacího provozu	ANO
pilotní konfigurace SSL/TLS dekrypce	ano - minimálně 1 týden před koncem testovacího provozu	ANO
vyhodnocení testovacího provozu	ano	ANO
finální doladění konfigurace firewallu a přechod do produkčního režimu	ano	ANO
Dokumentace skutečného provedení	ano	ANO

provozní a bezpečnostní dokumentace	ano	ANO
disaster recovery dokumentace	ano	ANO
Akceptace (fyzická montáž, testování vysoké dostupnosti, obnova po havárii, klíčová pravidla)	ano	ANO

9.3.2. NGFW + Remote VPN pro nezávislý přístup MGMT

Popis řešení

Vlastní nároky na výkon NGFW budou v tomto případě minimální. Úlohou je zajištění Servisních služeb Next Generation Firewall, Remote VPN (R-VPN) a Out of Band Management (OOB), které jsou vázány pouze k vlastnímu Management modulu. Důraz je spíše kladen na vysokou ochranu pomocí technologií typu Advanced Threath Protection, jako jsou např. IPS, Application Control, WebFiltering, Malware Defence a jiné. V lokalitě DC1 a DC2 bude umístěn vždy jeden HW kus NGFW. Řešení umožní konfiguraci do clusteru fungujícího v režimu minimálně Active-Pasive. Každý NGFW bude napojen do Internetu oddělenou, nezávislou cestou a ideálně odlišnými ISP (např. NGFW v DC1 pomocí ISP1, technologií xDSL a NGFW v DC2 pomocí ISP2, technologií LTE nebo 5G, apod.). Pokud je požadována v následujících vlastnostech produktu podpora nějaké funkce, jsou součástí řešení i veškeré licence na celou dobu servisní podpory tohoto produktu.

Další požadované funkce

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Splněno ANO/NE
Vlastnosti hardware		
Počet zařízení	2	ANO

Vlastnosti každého zařízení		Splněno ANO/NE
Formát zařízení	HW appliance	ANO, FortiGate 60F, Licence Advanced Threat Protection + FortiCare Premium 5YR
Minimální počet 1 GbE RJ45 rozhraní	10	ANO
Zařízení obsahuje redundantní zdroje napájení nebo používá externí napájecí zdroj s možností výměny	ano - 2 zdroje	ANO
Konzolový sériový port	1x	ANO
Podpora vytváření virtuálních izolovaných kontextu NGFW s vlastním konfiguračním rozhraním (řešení formou VRF není akceptovatelné)	min. 10 instancí	ANO
Podpora režimu vysoké dostupnosti	ano	ANO
Funkcionalita firewallu - per chassis		**Splněno**

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

		ANO/NE
Počet současně otevřených TCP spojení aplikačního FW	min 700 k	ANO
Rychlost vytváření nových TCP spojení přes aplikační FW (CPS)	min 35 k	ANO
Propustnost funkce ochrany před sítovými útoky (IPS), enterprise mix traffic	min. 1 Gbps	ANO
Propustnost funkce NGFW (stavový firewall, IPS, analýza a rozpoznávání aplikací na L7), enterprise mix traffic	min. 1 Gbps	ANO
Propustnost funkce ochrany proti sítovým hrozbám Threat Protection (stavový firewall, IPS, analýza a rozpoznávání aplikací na L7, ochrana před škodlivým kódem), enterprise mix traffic	min. 700 Mbps	ANO
Propustnost funkce IPSEC VPN (při použití AES256, SHA 256)	min. 6 Gbps	ANO
Minimální počet současných TCP spojení podléhajících současně funkci SSL inspekce	55 k	ANO
Propustnost funkce SSL inspekce	min. 600 Mbps	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	ANO
podpora 802.1Q tagovaných rámců	Ano	ANO
Minimálně počet VLAN	min. 1024	ANO
Vysoká dostupnost - stateful failover (active/standby)	Ano	ANO
Možnost sloučení více fyzických rozhraní - LACP 802.3ad	Ano	ANO
Dynamické směrování - min podpora alespoň OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – OSPFv3, BGP	Ano	ANO
Podpora Policy based Routing	Ano	ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Filtrace IPv4, IPv6	Ano	ANO
Možnost definovat platnost pravidla v čase (pravidlo funguje pouze v daném časovém rámci)	Ano	ANO
Funkce identity based firewallingu AD a Cisco ISE pomocí mechanismu PxGrid	Ano	ANO
Inspekce IPv6 provozu	Ano	ANO
Filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
IPS/IDS funkcionalita	Ano	ANO
Řízení rychlosti datových toků na úrovni pravidel FW (QoS)	Ano	ANO
FQDN objekty v přístupových pravidlech	Ano	ANO
Export logů protokolem SYSLOG as per RFC 5424 (nebo z managementu)	Ano	ANO
Protokol NTP (RFC 5905)	Ano	ANO
Protokol SNMP - v1, v2 i v3	Ano	ANO

Dostupná MIB pro SNMP daného zařízení	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy (může být nahrazeno API rozhraním na úrovni centrálního managementu)	Ano	ANO
Funkce IKEv1 a IKEv2 pro IPSEC	Ano	ANO
IPsec (ESP/AH)	Ano	ANO
Podpora algoritmů s Eliptický křivkami (např. ECDH apod.)	Ano	ANO
Podpora moderních hashovacích algoritmů SHA256-HMAC a SHA512-HMAC	Ano	ANO
Podpora Netflow (v9, nebo IPFIX protokol)	Ano	ANO

Funkce Next-Gen FW		**Splněno ANO/NE**
Dešifrování TLS komunikace (SSL dekrypce) včetnš TLS 1.3	Ano	ANO
Vzájemná propojitelnost s cílem sdílení provozních informací a incidentů s ostatními nabízenímy komponentami	Ano	ANO
Podpora aplikační firewall - rozeznávání aplikací (Layer7)	Ano	ANO
Min. počet rozeznávaných aplikací	Min. 4000	ANO
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO
Aplikace v databázi aplikací výrobce FW jsou kategorizovány a je posouzen jejich risk faktor	Ano	ANO
Geolokace v pravidlech - geolokační databáze, výrobcem udžovaná	Ano	ANO
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO
Podpora IDS režimu	Ano	ANO
Inspekce pro IPv4 i IPv6 v rámci IPS	Ano	ANO
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě	Ano	ANO
Možnost vytváření vlastních signatur pomocí popsané syntaxe (pro funkci IPS i pro funkci rozpoznávání aplikací L7)	Ano	ANO
Podpora automatické aktualizace IPS signatur/databáze	Ano	ANO
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO
Detailní popis k odhalenému bezpečnostnímu incidentu (např. odkaz na Wikipedii, stránky výrobce, CVE, …	Ano	ANO
IPS politiku lze aplikovat na různé firewally	Ano	ANO
Ochrana proti škodlivým IP/URL/DNS v internetu (známé BOT a C&C)	Ano	ANO
Možnost rozšíření o funkce URL filtrace na základě kategorie/reputace	Ano	ANO
Možnost zadat přehodnocení kategorie/reputace výrobci FW k posouzení	Ano	ANO
Dynamické seznamy URL a IP	Ano	ANO
Zadávání vyjímek (false positive - whitelisting)	Ano	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Site-to-site VPN

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Splněno ANO/NE
Vlastnosti hardware		
Počet zařízení	2	ANO

Vlastnosti každého zařízení		Splněno ANO/NE
Formát zařízení	HW appliance	ANO FortiGate 101F, Licence Advanced Threat Protection + FortiCare Premium 5YR
Minimální počet 10 GbE SFP+ rozhraní	2	ANO
Minimální počet 1 GbE SFP nebo RJ45 rozhraní	8	ANO
Zařízení obsahuje redundantní zdroje napájení	ano - 2 zdroje	ANO
Konzolový sériový port	1x	ANO
Podpora vytváření virtuálních izolovaných kontextu NGFW s vlastním konfiguračním rozhraním (řešení formou VRF není akceptovatelné)	min. 10 instancí	ANO
Integrovaný pevný SSD disk	min 480 GB	ANO
Dedikovaný HA/Failover/SYNC interface (nezapočítaný do počtu interface výše)	ano	ANO

Funkcionalita firewallu - per chassis		Splněno ANO/NE
Počet současně otevřených TCP spojení aplikačního FW	min 1.5 M	ANO
Rychlost vytváření nových TCP spojení přes aplikační FW (CPS)	min 55 k	ANO
Propustnost funkce ochrany před sítovými útoky (IPS), enterprise mix traffic	min. 2.5 Gbps	ANO
Propustnost funkce NGFW (stavový firewall, IPS, analýza a rozpoznávání aplikací na L7), enterprise mix traffic	min. 1.5 Gbps	ANO
Propustnost funkce ochrany proti sítovým hrozbám Threat Protection (stavový firewall, IPS, analýza a rozpoznávání aplikací na L7, ochrana před škodlivým kódem), enterprise mix traffic	min. 1 Gbps	ANO
Propustnost funkce IPSEC VPN (při použití AES256, SHA 256)	min. 10 Gbps	ANO
Minimální počet současných TCP spojení podléhajících současně funkci SSL inspekce	130 k	ANO
Propustnost funkce SSL inspekce	min. 1 Gbps	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	ANO
podpora 802.1Q tagovaných rámců	Ano	ANO

Minimálně počet VLAN	min. 1024	ANO
Vysoká dostupnost - stateful failover (active/standby)	Ano	ANO
Možnost sloučení více fyzických rozhraní - LACP 802.3ad	Ano	ANO
Dynamické směrování - min podpora alespoň OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – OSPFv3, BGP	Ano	ANO
Podpora Policy based Routing	Ano	ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Filtrace IPv4, IPv6	Ano	ANO
Možnost definovat platnost pravidla v čase (pravidlo funguje pouze v daném časovém rámci)	Ano	ANO
Funkce identity based firewallingu AD a Cisco ISE pomocí mechanismu PxGrid	Ano	ANO
Inspekce IPv6 provozu	Ano	ANO
Filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
IPS/IDS funkcionalita	Ano	ANO
Řízení rychlosti datových toků na úrovni pravidel FW (QoS)	Ano	ANO
FQDN objekty v přístupových pravidlech	Ano	ANO
Export logů protokolem SYSLOG as per RFC 5424 (nebo z managementu)	Ano	ANO
Protokol NTP (RFC 5905)	Ano	ANO
Protokol SNMP - v1, v2 i v3	Ano	ANO
Dostupná MIB pro SNMP daného zařízení	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy (může být nahrazeno API rozhraním na úrovni centrálního managementu)	Ano	ANO
Funkce IKEv1 a IKEv2 pro IPSEC	Ano	ANO
IPsec (ESP/AH)	Ano	ANO
Podpora algoritmů s Eliptický křivkami (např. ECDH apod.)	Ano	ANO
Podpora moderních hashovacích algoritmů SHA256-HMAC a SHA512-HMAC	Ano	ANO
Podpora Netflow (v9, nebo IPFIX protokol)	Ano	ANO

Funkce Next-Gen FW		**Splněno ANO/NE**
Dešifrování TLS komunikace (SSL dekrypce) včetnš TLS 1.3	Ano	ANO
Vzájemná propojitelnost s cílem sdílení provozních informací a incidentů s ostatními nabízenými komponentami	Ano	ANO
Podpora aplikační firewall - rozeznávání aplikací (Layer7)	Ano	ANO
Min. počet rozeznávaných aplikací	Min. 4000	ANO
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO
Aplikace v databázi aplikací výrobce FW jsou kategorizovány a je posouzen jejich risk faktor	Ano	ANO
Geolokace v pravidlech - geolokační databáze, výrobcem	Ano	ANO

udžovaná		
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO
Podpora IDS režimu	Ano	ANO
Inspekce pro IPv4 i IPv6 v rámci IPS	Ano	ANO
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě	Ano	ANO
Možnost vytváření vlastních signatur pomocí popsané syntaxe (pro funkci IPS i pro funkci rozpoznávání aplikací L7)	Ano	ANO
Podpora automatické aktualizace IPS signatur/databáze	Ano	ANO
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO
Detailní popis k odhalenému bezpečnostnímu incidentu (např. odkaz na Wikipedii, stránky výrobce, CVE, …	Ano	ANO
IPS politiku lze aplikovat na různé firewally	Ano	ANO
Ochrana proti škodlivým IP/URL/DNS v internetu (známé BOT a C&C)	Ano	ANO
Možnost rozšíření o funkce URL filtrace na základě kategorie/reputace	Ano	ANO
Možnost zadat přehodnocení kategorie/reputace výrobci FW k posouzení	Ano	ANO
Dynamické seznamy URL a IP	Ano	ANO
Zadávání vyjímek (false positive - whitelisting)	Ano	ANO

Segmentační firewall

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Splněno ANO/NE
Vlastnosti hardware		
Počet zařízení	2	ANO
chlazení boxu (airfflow)	předo-zadní (front-to-back)	ANO

Vlastnosti každého zařízení		Splněno ANO/NE
Formát zařízení	HW appliance	ANO FortiGate 1101E, Licence Advanced Threat Protection + FortiCare Premium bundle 5YR
Minimální počet 40 GbE QSFP+ rozhraní	2	ANO
Minimální počet 10 GbE SFP+ nebo 25 GbE SFP28/10 rozhraní	8	ANO
Zařízení obsahuje redundantní zdroje napájení	ano - 2 zdroje	ANO
Zdroj lze vyměnit za běhu (hot-swappable)	ano	ANO

Konzolový sériový port	1x	ANO
Podpora vytváření virtuálních izolovaných kontextu NGFW s vlastním konfiguračním rozhraním (řešení formou VRF není akceptovatelné)	min. 250 instancí	ANO
Integrovaný SSD disk	min. 2x 480 GB	ANO
Dedikovaný HA/Failover/SYNC interface (nezapočítaný do počtu interface výše)	ano	ANO

Funkcionalita firewallu - per chassis		**Splněno ANO/NE**
Počet současně otevřených TCP spojení aplikačního FW	min 8M	ANO
Rychlost vytváření nových TCP spojení přes aplikační FW (CPS)	min 500 k/s	ANO
Propustnost funkce ochrany před sítovými útoky (IPS), enterprise mix traffic	min. 12 Gbps	ANO
Propustnost funkce NGFW (stavový firewall, IPS, analýza a rozpoznávání aplikací na L7), enterprise mix traffic	min. 9.5 Gbps	ANO
Propustnost funkce ochrany proti sítovým hrozbám Threat Protection (stavový firewall, IPS, analýza a rozpoznávání aplikací na L7, ochrana před škodlivým kódem), enterprise mix traffic	min. 7 Gbps	ANO
Propustnost funkce IPSEC VPN (při použití AES256, SHA 256)	min. 45 Gbps	ANO
Minimální počet současných TCP spojení podléhajících současně funkci SSL inspekce	750 000	ANO
Propustnost funkce SSL inspekce	min. 10 Gbps	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	ANO
podpora 802.1Q tagovaných rámců	Ano	ANO
Minimálně počet VLAN	min. 1024	ANO
Vysoká dostupnost - stateful failover (active/standby)	Ano	ANO
Možnost sloučení více fyzických rozhraní - LACP 802.3ad	Ano	ANO
Dynamické směrování - min podpora alespoň OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – OSPFv3, BGP	Ano	ANO
Podpora Policy based Routing	Ano	ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Filtrace IPv4, IPv6	Ano	ANO
Možnost definovat platnost pravidla v čase (pravidlo funguje pouze v daném časovém rámci)	Ano	ANO
Funkce identity based firewallingu AD a Cisco ISE pomocí mechanismu PxGrid	Ano	ANO
Inspekce IPv6 provozu	Ano	ANO

Filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
IPS/IDS funkcionalita	Ano	ANO
Řízení rychlosti datových toků na úrovni pravidel FW (QoS)	Ano	ANO
FQDN objekty v přístupových pravidlech	Ano	ANO
Export logů protokolem SYSLOG as per RFC 5424 (nebo z managementu)	Ano	ANO
Protokol NTP (RFC 5905)	Ano	ANO
Protokol SNMP - v1, v2 i v3	Ano	ANO
Dostupná MIB pro SNMP daného zařízení	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy (může být nahrazeno API rozhraním na úrovni centrálního managementu)	Ano	ANO
Funkce IKEv1 a IKEv2 pro IPSEC	Ano	ANO
IPsec (ESP/AH)	Ano	ANO
Podpora algoritmů s Eliptický křivkami (např. ECDH apod.)	Ano	ANO
Podpora moderních hashovacích algoritmů SHA256-HMAC a SHA512-HMAC	Ano	ANO
Podpora Netflow	min. V9 a IPFIX	ANO

Funkce Next-Gen FW		**Splněno ANO/NE**
Dešifrování TLS komunikace (SSL dekrypce) včetně TLS 1.3	Ano	ANO
Vzájemná propojitelnost s cílem sdílení provozních informací a incidentů s ostatními nabízenými komponentami	Ano	ANO
Podpora aplikační firewall - rozeznávání aplikací (Layer7)	Ano	ANO
Min. počet rozeznávaných aplikací	Min. 4000	ANO
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO
Aplikace v databázi aplikací výrobce FW jsou kategorizovány a je posouzen jejich risk faktor	Ano	ANO
Geolokace v pravidlech - geolokační databáze, výrobcem udžovaná	Ano	ANO
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO
Podpora IDS režimu	Ano	ANO
Inspekce pro IPv4 i IPv6 v rámci IPS	Ano	ANO
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě	Ano	ANO
Možnost vytváření vlastních signatur pomocí popsané syntaxe (pro funkci IPS i pro funkci rozpoznávání aplikací L7)	Ano	ANO
Podpora automatické aktualizace IPS signatur/databáze	Ano	ANO
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO
Detailní popis k odhalenému bezpečnostnímu incidentu (např. odkaz na Wikipedii, stránky výrobce, CVE, …	Ano	ANO
IPS politiku lze aplikovat na různé firewally	Ano	ANO
Ochrana proti škodlivým IP/URL/DNS v internetu (známé BOT a C&C)	Ano	ANO

Možnost rozšíření o funkce URL filtrace na základě kategorie/reputace	Ano	ANO
Možnost zadat přehodnocení kategorie/reputace výrobci FW k posouzení	Ano	ANO
Dynamické seznamy URL a IP	Ano	ANO
Zadávání vyjímek (false positive - whitelisting)	Ano	ANO

Síťová analýza provozu – 1ks HW kolektor

Minimální požadované vlastnosti a funkce řešení

Požadované funkcionality/vlastnosti	Splněno ANO/NE
Je požadován 1x HW datový kolektor **pro zpracování min. typu NetFlow dat z aktivních prvků o celkovém objemu do 30Gbps zpracovávaných NetFlow dat.** **Minimální celková disková kapacita úložiště je** 50TB diskového uložiště **skládajícího se z kombinace NVMe a SSD disků pro** uchování 180 dnů **datové retence.** **Požadované rozhraní pro sběr NetFlow dat je 2x 1GE a 2x 10GE.** **Dále je vyžadován alespoň 1x 1GE pro management port.** **Součástí dodávky bude i 5 letý support, zaškolení a 20MD ročně na konzultaci a konfigurace dle přání zadavatele.** **Požadujeme možnost budoucí rozšiřitelnosti o sensor s propustností min. 40Gbps/**	ANO, HW server Kolektor model XXL / 50TB NVMe RAID6 datové úložiště/ HW-C-XXL/ + GreyCortex Mendel perpetuální SW licence: Plná funkcionalita/ MA-C-50k-SW + 5 let podpora
Systém pro bezpečnostní analýzu síťového provozu **Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální anomální chování a musí o nich v reálném čase vytvářet upozornění.** **Systém zajišťuje detailní viditelnost do síťové komunikace s drill down prokliky na veškerá uložená data.** **Všechny komponenty systému musí být instalované v interním prostředí zadavatele („on premise“) a použití externích komponent nebo cloudových služeb se nepřipouští.**	ANO
Analýza protokolů typu NetFlow **Dodaný systém musí analyzovat síť na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.**	ANO
Uchování a vyhledávání síťových toků **Je požadováno vysokorychlostní úložiště pro uchování datových toků na dobu minimálně 180 dnů.** **Dále je požadováno, aby uživatel mohl v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě minimálně těchto parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (klient nebo server), číslo portu, VLAN, země.**	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Filtrováním a vyhledáváním v reálném čase se rozumí, že výsledek jakéhokoliv dotazu nad jakýmikoliv daty v 24hodinovém intervalu bude zobrazen maximálně do 60 vteřin.	
Automatická identifikace důležitých systémů **Je požadována automatická detekce přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod.** **Systém musí být schopen upozornit na vznik nových služeb v interní síti a sledovat jejich změny, a to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Direktory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTPS, POP3S, IMAPS, MSSQL, TELNET, FTP, TFTP, a to i v případě, že nebudou využívat standardních „well known" portů.**	ANO
Požadavky na schopnost detekce bezpečnostních událostí	
Monitorování zařízení, segmentů sítě a využívaných síťových služeb **Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:** **změna IP/MAC adresy hosta,** **duplicitní IP/MAC adresa,** **změna VLAN,** **vytvoření nové podsítě,** **připojení nového zařízení,** **použití nové služby,** **nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,** **přístup nového zařízení ke službě či zařízení.** **Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.**	ANO
Samostatné učení behaviorálních aktivit a detekce anomálií **Systém musí používat matematické metody samostatného učení (např. strojové učení) pro analýzu síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.** **Systém musí mít schopnost na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména:** **odchylku od modelu pro přenos dat, toků a paketů,** **odchylku od modelu pro počet komunikačních partnerů a entropie na komunikačních portech,** **odchylku od modelu pro počet síťových toků a využitých síťových služeb,** **odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).** **Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.**	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Asistované učení a korelace událostí **Systém musí být schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.** **Systém musí být schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí – minimálně v rozsahu kritické a důležité.**	ANO
Aktuální databáze blacklistů **Systém musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v sítí prostřednictvím minimálně denně aktualizovaných reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze.**	ANO
Požadavky na zajištění síťové viditelnosti	
Vyhledávání, filtrování a vizualizace všech dat **Systém musí být schopen okamžitého vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů.** **Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech zpracovávaných dat, tj. bezpečnostních událostí a zaznamenaných síťových toků, a to minimálně podle parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.** **Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.** **Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.**	ANO
Kontextuální informace **Systém musí být schopen pro každé zařízení získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace:** **Jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie** **Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu** **IP geolokace** **IP reputace, vč. údaje, jestli je IP adresa blacklistovaná nebo podezřelá** **Historie použitých MAC adresa a výrobce zařízení** **Operační systém a jeho historie na zařízení** **Uživatelem zadané poznámky a informace k zařízení**	ANO
Monitoring výkonu aplikací a sítě **Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty nebo jiné parametry) model normálního chování pro výkonnostní parametry minimálně:**	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

přenosová rychlost sítě, **rychlost odezvy aplikace,** **odezva systému z pohledu uživatele,** **informace o retransmission a out of order paketech.** **Výkonnostní anomálie na jednotlivých zařízeních a jejich službách jsou reportovány uživateli.**	
Jednotné grafické rozhraní **Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.**	ANO
Uživatelské profily a nastavení **Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:** **granulární nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),** **granulární nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),** **vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,** **vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.**	ANO
Požadavky na procesní zpracování kybernetických událostí	
Management bezpečnostních událostí a incidentů **Systém musí poskytovat integrované rozhraní pro:** **reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),** **spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,** **jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,** **možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).**	ANO
Požadavky na integraci, reporting a alerting	**Splněno ANO/NE**
Integrace **Systém musí být schopen rychlé a jednoduché uživatelské integrace s nástroji třetích stran:** **nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,** **nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů** **s dalšími nástroji prostřednictvím okamžitě definovatelných a jednoduše použitelných odkazů (URL) na požadované pohledy v nástroji.**	ANO
Automatické bezpečnostní hlášení (alerty) **Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně**	ANO

emailu a logu o: **všech identifikovaných událostech,** **událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.** **Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní aplikace.**	
Možnost automatizovaného reportingu **Možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).** **Je požadováno vytváření reportů v českém jazyce.**	ANO
Jednotné ovládání **Síťová analýza provozu musí být rozšiřitelná o sondu ve své behaviorální bezpečnostní funkci a mít stejné GUI rozhraní ovládání jako má Bezpečností analýza služeb**	ANO

Bezpečnostní analýza služeb

Minimální požadované vlastnosti a funkce řešení

Požadované funkcionality/vlastnosti	Splněno ANO/NE
Je požadován 1x HW datový kolektor a sensor společně pro zpracování síťové komunikace **o celkové propustnosti alespoň 200Mbps s monitorovacím rozhraním min. 2x 1GE RJ-45.** **Minimální celková disková kapacita úložiště je 2TB SSD.** **Součástí dodávky bude i 5 letý support, zaškolení a 10MD ročně na konzultaci a konfiguraci dle přání zadavatele.**	ANO, HW server kolektor All-in-one model S / HW-SC-S + GreyCortex Mendel perpetuální SW licence: Plná funkcionalita /MA-SC-200-SW + 5 let podpora
Systém pro bezpečnostní analýzu síťového provozu **Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.** **Systém zajišťuje detailní viditelnost do síťové komunikace s drill down prokliky na veškerá uložená data.** **Všechny komponenty systému musí být instalované v interním prostředí zadavatele („on premise“) a použití externích komponent nebo cloudových služeb se nepřipouští.**	ANO
Analýza plného síťového provozu s využitím sensoru **Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další**	ANO

zařízení v síti. **Systém musí být schopen získávat data zrcadlené komunikace ze SPAN portů a síťových TAPů.** **Systém je zcela pasivní vzhledem k monitorovanému provozu, monitorovaný provoz přes něj neprochází.**	
Analýza protokolů typu NetFlow **Dodaný systém musí analyzovat síť na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.**	ANO
Ukládání síťových toků s využitím sensoru **Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.** **Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, LDAP, KERBEROS, SNMP, CIFS, SMTPS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, SSL/TLS zapouzdření.**	ANO
Uchování a vyhledávání síťových toků **Je požadováno vysokorychlostní úložiště pro uchování datových toků na dobu minimálně 180 dnů složené.** **Dále je požadováno, aby uživatel mohl v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě minimálně těchto parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (klient nebo server), číslo portu, VLAN, země, ASN.** **Filtrováním a vyhledáváním v reálném čase se rozumí, že výsledek jakéhokoliv dotazu nad jakýmikoliv daty v 24hodinovém intervalu bude zobrazen maximálně do 60 vteřin.**	ANO
Automatická identifikace důležitých systémů **Je požadována automatická detekce přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod.** **Systém musí být schopen upozornit na vznik nových služeb v interní síti a sledovat jejich změny, a to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Direktory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTPS, POP3S, IMAPS, MSSQL, TELNET, FTP, TFTP, a to i v případě, že nebudou využívat standardních „well known" portů.**	ANO
Požadavky na schopnost detekce bezpečnostních událostí	**Splněno ANO/NE**
Monitorování zařízení, segmentů sítě a využívaných síťových služeb **Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:**	ANO

• **změna IP/MAC adresy hosta,** • **duplicitní IP/MAC adresa,** • **změna VLAN,** • **vytvoření nové podsítě,** • **připojení nového zařízení,** • **použití nové služby,** • **nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,** • **přístup nového zařízení ke službě či zařízení.** **Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.**	
Detekce síťových služeb s využitím sensoru **Systém musí být schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu.**	ANO
Samostatné učení behaviorálních aktivit a detekce anomálií **Systém musí používat matematické metody samostatného učení (např. strojové učení) pro analýzu síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.** **Systém musí mít schopnost na základě modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména:** • **odchylku od modelu pro přenos dat, toků a paketů,** • **odchylku od modelu pro počet komunikačních partnerů a entropie na komunikačních portech,** • **odchylku od modelu pro počet síťových toků a využitých síťových služeb,** • **odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).** **Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.**	ANO
Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik s využitím sensoru **Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod.** **Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:** • **průzkumné aktivity v síti,** • **potenciální úniky dat,** • **detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,** • **detekce repetitivních vzorců chování na síti,**	ANO

• **detekce botnetů a ovládání kompromitované stanice,** • **detekce příznaků těžení kryptoměn,** • **útoky hrubou silou a enumerace dat,** • **rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.**	
Detekce na základě databáze známých hrozeb (signaturní detekce) s využitím sensoru **Systém musí být schopen identifikovat a reportovat události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices" a dalších rizik. Tato databáze musí být aktualizovaná minimálně na hodinové bázi. Nesmí se jednat o volně dostupnou/open-source databázi, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.** **Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7.** **Systém musí využívat tuto signaturní detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.** **Systém musí detekovat události na základě vysokého počtu signaturních pravidel** **Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu.**	ANO
Detekce přenosu škodlivých souborů s využitím sensoru **Systém musí být schopen v monitorovaném provozu porovnávat hash zachycených souborů s databázemi známých hashů škodlivých souborů.**	ANO
Analýza šifrované komunikace s využitím sensoru **Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.**	ANO
Kontrola platnosti certifikátů s využitím sensoru **Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.**	ANO
Asistované učení a korelace událostí **Systém musí být schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.** **Systém musí být schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí – minimálně v rozsahu kritické a důležité.**	ANO
Aktuální databáze blacklistů **Systém musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v síti prostřednictvím minimálně denně aktualizovaných**	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze.	
Požadavky na zajištění síťové viditelnosti	**Splněno ANO/NE**
Vyhledávání, filtrování a vizualizace všech dat **Systém musí být schopen okamžitého vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů. Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech zpracovávaných dat, tj. bezpečnostních událostí a zaznamenaných síťových toků, a to minimálně podle parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.** **Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.** **Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.**	ANO
Ukládání a vyhledávání aplikačních metadat s využitím sensoru **Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, Kerberos, SSL/TLS, ARP, MODBUS.** **V rámci metadat u HTTP, SMTP, SMB a NFS je požadováno ukládání informací o po síti přenášených souborech alespoň v rozsahu:** • **název souboru,** • **velikost souboru,** • **HASH souboru.**	ANO
Kontextuální informace **Systém musí být schopen pro každé zařízení získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace:** • **Jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie** • **Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu** • **IP geolokace** • **IP reputace, vč. údaje, jestli je IP adresa blacklistovaná nebo podezřelá** • **Historie použitých MAC adresa a výrobce zařízení** • **Operační systém a jeho historie na zařízení** • **Uživatelem zadané poznámky a informace k zařízení**	ANO

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Monitoring výkonu aplikací a sítě **Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty nebo jiné parametry) model normálního chování pro výkonnostní parametry minimálně:** • **přenosová rychlost sítě,** • **rychlost odezvy aplikace,** • **odezva systému z pohledu uživatele,** • **informace o retransmission a out of order paketech.** **Výkonnostní anomálie na jednotlivých zařízeních a jejich službách jsou reportovány uživateli.**	ANO
Zaznamenávání a ukládání plného provozu s využitím sensoru **Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.**	ANO
Jednotné grafické rozhraní **Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.**	ANO
Uživatelské profily a nastavení **Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:** • **granulární nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),** • **granulární nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),** • **vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,** • **vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.**	ANO
Požadavky na procesní zpracování kybernetických událostí	**Splněno ANO/NE**
Management bezpečnostních událostí a incidentů **Systém musí poskytovat integrované rozhraní pro:** • **reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),** • **spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,** • **jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,**	ANO

• **možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).**	
Požadavky na integraci, reporting a alerting	**Splněno ANO/NE**
Integrace **Systém musí být schopen rychlé a jednoduché uživatelské integrace s nástroji třetích stran:** • **nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,** • **nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů jako výše,** • **s dalšími nástroji prostřednictvím okamžitě definovatelných a jednoduše použitelných odkazů (URL) na požadované pohledy v nástroji.**	ANO
Automatické bezpečnostní hlášení (alerty) **Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o:** • **všech identifikovaných událostech,** • **událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.** **Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní aplikace.**	ANO
Možnost automatizovaného reportingu **Možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).** **Je požadováno vytváření reportů v českém jazyce.**	ANO

9.4. Ostatní parametry řešení

9.4.1. Kabeláž

Součástí řešení bude veškerá kabeláž LAN v potřebném množství pro propojení. Přesné délky požadovaných kabelů budou upřesněny v rámci přípravného prováděcího projektu. Pokud nějaký kabel bude v provedení Fiber Optic, budou potřebné optické transceivery součástí dodávky na obou stranách připojení. Výjimkou z tohoto bodu jsou vlastní propojovací optické kabely mezi lokalitami i uzly.

Implementační práce

Součástí dodávek jsou dále následující implementační a migrační práce:

- Předimplementační analýza a prováděcí projektová dokumentace včetně stanovení podrobného postupu prací a akceptačních kritérií, popisu a návrhu harmonogramu implementace a popisu detailní postupné migrace s důrazem na minimalizaci nutných odstávek provozu dle potřeb stávající RDS. A dále bezpečnostní návrh zapojení a maximální spolupráce všech dodaných zařízení v rámci tohoto projektu.
- Konfigurace všech HW a SW komponent, aby byl zajištěn provoz Servisních služeb RDS 2.0 dle předimplementační analýzy a prováděcího projektu
- Instalace dodaného hardware do racku v rámci uvažovaných datových lokalit
- Zapojení do napájení
- Zapojení do LAN
- Příprava návrhu služeb Služba bezpečného ověření identity a Adresářová služba do prostředí virtualizační platformy
- Akceptační testy instalovaného hw
- Projektové vedení
- Implementace komponent Služba bezpečného ověření identity a Adresářová služba do prostředí virtualizační platformy
- Zaškolení
- Podrobné nastavení těchto komponent za přítomnosti zadavatele
- Zapojení, konfigurace a nastavení zařízení HW do Out Off Band Management
- Hardening OS
- Akceptační testy zbytku
- Dokumentace dodaného řešení (Dokumentace skutečného stavu), ostatní dokumentace
- Školení

10. Obsah záruky

10.1. Základní záruka

Základní záruka je součástí ceny dodávky. Poskytovatel se zavazuje po dobu tří let základní záruky řešit nahlášené incidenty/vady v parametrech:

- Odezva: NBD
- Doba vyřešení závady: 5NBD
- Způsob vyřešení: onsite
- Účel: Oprava vad a řešení incidentů vedoucích k udržení parametrů daných Akceptačním protokolem.

a z tohoto důvodu vést systém zaznamenání incidentu/vady, minimálně na úrovni emailové schránky v režimu 24x7x365

Součástí základní záruky je také:

- Dodání bezpečnostních a systémových záplat.
- Upozornění na významné zranitelnosti.

10.2. Rozšířená záruka a servisní podpora

Součástí požadavku zapojení je vysoká dostupnost na úrovni active-active. Tím je vytvářena služba Management modulu, která musí mít dostupnost (SLA) na úrovni minimálně 99,5%. Tato dostupnost platí tedy na službu, potažmo na celé HA řešení. Jednotlivá zařízení nejsou tedy u takto vysokého SLA brána v potaz. Pro jednotlivá zařízení platí zmenšené SLA jako v celém projektu – 98%. Ale pouze za podmínky dostupnosti služby jako takové (celého řešení).

Dále je součástí rozšířené záruky a servisní podpory:

a) Udržení dostupnosti 24x7x365 předmětu plnění v kvalitě předané akceptačním protokolem, tedy spolupráce s objednatelem nebo jím určenou třetí stranou na identifikaci a návrhu řešení případného incidentu a obnovení dostupnosti prvku/služby v požadovaných parametrech, viz níže.

b) Provoz Helpdesk

c) Provoz Hotline

e) Maximální součet doby poruch – 3,5h/měsíc

f) Požadovaná garance dostupnosti – 99,5%/účtované období

g) Maximální doba odezvy při nahlášení poruchy – viz tabulka dle kategorie incidentu

h) Povolený počet hodin plánovaných výpadků – 1%/měsíc

i) Report stavu provozu jako součást vyúčtování

l) Servisní tým – management a vybavení servisního týmu Poskytovatele připraveného zasáhnout v případě poruchy v nejbližším možném čase pro splnění smluvního vztahu

m) Aktivní činnost Poskytovatele předcházející nedostupnosti předmětu smlouvy či jeho délce na základě podnětů z další činnosti a best practise (např. upozornění na zranitelnosti či bezpečnostní záplaty)

n) Obnova dostupnosti předmětu smlouvy dle sjednaných parametrů při zavinění (byť i částečného) Objednatele, třetí strany či vyšší moci – max. 1 / rok /každá kategorie jako součást plateb „za službu servisu“.

o) Přístupy servisního týmu do prostor objektů Partnerů projektu (ukončení tras) se může řídit metodickými pokyny Partnerů projektu. Pokud nejsou metodiky známy, anebo poskytovateli předloženy, musí mít každý člen servisního týmu platný občanský průkaz nebo platný cestovní pas pro identifikaci a případně i ztotožnění v prostorách Partnerů projektu.

10.3. Kategorie incidentů a příslušné odezvy

V následujících tabulkách jsou zobrazeny požadované parametry odezev pro incidenty A, B, C a definice jednotlivé kategorie incidentů.

Tabulka č. 13 – Požadavky na garantované parametry SLA

Kategorie incidentu	Garantovaná doba přijetí a akceptace hlášeného incidentu	Garantovaná doba zahájení prací na řešení incidentu po řádném nahlášení a maximální doba pro pravidelné ohlašování stavu incidentu	Garantovaná doba obnovení služby
A	30 min	2 hod	do 12 h
B	30 min	4 hod	Next day
C	60 min	Next business day	5 pracovních dní
Konfigurace / změna na požádání zadavatelem	60 min	--	Next business day

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Tabulka č. 14 – Kategorie incidentů

Kategorie incidentů
Incident/vada kategorie A
Prvek IT/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.
Prvek IT/služba má známou zranitelnost nebo nemá bezpečnostní aktualizace doporučené výrobcem.
Incident/vada kategorie B
Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz.
Prvky nejsou stejně nakonfigurované nebo zazáplatované.
Incident/vada kategorie C
Ostatní drobné incidenty/vady, které nespadají do kategorií A a/nebo B.

Tyto parametry jsou výchozími požadavkem zadavatele, zhotovitel může navrhnout parametry úměrně přísnější s ohledem na kvalitu jím realizované sítě.

11. Školení

Zadavatel požaduje vyškolení administrativního týmu zadavatele ve všech technologiích a administrativních postupech potřebných k provozu a bezpečnosti sítě.

Školení proběhne v místě sídla zadavatele nejdříve v době testovacího provozu, materiály jsou dodány týden před vlastním školením, pokud není níže u jednotlivých školení řečeno jinak.

Zaškolení předchází implementaci nebo je její součástí.(doba implementace se však do školení nepočítá)

11.1. Povinné oblasti zaškolení pro 2 osoby zadavatele a 2 osoby servisní organizace

- Analytické bezpečnostní nástroje - – 5MD
- Firewally administrace, management – 3 MD
- Firewally nastavení pravidel a funkcí– 3MD
- OpenLDAP, AAA – 2MD
- RADIUS/TACACS+ - 2MD

11.2. Certifikované školení

Zadavatel dále vyžaduje, aby min. 2 správci určení zadavatelem procházeli na náklady zhotovitele pravidelným školením s certifikovaným lektorem na technologie užité v síti. Školení v době ostrého provozu nemusí být na stejných zařízeních ani na zařízeních stejného výrobce, vyučovací postupy však musí vést ke konfiguracím dle standardů užitých v síti. Časový rozsah každého školení je min. 5MD na osobu a může být složen z více navazujících kurzů. Jazykem školeni je čeština. Školení nemusí být realizováno v sídle zadavatele. Materiály ke školení musí být předány školenému nejdéle první den školení.

Požadovaný harmonogram:

- Realizace projektu – 1x administrace Firewallu
- Druhý rok provozu – 1x Linux bezpečnost
- Třetí rok provozu – 1x Firewally, opakování

Zhotovitel vždy nabídne tři termíny každého školení v průběhu roku pro možnost přihlášení osob zadavatele.

12. Požadavky na dokumentaci

Struktura dokumentace musí současně splňovat také dotační podmínky. Dokumentace budou v českém jazyce, technické výrazy mohou být v jazyce anglickém. Předaná dokumentace je 1x ve standardním editovatelném formátu pro elektronickou formu (např. MS Office – Word, Excel, Visio a Open Office) a 1x v needitovatelném standardním formátu, např. PDF. Tištěná verze je také min. v jedné kopii. Zmenšit rozsah dokumentací může pouze zhotovitel.

Dokumentace zde uvedená je předána v sídle zhotovitele.

12.1. Prováděcí dokumentace

1) Před spuštěním implementace díla předloží zhotovitel do 4 týdnů od účinnosti smlouvy návrh prováděcí dokumentace ke schválení. Schválení mimo zadavatele provádí i oprávněná osoba ze sídla umístění uzlu sítě. Implementace poté bude v souladu s prováděcí dokumentací. V případě zadavatelem požadovaných úprav dokumentace, zhotovitel zpracuje pozměňovací verzi do 4 pracovních dní a znova předá dokumentaci ke schválení dle požadavků tohoto bodu.
2) Změna v průběhu implementace je podmíněna schválením zadavatele a případně jím určenou další osobou (v případě změny v objektech partnera projektu).
3) Dokument obsahuje všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění do stavu odpovídajícího požadovaným parametrům zadavatele. Dokumentace a popsané aktivity musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
    a. Detailní schéma fyzického zapojení včetně popisu, úrovní detailu je min. vlnová lamda /transceiver / port aktivního prvku.
    b. Detailní schéma logického schéma včetně popisu, úrovní detailu je vlan / vrf či jiná nejmenší virtuální jednotka.
    c. Detailní popis cílového stavu a funkcionalit jednotlivých částí.
    d. Popis zapracování adresního rozsahu, zapracování veřejných a dodavatelsky neutrálních adres zhotovitele.
    e. Způsob zajištění potřebných dodávek včetně technické podpory
    f. Způsob zajištění projektového řízení na straně uchazeče pro realizaci předmětu plnění
    g. Detailní návrh a popis postupu implementace předmětu plnění
    h. Detailní popis zajištění bezpečnosti informací

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

i. Detailní harmonogram projektu včetně uvedení kritických milníků. Minimální kritické milníky pro dokumentaci uzlu Krajský úřad Pk, kde budou i obecné informace pro zadavatele:
    i. Zahájení projektu
    ii. Provedení předimplementační analýzy včetně případné první návštěvy budoucího umístění uzlu.
    iii. Předání prováděcí dokumentace
    iv. Zahájení implementace předmětu plnění
    v. Školení
    vi. Zahájení testovacího (zkušebního) provozu. Testovací provozu bude trvat minimálně 3 týdny.
    vii. Akceptační testy – rozsah i způsob provedení. Popis provedení musí být v takovém detailu, aby šel test znova zopakovat. V případě zadavatelem požadovaných úprav dokumentace, zhotovitel zpracuje pozměňovací verzi do 4 pracovních dní a předá dokumentaci znova ke schválení.
    viii. Zahájení plného provozu
    ix. Návrh akceptačních kritérií a akceptačních testů
    x. Detailní popis navrhovaných školení
    xi. Detailní popis údržby systémů
    xii. Detailní struktura dalších dokumentací

12.2. Dokumentace skutečného provedení

1) V průběhu implementace provádí zhotovitel aktualizaci prováděcí dokumentace a spuštění ostrého provozu finalizuje dokumentaci odpovídající skutečnému stavu implementace. Součástí dokumentace je i výpis konfigurací jednotlivých aktivních prvků. V případě, že zařízení neumožňuje zobrazení konfigurace v čitelné podobě a zařízení má webové rozhraní, jsou součástí dokumentace screenshoty všeho nastavení.
2) Součástí předané dokumentace v elektronické podobě budou i zálohy všech aktivních prvků s poslední konfigurací.
3) Dokumentace skutečného provedení je zhotovitelem udržována v aktuálním stavu po dobu platnosti Smlouvy o servisní podpoře. Zálohy jsou i nadále prováděny, výpisy konfigurací jednotlivých aktivních prvků se v dokumentaci nadále neaktualizují.

12.3. Bezpečnostně-provozní dokumentace

1) Dokumentace popisující obecně stav sítě jako celku, následně se věnující bezpečnému provozu každého konkrétního uzlu z pohledu administrátorů daných uzlů.
2) Dokumentace uzlů Krajský úřad a Nemocnice Pardubice je podrobná, zahrnující informace o celé síti a rozšířená pro podrobný provoz a bezpečnou administraci celé sítě, včetně vnějšího perimetru, monitoringu a bezpečnosti.
3) Součástí dokumentace každého uzlu jsou minimálně:
4) Bezpečnostní pravidla z pohledu fyzické i síťové bezpečnosti ve vztahu k použitým aktivním prvkům a dodaným technologiím.
5) Bezpečnostní směrnice s popisem implementovaných a provozovaných bezpečnostních mechanismů a zásadami pro bezpečný provoz sítě

12.4. DR dokumentace

1) Dokumentace popisuje krok po kroku postupy při:
    - Spuštění systému
    - Řešení výpadku jedné komponenty. Popsány musí být možná řešení všech možných výpadků a přepnutí do redundantního režimu. Součástí je i popis správné funkce redundantní komponenty pro vizuální kontrolu.
    - Eskalační mechanismus základního ověření funkčnosti a poté nahlášení závady dle povahy konkrétního uzlu.

12.5. Dokumentace hesel

1) Zadavatel zakazuje jakákoliv hesla v ostatních dokumentacích, umožňuje pouze jednoznačný odkaz do dokumentace hesel.
2) Hesla jsou rozdělena v kapitolách po dokumentacích nebo dle abecedně vzestupně seřazených odkazů, pokud se zhotovitel nedohodne v přípravné fázi projektu se zadavatelem jinak.

12.6. Inventární dokumentace

1) Po realizaci celého projektu je zhotoviteli předán soupis všech zařízení, každé identifikované svým produktovým označením, umístěním, množstvím v daném umístění, sériovým číslem (pokud existuje), zařazením do kategorie (služba, hardware, software, příslušenství k hw, licence k hw, jiné) a cenovým ohodnocením dané položky.

12.7. Dokumentace o licencích

1) Zadavatel obdrží soupis zařízení s připsanými jednotlivými licenčními politikami včetně případných licenčních čísel nebo kódů a jejich platnosti.

12.8. Analýza rizik

1) Zhotovitel na základě analýzy definuje možná rizika provozu Regionální datové sítě v každém uzlu zvlášť a navrhne možná opatření pro jejich snížení. Realizace opatření není součástí projektu.
2) Metodika stanovení rizik musí být standardizovaná a zopakovatelná. Zadavatel doporučuje metodiku vyhlášky č. 82/2018Sb., o kybernetické bezpečnosti.

12.9. Materiály k proběhlému školení

Případné další materiály jako reakce na otázky při školení

12.10. Upozornění k dokumentaci

Dokumentace hesel a bezpečnostní dokumentace je na přední straně výrazně označena názvem a textem v červené barvě na kontrastním podkladu:

TLP:RED – Dokument důvěrného charakteru v majetku oddělení informatiky Pardubického kraje. Je zakázáno pořizování kopií nebo zapůjčení třetí osobě bez svolení vedoucího oddělení informatiky Pardubického kraje!

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

13. Bezpečnostní vymezení

Zadavatel provedl na základě Varování Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17.12.2018 hodnocení rizik potencionálního provozu technických a programových prostředků vzešlých z této veřejné zakázky od společnostní zmíněných ve Varování NÚKIB.

Zadavatel jako osoba uvedená v §3 písm. c) až f) zákona o kybernetické bezpečnosti v tomto případě zohledňuje požadavky vyplývající z bezpečnostních opatření při výběru dodavatele na technické a programové prostředky dle §4 odst. 4 stejného zákona a tímto se proti společnostem zmíněných ve Varování NÚKIB v tomto případě **vymezuje a nabídka s produkty** těchto společností **bude vyloučena**.

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Příloha č. 2 smlouvy
Vzor akceptačního protokolu

AKCEPTAČNÍ PROTOKOL

Poskytovatel	[BUDE DOPLNĚNO]
Objednatel	**Pardubický kraj**
Smlouva	*Smlouva o dodávce HW a SW a o poskytování souvisejících služeb č.* [BUDE DOPLNĚNO]
Název Projektu	„Modernizace infrastruktury pro sdílení informací a dat s obcemi Pardubického kraje“
Číslo Projektu	CZ.06.3.05/0.0/0.0/16_044/0006323
Datum předání	[BUDE DOPLNĚNO]
Předávací protokol č.	[BUDE DOPLNĚNO]

Popis dílčího plnění	Akceptováno bez výhrad	Akceptováno s výhradou	Neakceptováno

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

V Pardubicích dne ……

V …… dne ……

_____

[BUDE DOPLNĚNO]

_____

[BUDE DOPLNĚNO]

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Příloha č. 3 smlouvy

Hlášení poruchy

K odeslání elektronickou poštou na adresu [redacted]

Číslo smlouvy o servisní činnosti: [BUDE DOPLNĚNO]

Pracovník odpovídající za správnost hlášení:

Jméno: …… tel: …… e-mail: ……

Datum a čas hlášení poruchy: ……

Navrhovaný stupeň priority: ……

Informace o místě instalace:

Adresa: …… tel/fax: ……

Popis poruchy:

Příloha č. 3 Zadávací dokumentace – Závazný návrh smlouvy

Příloha č. 4 smlouvy

Protokol o provedení servisní činnosti

Jméno zástupce poskytovatele: …….

Název lokality, kde byl proveden zásah: ……

Adresa: ……

Datum a čas nahlášení poruchy: ……

Datum a čas odstranění poruchy: ……

Informace o servisovaném prvku KI a poruše:

……

Popis poruchy:

Způsob odstranění poruchy:

Razítka, jména a podpisy odpovědných osob:

_____ za objednatele

_____ za poskytovatele