

## ZMLUVA O DIELO

uzatvorená podľa § 536 a nasl. zákona číslo 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „**Obchodný zákonník**“)  
(ďalej len „**Zmluva o dielo**“)

### Článok 1. ZMLUVNÉ STRANY

**Objednávateľ:** **Mesto Šaľa**  
sídlo: Námestie Sv. Trojice 7, 927 15 Šaľa  
IČO: 00306185  
DIČ / IČ DPH: 2021024049 / nie je platiteľ DPH  
v mene ktorého koná: Mgr. Jozef Belický, primátor mesta  
bankové spojenie: Slovenská sporiteľňa a. s.  
IBAN: SK7909000000005139388575  
e-mail: mesto@sala.sk  
(ďalej len „**Objednávateľ**“)

a

**Zhotoviteľ:** **airo, s. r. o.**  
sídlo: Ivanská cesta 30/B, 821 04 Bratislava  
IČO: 48286621  
DIČ / IČ DPH: 2120122488 / SK2120122488  
registrovaný: v Obchodnom registri Okresného súdu Bratislava I, Oddiel: Sro  
Vložka č. 106156/B  
v mene ktorého koná: Mgr. Jakub Čeles, Ing. Rudolf Törvényi, Ing. Štefan Kopaj  
bankové spojenie: Tatra banka, a.s.  
číslo účtu v tvare IBAN: SK8211000000002941044557  
e-mail: info@airo.sk  
(ďalej len „**Zhotoviteľ**“)  
(Objednávateľ a Zhotoviteľ spoločne aj ako „**Zmluvné strany**“)

### ÚVODNÉ USTANOVENIA

- A. Objednávateľ potrebuje na plnenie svojich zákonných úloh a riadny výkon správy zabezpečiť dodanie informačných a komunikačných technológií, hardvérového a softvérového vybavenia, licencií a služieb pre projekt „**Zvýšenie kybernetickej bezpečnosti mesta Šaľa**“, kód **311071BPN3**, vrátane dopravy, inštalácie, testovania a zaškolenia obsluhy (ďalej len „**Dielo**“). Tento projekt je považovaný za Dielo vytvorené na základe tejto Zmluvy o dielo a uplatňuje sa naň príslušná platná a účinná legislatíva Slovenskej republiky. Objednávateľ na tento účel vyhlásil Verejné obstarávanie a Zhotoviteľ sa stal úspešným uchádzačom. Verejné obstarávanie sa týkalo zákazky rozdelenej na dve časti s tým, že táto Zmluva o dielo sa vzťahuje na časť I. predmetu zákazky v zmysle Výzvy na predkladanie ponúk.
- B. Účelom tejto Zmluvy o dielo je zabezpečenie vytvorenia Diela, ktoré bude v plnom rozsahu zodpovedať všetkým funkčným, technickým a legislatívnym požiadavkám Objednávateľa uvedeným v tejto Zmluve o dielo a vo Výzve na predmet zákazky Verejného obstarávania, a ktoré bude spôsobilým nástrojom na plnenie úloh Objednávateľa.
- C. Zmluvné strany, vedomé si svojich záväzkov obsiahnutých v tejto Zmluve o dielo a s úmyslom byť touto Zmluvou o dielo viazané, sa dohodli na uzatvorení tejto Zmluvy o dielo v nasledujúcom znení.

- D. Postup verejného obstarávania v zmysle § 117 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon o VO“), v ktorom bola ponuka Poskytovateľa predložená Objednávateľovi vyhodnotená ako najvýhodnejšia.
- E. Predmet tejto Zmluvy o dielo bude zo strany Objednávateľa financovaný z Operačného programu Integrovaná infraštruktúra („OPII“) a prostriedkov Objednávateľa.

## Článok 2. VYHLÁSENIA ZMLUVNÝCH STRÁN

- 2.1 Zhotoviteľ potvrdzuje, že je osobou vykonávajúcou podnikateľskú činnosť v súlade s právnym poriadkom SR a spĺňa všetky podmienky a požiadavky v zmysle tejto Zmluvy o dielo a Výzvy na predkladanie ponúk.
- 2.2 V prípade, ak sa stal Zhotoviteľ úspešným uchádzačom vo Verejnom obstarávaní ako člen Skupiny dodávateľov potvrdzuje, že Skupina dodávateľov, ktorej je členom pred podpisom tejto Zmluvy o dielo uzatvorila a predložila Objednávateľovi zmluvu, v ktorej sú jednoznačne stanovené vzájomné práva a povinnosti, kto sa akou časťou bude podieľať na plnení Diela, ako aj skutočnosť, že všetci členovia Skupiny dodávateľov sú zaviazaní zo záväzkov voči Objednávateľovi spoločne a nerozdielne a že Zhotoviteľovi bola udelená plná moc na vykonávanie všetkých právnych úkonov v mene všetkých členov Skupiny dodávateľov.
- 2.3 Zhotoviteľ vyhlasuje, že je spôsobilý uzatvoriť túto Zmluvu o dielo a riadne plniť záväzky z nej vyplývajúce a že sa oboznámil s podkladmi tvoriacimi výzvu na predkladanie ponúk vrátane jej príloh, ktoré ustanovujú požiadavky na predmet plnenia Diela a s touto Zmluvou o dielo.
- 2.4 Zhotoviteľ vyhlasuje, že má na realizáciu a dodanie Diela k dispozícii také nevyhnutné kapacity a technické schopnosti, aby splnil svoje povinnosti v zmysle tejto Zmluvy o dielo.
- 2.5 Zhotoviteľ vyhlasuje, že disponuje všetkými oprávneniami požadovanými príslušnými orgánmi a v zmysle príslušných právnych predpisov, ako aj kapacitami a odbornými znalosťami nevyhnutnými na riadnu a včasnú realizáciu Diela.

## Článok 3. PREDMET ZMLUVY

- 3.1 Predmetom tejto Zmluvy o dielo je úprava práv a povinností Zmluvných strán spojených so záväzkom Zhotoviteľa na vlastné náklady a nebezpečenstvo vykonať, riadne a včas a za cenu a podmienok dohodnutých ďalej v tejto Zmluve o dielo, Dielo spočívajúce v dodaní informačných a technológií, hardvérového a softvérového vybavenia a služieb pre projekt „**Zvýšenie kybernetickej bezpečnosti mesta Šaľa**“ vrátane dopravy, inštalácie, implementácie, testovania či zaškolenia obsluhy. Vykonanie Diela v sebe zahŕňa vytvorenie a dodanie výstupov z plnenia tejto Zmluvy o dielo, ako aj udelenie súhlasu na používanie predmetov práv duševného vlastníctva, ktoré boli vytvorené na základe alebo v rámci plnenia tejto Zmluvy o dielo, a to v uvedenom rozsahu, ako i dodanie alebo zabezpečenie poskytnutia potrebných licencií k SW produktom. Pre vylúčenie akýchkoľvek pochybností Zmluvné strany výslovne uvádzajú, že súčasťou plnenia na základe tejto Zmluvy o dielo je aj dodávka HW.
- 3.2 Záväzku Zhotoviteľa v zmysle tejto Zmluvy o dielo zodpovedá záväzok Objednávateľa riadne a včas vykonať Dielo alebo jeho časť prevziať a uhradiť Zhotoviteľovi cenu v rozsahu a za podmienok v zmysle tejto Zmluvy o dielo.
- 3.3 Ak sa budú na strane Zhotoviteľa, ako Zmluvnej strany podieľať viaceré subjekty, práva z tejto Zmluvy o dielo voči Objednávateľovi môže uplatňovať výlučne Zhotoviteľ. Zhotoviteľ bude vo vzťahu k Objednávateľovi zodpovedať za fakturáciu, dodávky častí Diela, vrátane všetkých a akýchkoľvek úkonov týkajúcich sa plnenia z tejto Zmluvy o dielo. Subjekty na strane Zhotoviteľa si osobitnou písomnou dohodou určia a vysporiadajú vzájomné záväzky a oprávnenia vyplývajúce im z tejto Zmluvy o dielo.

- 3.4 Zhotoviteľ sa zaväzuje riadne a včas vyhotoviť a dodať Objednávateľovi Dielo v rozsahu a za podmienok v zmysle tejto Zmluvy o dielo nasledovne:
- a) dodávka a vyhotovenie riešenia v súlade s Opisom predmetu zákazky pre časť I. predmetu zákazky, ktorý tvorí prílohu č. 1 Výzvy na predkladanie ponúk a v súlade s Návrhom na plnenie kritérií, ktorý tvorí prílohu č. 3 Výzvy na predkladanie ponúk a ktoré sú obsahom Prílohy č. 1 a Prílohou č. 2 tejto Zmluvy o dielo („Opis predmetu zákazky – časť I. a Návrh na plnenie kritérií časť I.“) a na základe požiadaviek Objednávateľa uvedených v tejto Zmluve o dielo a jeho dodanie Objednávateľovi v súlade s podmienkami uvedenými v tejto Zmluve o dielo,
  - b) realizácia riešenia vrátane implementácie a testovania v súlade s Opisom predmetu zákazky pre časť I. predmetu zákazky, ktorý tvorí prílohu č. 1 Výzvy na predkladanie ponúk Objednávateľom a ďalšími podmienkami v zmysle tejto Zmluvy o dielo:
    - i. doprava, inštalácia, nastavenie parametrov a ďalších nastavení HW A SW,
    - ii. testovanie a overenie funkčnosti a kompletnosti Diela alebo jeho časti,
    - iii. poskytnutie súčinnosti Objednávateľovi pri implementácii dodaného riešenia do informačného systému a pri jeho uvedení do prevádzky na príslušnom pracovisku Objednávateľa v súlade s podmienkami v zmysle tejto Zmluvy o dielo,
  - c) školenia – uskutočnenie školenia používateľov Diela alebo jeho časti v súlade s podmienkami v zmysle tejto Zmluvy o dielo,
  - d) ďalšie dodávky, činnosti a práce nevyhnutné pre realizáciu Diela alebo jeho časti alebo užívanie Diela alebo jeho časti Objednávateľom, ktoré nie sú výslovne stanovené ako povinnosť Objednávateľa v zmysle tejto Zmluvy o dielo.
- 3.5 Podrobná špecifikácia obsahu, rozsahu a spôsobu zhotovenia Diela je obsahom Prílohy č. 1 tejto Zmluvy o dielo, ktorá obsahuje:
- a) Opis predmetu zákazky – časť I,
  - b) Návrh na plnenie kritérií – časť I.
- 3.6 Zhotoviteľ sa zaväzuje vykonať Dielo alebo jeho časť najneskôr do 12 (slovom: dvanástich) mesiacov odo dňa účinnosti tejto Zmluvy o dielo, a to vrátane skúšobnej prevádzky podľa Článok 6. tejto Zmluvy o dielo.
- 3.7 Zhotoviteľ sa zaväzuje vykonať Dielo v súlade s podmienkami v zmysle tejto Zmluvy o dielo, Výzvy na predkladanie ponúk a jej príloh, akejkoľvek ďalšej súvisiacej dokumentácie, ktorá mu je známa a v súlade s všeobecne záväznými právnymi predpismi SR a EÚ.

#### **Článok 4. PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN**

- 4.1 Objednávateľ sa zaväzuje:
- a) zabezpečiť Zhotoviteľovi v primeranom rozsahu potrebné informácie a prípadné konzultácie k plneniu predmetu tejto Zmluvy o dielo, ak bude Objednávateľ takými informáciami disponovať,
  - b) postupovať pri poskytovaní súčinnosti v zmysle tohto bodu 4.1 písm. a) tejto Zmluvy o dielo takým spôsobom, aby konal v súlade so Zákonom o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej aj ako len zákon o ITVS)

- c) za predpokladu dodržania bezpečnostných a prípadných ďalších predpisov Objednávateľa zabezpečiť pre Zhotoviteľa poverenia Zodpovednej osoby Zhotoviteľa nevyhnutné na plnenie tejto Zmluvy o dielo,
- d) za predpokladu dodržania bezpečnostných a prípadných ďalších predpisov Objednávateľa sprístupniť technickú, komunikačnú a systémovú infraštruktúru Objednávateľa pre zhotovovanie Diela alebo jeho časti v zmysle tejto Zmluvy o dielo a podľa potreby vzdialeného prístupu dohodnutou technológiou poskytnúť Zhotoviteľovi na jeho žiadosť súčinnosť ohľadom prístupu k všetkým zariadeniam, ku ktorým je jeho prístup potrebný pre zhotovenie Diela alebo jeho časti, vrátane zdrojov energie, elektronickej komunikačnej siete, vzdialeného prístupu, a to všetko v rozsahu nevyhnutnom pre riadne zhotovenie Diela alebo jeho časti v zmysle tejto Zmluvy o dielo na náklady Objednávateľa,
- e) zabezpečiť v nevyhnutnom rozsahu prítomnosť Zodpovednej osoby Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo v prípadoch vyplývajúcich z tejto Zmluvy o dielo,
- f) zabezpečiť Zhotoviteľovi všetky prípadné relevantné legislatívne, metodické, koncepčné, dokumentačné, normatívne a ďalšie materiály týkajúce sa Diela alebo jeho časti, ak bude Objednávateľ takými informáciami disponovať a Zhotoviteľ ich bude potrebovať k zhotoveniu Diela alebo jeho časti, to však len za predpokladu, že Zhotoviteľ nemá k takýmto materiálom sám prístup a len v rozsahu, v akom si tento prístup nevie Zhotoviteľ zabezpečiť sám.

#### 4.2 Zhotoviteľ sa zaväzuje:

- a) Zhotoviť a dodať Dielo riadne, včas, na svoje náklady a na svoje nebezpečenstvo, v súlade s požiadavkami Objednávateľa uvedenými v tejto Zmluve o dielo, vrátane jej príloh,
- b) postupovať s odbornou starostlivosťou, čestne, svedomito, hospodárne s využitím dostupných odborných znalostí a skúseností a v súlade s jemu známymi záujmami Objednávateľa,
- c) pri plnení tejto Zmluvy o dielo dodržiavať pokyny a podklady Objednávateľa, ktoré nie sú v rozpore s ustanoveniami tejto Zmluvy o dielo,
- d) bez zbytočného odkladu upozorniť Objednávateľa na nevhodnú povahu pokynov alebo podkladov poskytnutých Zhotoviteľovi zo strany Objednávateľa, ak mohol túto nevhodnosť zistiť pri vynaložení odbornej starostlivosti, a to elektronicky prostredníctvom e-mailovej adresy Zodpovednej osoby Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo; v prípade nevhodných pokynov Objednávateľa prerušiť dodávku Diela alebo jeho časti až do doby odstránenia alebo nahradenia nesprávnych alebo nevhodných pokynov,
- e) neodkladne písomne informovať Objednávateľa o každom prípadnom omeškaní, či iných skutočnostiach, ktoré by mohli ohroziť riadne a včasné zhotovenie Diela alebo jeho časti,
- f) nie byť zodpovedný za vzniknutú škodu, ktorú bolo možné vopred predvídať, spôsobenú Objednávateľovi porušením svojich povinností v zmysle tejto Zmluvy o dielo alebo všeobecne záväzných právnych predpisov,
- g) zodpovedať za to, že Dielo neobsahuje žiadne Objednávateľom nevyžiadané alebo neschválené vlastnosti,
- h) zabezpečiť vedenie pracovných výkazov a zabezpečiť, aby aj jeho Subdodávateľa priebežne viedli pracovné výkazy a bezodkladne ich poskytnúť na požiadanie,
- i) v rozsahu a za podmienok v zmysle tejto Zmluvy o dielo podávať Objednávateľovi tzv. správy o plnení tejto Zmluvy o dielo a zároveň sa zaväzuje, že pri plnení tejto Zmluvy o dielo bude bez zbytočného odkladu prerokúvať s Objednávateľom všetky otázky, ktoré by mohli negatívne ovplyvniť plnenie tejto Zmluvy o dielo,

- j) až do odovzdania a prevzatia Diela, ako celku, udržiavať jeho jednotlivé časti, ktoré sú už v prevádzke, v súlade s dodanou administrátorskou dokumentáciou a poskytovať Objednávateľovi nevyhnutnú súčinnosť za účelom ich užívania,
- k) povinný strpieť výkon kontroly/auditú súvisiaceho s plnením tejto Zmluvy o dielo kedykoľvek počas platnosti a účinnosti Zmluvy o poskytnutí nenávratného finančného príspevku č. 526/2022, uzatvorenej dňa 07.04.2022 medzi Objednávateľom, ako prijímateľom NFP, ktorej znenie je dostupné na <https://crz.gov.sk/zmluva/6334615/> („Zmluva o poskytnutí NFP“), a to zo strany oprávnených osôb na výkon tejto kontroly/auditú v zmysle príslušných právnych predpisov SR a EÚ, najmä ohľadom dodržiavania Zákona o EŠIF, Zákona č. 357/2015 Z. z. a Zmluvy o poskytnutí NFP a jej príloh vrátane príslušných všeobecných zmluvných podmienok a poskytnúť im riadne a včas všetku potrebnú súčinnosť,
- l) poskytnúť Objednávateľovi plnú súčinnosť pri riešení bezpečnostného incidentu a vyšetrovaní bezpečnostnej udalosti, ktoré súvisia s plnením tejto Zmluvy o dielo,
- m) poskytnúť Objednávateľovi kompletnú dokumentáciu týkajúcu sa Diela alebo jeho časti, vrátane administrátorských prístupov,
- n) zabezpečiť súlad dodávaného Diela alebo jeho časti so Zákonom o ITVS, zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“ a o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) (ďalej len „Zákon o e-Governmente“),
- o) zabezpečiť, aby zhotovené Dielo alebo jeho časť poskytovala funkcionality automatizovaného testovania každej služby na nefunkčnosť a odosielania (automatizovaných) hlásení o nefunkčnosti služby,
- p) pri plnení tejto Zmluvy o dielo dodržiavať relevantné ustanovenia všeobecne záväzných právnych predpisov a metodík.

## **Článok 5. MIESTO A TERMÍN VYKONANIA DIELA**

- 5.1 Miestom zhotovenia Diela alebo jeho časti je sídlo Objednávateľa s tým, že ak to technické podmienky umožňujú a ak sa Zmluvné strany na tom dohodnú, Zhotoviteľ môže zhotovovať Dielo alebo jeho časť aj prostredníctvom vzdialeného prístupu.
- 5.2 Zhotoviteľ sa zaväzuje zhotoviť Dielo alebo jeho časť najneskôr do 12 (slovom: dvanástich) mesiacov odo dňa účinnosti tejto Zmluvy o dielo a to vrátane skúšobnej prevádzky podľa Článok 6.12 tejto Zmluvy o dielo.
- 5.3 Zmluvné strany sa dohodli, že akúkoľvek zmenu týkajúcu sa miesta a termínu vykonania Diela alebo jeho časti je možné vykonať na základe uzatvorenia písomného dodatku k tejto Zmluve o dielo v zmysle ust. § 18 Zákona o VO.
- 5.4 Zmluvné strany sa osobitne dohodli, že ak by nastali nepredvídateľné okolnosti vyplývajúce napr. z opatrení v súvislosti s pandemiou ochorenia COVID 19, ktoré by mali vplyv na termín vykonania Diela, Zmluvné strany sú oprávnené uzatvoriť dodatok k tejto Zmluve o dielo v zmysle ust. § 18 Zákona o VO reflektujúci konkrétne v momente uzatvorenia tejto Zmluvy o dielo nepredvídateľné okolnosti.

## **Článok 6. ODOVZDANIE A PREVZATIE DIELA, VLASTNÍCKE PRÁVO A SKÚŠOBNÁ PREVÁDZKA**

- 6.1 Výsledkom odovzdania a prevzatia Diela alebo jeho časti je vyhotovenie a podpísanie akceptačného protokolu obidvoma Zmluvnými stranami (ďalej len „Akceptačný protokol“). Akceptačný protokol musí schválený a podpísaný Zodpovednou osobou Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo.
- 6.2 Ak to vyplýva z povahy Diela alebo jeho časti, Zmluvné strany vykonajú skúšobné a akceptačné testy Diela alebo jeho časti, o ktorých vyhotovia zápisnicu (ďalej len „Zápisnica z testov“). Zmluvné strany sa dohodli, že pri vykonávaní skúšobných a akceptačných testov musí byť vždy prítomná Zodpovedná osoba Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo a Zodpovedná osoba Zhotoviteľa podľa bodu 12.4 tejto Zmluvy o dielo alebo nimi preukázateľne splnomocnená osoba, inak sa tieto testy nevykonajú. Zápisnica z testov musí obsahovať najmä identifikáciu Zmluvných strán a oprávnených osôb, ktoré sa zúčastnili skúšobných a akceptačných v ich mene, identifikáciu Diela alebo jeho časti, na ktorej prebehli skúšobné a akceptačné testy, výsledok týchto testov, zistené vady a lehotu na odstránenie zistených väd Zhotoviteľom.
- 6.3 Odovzdanie Diela alebo jeho časti sa považuje za zrealizované podpísaním Akceptačného protokolu oboma Zmluvnými stranami, ktorého súčasťou bude aj Zápisnica z testov. Zmluvné strany sa zaväzujú podpísať Akceptačný protokol v 4 (slovom: štyroch) vyhotoveniach, z ktorých každá zo Zmluvných strán obdrží 2 (slovom: dve) vyhotovenia. Akceptačný protokol musí obsahovať najmä identifikáciu Zmluvných strán, ich zodpovedných osôb, špecifikáciu odovzdávaného a preberaného Diela alebo jeho časti a prílohy v zmysle tejto Zmluvy o dielo.
- 6.4 Prílohami Akceptačného protokolu budú:
- Zápisnica z testov,
  - prezenčné listiny zo školení vykonaných v rámci plnenia tejto Zmluvy o dielo a,
  - ak bude preberané plnenie Diela alebo jeho časti, na ktoré sa vzťahuje Vyhláška 78/2020 Z. z., Vyhláška 85/2020 Z. z. a Vyhláška 179/2020 Z. z., tak vyhlásenie o dodržaní štandardov pre ISVS/ITVS formou podrobného odpočtu splnenia jednotlivých relevantných požiadaviek.
- 6.5 Ak sa bude odovzdanie a prevzatie týkať Diela alebo jeho časti, ktorá vyžaduje osvedčenie kvality, Zhotoviteľ je povinný priložiť k Akceptačnému protokolu aj dokumenty a doklady osvedčujúce kvalitu alebo kompletnosť Diela alebo jeho časti (napr. zoznam dodávok a zariadení, osvedčenie o akosti a kompletnosti, návody na montáž a obsluhu, testy, správy o vykonaní odborných prehliadok a skúšok, výsledky testovania a skúšok, certifikáty, osvedčenia o vykonaných skúškach, použitých materiáloch a výrobkoch, doklady o spôsobe likvidácie odpadov a i.), a to za predpokladu, že takéto dokumenty a doklady neboli súčasťou ponuky predloženej Objednávateľovi vo verejnom obstarávaní.
- 6.6 Akceptačné testy sa vykonajú v prostredí a na infraštruktúre Objednávateľa a v oddelených testovacích prostrediach (t. j. bez možnosti ovplyvniť bežnú činnosť Objednávateľa, mimo produkčných databáz), ak sa Zmluvné strany vopred výslovne nedohodnú inak.
- 6.7 Ak sa Zmluvné strany nedohodnú inak, Zhotoviteľ je povinný odovzdať Objednávateľovi dokumentáciu k Dielu alebo jeho časti v elektronickom formáte na CD alebo DVD nosiči alebo na inom vhodnom, Zmluvnými stranami odsúhlasením nosiči dať a v prípade potreby a požiadavky Objednávateľa aj v 1 (slovom: jednom) vyhotovení v písomnej forme. Proces akceptácie dokumentácie, ktorá je súčasťou Diela alebo jeho časti bude po jej doručení Objednávateľovi zo strany Zhotoviteľa akceptovaná nasledovne:
- Objednávateľ je oprávnený zaslať pripomienky k dokumentácii k Dielu alebo jeho časti v dohodnutom formáte v lehote 10 (slovom: desiatich) kalendárnych dní odo dňa jej odovzdania Objednávateľovi; v prípade, ak Objednávateľ v tejto lehote nezašle Zhotoviteľovi žiadne pripomienky, dokumentácia k Dielu alebo jeho časti sa považuje za akceptovanú, t. j. odovzdanú,

- b) Zhotoviteľ je povinný odborne posúdiť pripomienky Objednávateľa podľa bodu 6.7 písm. a) tejto Zmluvy o dielo a upraviť dokumentáciu k Dielu alebo jeho časti v súlade so vznesenými pripomienkami Objednávateľa; v prípade, ak nie je možné niektorú z pripomienok Objednávateľa akceptovať, Zhotoviteľ túto skutočnosť bezodkladne oznámi a vysvetlí Objednávateľovi,
  - c) Objednávateľ je povinný najneskôr v lehote do 7 (slovom: siedmich) pracovných dní od dodania dokumentácie k Dielu alebo jeho časti po zapracovaní pripomienok podľa bodu 6.7 písm. b) tejto Zmluvy o dielo preveriť spôsob zapracovania pripomienok zo strany Zhotoviteľa a v prípade existencie nejakej výhrady zaslať Zhotoviteľovi v tejto lehote svoje stanovisko; v prípade, ak Objednávateľ nezašle Zhotoviteľovi svoje stanovisko s prípadnou výhradou, dokumentácia k Dielu alebo jeho časti sa považuje za akceptovanú, t. j. odovzdanú.
- 6.8 Zhotoviteľ je povinný dodať Objednávateľovi súčasne s dodaním Diela alebo jeho časti dokumentáciu minimálne v súlade a v rozsahu relevantných ustanovení Prílohy č. 1 k Vyhláske 85/2020 Z. z:
- a) technickú dokumentáciu v slovenskom jazyku v elektronickej forme na CD/DVD, ktorá bude obsahovať postup skompilovania aplikácie, dátový model Diela, popis integračnej, aplikačnej a technickej architektúry, väzby na iné systémy, popis tokov dát, procesné modely elektronických služieb,
  - b) prevádzkovú dokumentáciu v slovenskom jazyku v elektronickej forme na CD/DVD, ktorá bude obsahovať inštalčný postup aplikácie, konfiguráciu systémového SW, serverov a pracovných staníc, chybové stavy a postup ich riešenia, popis mechanizmu riadenia prístupu užívateľov k dátam a k funkciám aplikácie, popis procedúr pre zálohovanie a obnovu dát, popis použitých a navrhovaných technických číselníkov, ich naplnenie pri inicializácii,
  - c) užívateľskú dokumentáciu v slovenskom jazyku v písomnej forme v počte 2 (slovom: dvoch) kusov a v elektronickej forme na CD/DVD, ktorá bude obsahovať popis počítačového programu a jeho funkcií, postupy a úkony potrebné pre riadne užívanie počítačového programu, chybové a neštandardné stavy a dostupné spôsoby ich riešenia.
- 6.9 Po úplnom odovzdaní Diela alebo jeho poslednej časti podľa tohto Článok 6. tejto Zmluvy o dielo Zmluvné strany vyhotovia záverečný Akceptačný protokol (ďalej len „Záverečný akceptačný protokol“), ktorého podpísaním sa má za to, že Dielo bolo riadne dokončené a odovzdané Zhotoviteľom a prevzaté zo strany Objednávateľa. Všetky ustanovenia tejto Zmluvy o dielo, ktoré sa vzťahujú na Akceptačný protokol sa vzťahujú aj na Záverečný akceptačný protokol.
- 6.10 Odovzdaním Diela alebo jeho časti podľa tohto Článok 6. tejto Zmluvy o dielo sa Objednávateľ stáva vlastníkom Diela alebo jeho časti.
- 6.11 Odovzдание Diela alebo jeho časti v rozpore s týmto Článok 6. tejto Zmluvy o dielo sa považuje za podstatné porušenie tejto Zmluvy o dielo.
- 6.12 Pred vyhotovením Záverečného akceptačného protokolu je Zhotoviteľ povinný zabezpečiť skúšobnú prevádzku Diela ako celku v trvaní 4 (slovom: štyroch) týždňov. Všetky ustanovenia tejto Zmluvy o dielo, ktoré sa vzťahujú na Akceptačný protokol, sa vzťahujú aj na skúšobnú prevádzku Diela podľa tohto bodu 6.12 tejto Zmluvy o dielo. Výsledkom úspešného ukončenia skúšobnej prevádzky podľa tohto bodu 6.12 tejto Zmluvy o dielo je odovzдание Diela ako celku prostredníctvom Záverečného akceptačného protokolu.
- 6.13 V rámci vykonania skúšobnej prevádzky sa preverí funkcia všetkých implementovaných systémov v prevádzkových podmienkach a preukáže sa, že sú vytvorené predpoklady na dosiahnutie projektovaných parametrov. Skúšobná prevádzka preukáže pripravenosť systémov plniť požadované funkcie ako aj vytvorenie podmienok pre trvalú prevádzku.

## **Článok 7. SPRÁVA O PLNENÍ**

- 7.1 Zhotoviteľ je počas trvania tejto Zmluvy o dielo povinný predkladať Zodpovednej osobe Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo priebežné správy o plnení tejto Zmluvy o dielo (ďalej len „Správa o plnení“).
- 7.2 Správy o plnení je Zhotoviteľ povinný predkladať Objednávateľovi za každý mesiac plnenia tejto Zmluvy o dielo, a to najneskôr do 15 (slovom: pätnásteho) dňa mesiaca nasledujúceho po mesiaci, za ktorý sa predkladá príslušná Správa o plnení.
- 7.3 Správy o plnení musia obsahovať:
- a) sumarizácia progresu aktivít – informácie o postupe prác, ktoré umožnia kontrolu plnenia úloh stanovených v projekte,
  - b) zhodnotenie celkového vývoja plnenia tejto Zmluvy o dielo s ohľadom na úspešnosť činnosti plnenia termínov,
  - c) identifikácia dôležitých problémov, ktoré sa vyskytnú v priebehu plnenia tejto Zmluvy o dielo a spôsobu ich riešenia.

## **Článok 8. ZÁRUKA A ODSTRAŇOVANIE VÁD POČAS ZÁRUKY**

- 8.1 Zhotoviteľ zodpovedá za to, že Dielo je ku dňu podpisu Záverečného akceptačného protokolu podľa bodu 6.13 tejto Zmluvy o dielo a počas záručnej doby bez väd, t. j. najmä ale nielen má funkčné a technické vlastnosti v zmysle tejto Zmluvy o dielo.
- 8.2 Zhotoviteľ poskytuje Objednávateľovi na Dielo záruku počas trvania záručnej doby, ktorá je 60 (slovom: šesťdesiat) mesiacov odo dňa riadneho odovzdania a prevzatia Diela ako celku, t. j. odo dňa odovzdania úplného Diela podľa tejto Zmluvy o dielo (ďalej len „Záručná doba“).
- 8.3 Počas Záručnej doby Zhotoviteľ zodpovedá za funkcionality a funkčnosť Diela alebo jeho časti, ktorá musí byť v súlade s touto Zmluvou o dielo s tým, že Zhotoviteľ zaručuje, že v Záručnej dobe bude Dielo spôsobilé na použitie na účel zodpovedajúci jeho určeniu, a to všetko v rozsahu určenom v Opise predmetu zákazky – časť č. 1.
- 8.4 Zhotoviteľ zaručuje, že odovzdané Dielo alebo jeho časť nemá právne vady, predovšetkým nie je zaťažené právami tretích osôb z priemyselného alebo iného duševného vlastníctva. Zhotoviteľ sa zaväzuje nahradiť Objednávateľovi škodu spôsobenú uplatnením nárokov tretích osôb z titulu porušenia ich chránených práv súvisiacich s plnením Zhotoviteľa alebo jeho Subdodávateľov podľa tejto Zmluvy o dielo.
- 8.5 Zhotoviteľ zaručuje, že k Dielu alebo jeho časti neexistujú v čase jeho odovzdania akékoľvek právne nároky tretích osôb, a že Dielo alebo jeho časť nie je predmetom vecného bremena alebo iného obdobného právneho vzťahu, ktorý by bol spôsobilý obmedziť Objednávateľa v užívaní Diela alebo jeho časti.
- 8.6 Objednávateľ je povinný oznámiť Zhotoviteľovi vady Diela alebo jeho časti kedykoľvek do uplynutia Záručnej doby, avšak bez zbytočného odkladu po tom, ako sa o nich dozvedel. Objednávateľ je oprávnený požadovať od Zhotoviteľa bezplatné odstránenie vady Diela alebo jeho časti, na ktorú sa vzťahuje záruka podľa tejto Zmluvy o dielo. Pre vylúčenie akýchkoľvek pochybností Zmluvné strany potvrdzujú, že odstránením Vady sa rozumie trvalé vyriešenie Vady



alebo poskytnutie náhradného riešenia, to však len na dobu do uplynutia lehoty na trvalé vyriešenie Vady.

- 8.7 Zmluvné strany sa zaväzujú potvrdiť odstránenie Vady Diela alebo jeho časti v zápisnici o odstránení Vady podpísanej Zodpovednou osobou Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo a Zodpovednou osobou Zhotoviteľa podľa bodu 12.4 tejto Zmluvy o dielo, v ktorej uvedú aj predmet Vady a spôsob a čas jej odstránenia.
- 8.8 V prípade, ak nedôjde k odstráneniu Vady Diela alebo jeho časti v príslušnej lehote, Objednávateľovi vznikne nárok na zmluvnú pokutu podľa Článok 17. tejto Zmluvy o dielo.

## **Článok 9. CENA A PLATOBNÉ PODMIENKY**

- 9.1 Objednávateľ je povinný zaplatiť Zhotoviteľovi za riadne vykonanie Diela na základe tejto Zmluvy o dielo cenu dojednanú v zmysle Zákona o cenách v celkovej výške
- 123 795,24 EUR (slovom: stodvadsaťtritisíc sedemstodevät'desiatpäť eur a dvadsaťštyri centov) bez DPH (ďalej len „Cena za Dielo“).
- DPH (20%) 24 759,05 (slovom: dvadsaťštyritisíc sedemstopäť'desiatdeväť eur a päť centov)
- Cena celkom v EUR s DPH 148 554,29 (slovom: stoštyridsaťosemtisíc päť'stopäť'desiatštyri eur a dvadsaťdeväť centov )
- 9.2 Cena za Dielo sa skladá z cien za jednotlivé čiastkové plnenia Diela, t. j. jednotlivé časti Diela v súlade s vyplnenou Prílohou č. 3 Návrh na plnenie kritérií, ktorý tvorí Prílohu č. 2 tejto Zmluvy o dielo (ďalej len „Návrh na plnenie kritérií“).
- 9.3 Objednávateľ nie je platcom DPH.
- 9.4 Cena za Dielo predstavuje odplatu za splnenie všetkých zmluvných záväzkov Zhotoviteľa vyplývajúcich z tejto Zmluvy o dielo a zahŕňa všetky náklady a výdavky Zhotoviteľa na riadne a včasné vykonanie Diela alebo jeho častí v zmysle tejto Zmluvy o dielo, ako aj odplatu za udelenie autorských majetkových práv k Dielu alebo jeho časti v zmysle tejto Zmluvy o dielo. Objednávateľ neposkytuje preddavok, ani zálohovú platbu.
- 9.5 Zhotoviteľ je oprávnený požadovať zaplatenie Ceny za Dielo po častiach max. v rámci čiastkových 2 faktúr.
- 9.6 Objednávateľ uhradí Zhotoviteľovi Cenu za Dielo alebo jeho časť podľa bodu 9.5 tejto Zmluvy o dielo bezhotovostným prevodom na základe faktúry vystavenej Zhotoviteľom po včasnom vykonaní Diela alebo jeho časti a jeho odovzdaní Objednávateľovi v súlade s touto Zmluvou o dielo. Podkladom pre vystavenie faktúry je Akceptačný protokol, ktorý bude spĺňať všetky podmienky v zmysle tejto Zmluvy o dielo.
- 9.7 Výdavky vo faktúre musia byť rozdelené do jednotlivých položiek s jednotkovými cenami zaokrúhlenými na 2 (slovom: dve) desatinné miesta s jednoznačnou identifikáciou, ktorej položky Návrhu na plnenie kritérií, ktorý tvorí Prílohu č. 2, sa predmetná fakturovaná čiastka týka. Ku každej faktúre musí byť priložený originál Akceptačného protokolu podpísaného Zodpovednou osobou Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo a Zodpovednou osobou Zhotoviteľa podľa bodu 12.4 tejto Zmluvy o dielo.
- 9.8 Faktúra musí obsahovať náležitosti daňového dokladu v zmysle všeobecne záväzných právnych predpisov, najmä v zmysle Zákona o DPH a Zákona o účtovníctve. Faktúra musí ďalej obsahovať číslo tejto Zmluvy o dielo, ktoré jej bolo pridelené na účely evidencie Objednávateľom. Ak faktúra nebude obsahovať náležitosti podľa tohto Článku 9. tejto Zmluvy o dielo alebo ak bude obsahovať nesprávne alebo neúplné údaje, Objednávateľ je oprávnený faktúru vrátiť Zhotoviteľovi v lehote splatnosti bez zaplatenia za účelom opravy a Zhotoviteľ je povinný bez

zbytočné odkladu vykonať nápravu, prípadne vystaviť novú faktúru, pričom nová doba splatnosti faktúry začína plynúť odo dňa doručenia opravenej alebo novej faktúry Objednávateľovi s tým, že Objednávateľ sa z toho dôvodu nedostáva do omeškania.

- 9.9 Splatnosť faktúr je 60 (slovom: šesťdesiat) kalendárnych dní odo dňa ich doručenia Objednávateľovi za predpokladu, že faktúra bude spĺňať všetky náležitosti podľa bodu 9.8 tejto Zmluvy o dielo. Zmluvné strany vyhlasujú, že uvedená lehota nie je v hrubom nepomere k právam a povinnostiam vyplývajúcim zo záväzkového vzťahu, nakoľko je predmet realizácie spolufinancovaný zo zdrojov EÚ a SR a objednávatel' má záujem využiť systém predfinancovania.
- 9.10 Platba faktúry podľa tejto Zmluvy o dielo bude uskutočnená bezhotovostným prevodom na účet Zhotoviteľa uvedený na titulnej strane tejto Zmluvy o dielo. Zmluvné strany a dohodli, že zmena bankových údajov je možná len na základe uzatvorenia dodatku k tejto Zmluve o dielo.
- 9.11 Zmluvné strany sa dohodli, že Objednávateľ nie je v omeškaní so zaplatením faktúry za predpokladu, že najneskôr v posledný deň lehoty jej splatnosti zadal platobný príkaz na jej zaplatenie.

## **Článok 10. OCHRANA DÔVERNÝCH INFORMÁCIÍ A OSOBNÝCH ÚDAJOV**

- 10.1 Ak Zhotoviteľ pri plnení tejto Zmluvy o dielo bude spracúvať v mene Objednávateľa osobné údaje dotknutých osôb, a teda bude vystupovať v postavení sprostredkovateľa v zmysle Článku 4 ods. 8. Nariadenia GDPR a § 5 písm. p) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákona o ochrane OÚ“), Zmluvné strany sa zaväzujú uzatvoriť zmluvu o poverení spracúvaním osobných údajov v zmysle Článku 28 Nariadenia GDPR a ust. § 34 Zákona o ochrane OÚ, a to súčasne s uzatvorením tejto Zmluvy o dielo alebo bezprostredne po jej uzatvorení. V zmluve o poverení spracúvaním osobných údajov podľa predchádzajúcej vety tohto bodu 10.1 tejto Zmluvy o dielo si Zmluvné strany vymedzia predmet, dobu, povahu a účel spracúvania osobných údajov, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva Objednávateľa ako prevádzkovateľa a tiež ďalšie práva a povinnosti v zmysle Nariadenia GDPR a Zákona o ochrane OÚ.
- 10.2 Zmluvné strany sú povinné zaviazat' fyzické osoby, ktoré prídu do styku s osobnými údajmi mlčanlivosťou o osobných údajoch, pričom táto povinnosť mlčanlivosti musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru alebo obdobného pracovného vzťahu fyzických osôb.
- 10.3 Zmluvné strany sú povinné zachovávať mlčanlivosť o informáciách, ktoré získali v súvislosti s plnením predmetu tejto Zmluvy o dielo a získané výsledky nesmú ďalej použiť na iné účely ako plnenie predmetu tejto Zmluvy o dielo, okrem prípadu poskytnutia informácií odborným poradcem Zhotoviteľa (vrátane právnych, účtovných, daňových a iných poradcov alebo audítorov), ktorí sú viazaní všeobecnou povinnosťou mlčanlivosti na základe osobitných právnych predpisov alebo sú povinní zachovávať mlčanlivosť na základe písomnej dohody s dotknutou Zmluvnou stranou alebo Subdodávateľom, ak sa Subdodávateľ podieľa na plnení predmetu tejto Zmluvy o dielo, a ak je to potrebné na účely plnenia povinností Zhotoviteľa podľa tejto Zmluvy o dielo.
- 10.4 Zmluvné strany označujú informácie, ktoré budú získané v súvislosti s plnením tejto Zmluvy o dielo a výsledky získané v súvislosti s plnením tejto Zmluvy o dielo za Dôverné informácie.
- 10.5 Povinnosť Zhotoviteľa a Objednávateľa zachovávať mlčanlivosť o informáciách, ktoré získali v súvislosti s plnením tejto Zmluvy o dielo sa nevzťahuje na informácie, ktoré:
- a) boli zverejnené už pred uzatvorením tejto Zmluvy o dielo,

- b) sa stanú všeobecne a verejne dostupné po uzatvorení tejto Zmluvy o dielo z iného dôvodu ako z dôvodu porušenia povinností podľa tejto Zmluvy o dielo,
  - c) majú byť sprístupnené na základe povinnosti stanovenej všeobecne záväzným právnym predpisom, rozhodnutím súdu, prokuratúry alebo na základe iného záväzného rozhodnutia príslušného orgánu,
  - d) boli získané Zhotoviteľom, resp. Objednávateľom od tretej strany, ktorá ich legitímne získala alebo vyvinula, a ktorá nemá žiadnu povinnosť, ktorá by obmedzovala ich zverejňovanie.
- 10.6 Zmluvné strany sa zaväzujú, že poučia svojich zamestnancov, štatutárne orgány, ich členov, členov Skupiny dodávateľov a Subdodávateľov, ktorým sú sprístupnené Dôverné informácie, o povinnosti mlčanlivosti v zmysle tohto Článok 10. tejto Zmluvy o dielo a v rozsahu zaist'ujúcim splnenie povinnosti mlčanlivosti v zmysle tohto Článok 10. tejto Zmluvy o dielo Zhotoviteľ uzatvorí s každým členom Skupiny dodávateľov a Subdodávateľom dohodu o mlčanlivosti, pokiaľ obdobný záväzok nevyplýva pre takého člena Skupiny dodávateľov a Subdodávateľa zo zákona. Zhotoviteľ vyhlasuje, že oboznámil svojich zamestnancov, ktorí sa budú podieľať na plnení tejto Zmluvy o dielo, s povinnosťou mlčanlivosti v zmysle tejto Zmluvy o dielo.
- 10.7 Zmluvné strany sa zaväzujú užívať Dôverné informácie výlučne na účel, na ktorý im boli poskytnuté a zároveň sa zaväzujú Dôverné informácie ochraňovať najmenej s rovnakou starostlivosťou ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti, predovšetkým ich budú chrániť pred náhodným alebo neoprávneným poškodením a zničením, náhodnou stratou, zmenou alebo iným znehodnotením, nedovoleným prístupom alebo sprístupnením alebo zverejnením, pričom ak nie je v tejto Zmluve o dielo ustanovené inak, zaväzujú sa, že bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany neposkytnú, neodovzdajú, neoznámia alebo iným spôsobom nevyzradia, resp. nesprístupnia Dôverné informácie druhej Zmluvnej strany tretej osobe.

### **Článok 11. SÚČINNOSŤ**

- 11.1 Zmluvné strany sa zaväzujú vzájomne spolupracovať a poskytovať si všetky informácie a nevyhnutnú súčinnosť potrebnú pre riadne plnenie svojich záväzkov vyplývajúcich im z tejto Zmluvy o dielo.
- 11.2 Objednávateľ je povinný počas celej doby trvania tejto Zmluvy o dielo poskytovať Zhotoviteľovi súčinnosť v oblasti doplnenia údajov, podkladov a iných dokladov na základe požiadaviek Zhotoviteľa, ktoré sú potrebné na splnenie povinnosti vykonať Dielo alebo jeho časť v súlade s podmienkami v zmysle tejto Zmluvy o dielo.
- 11.3 Zhotoviteľ sa zaväzuje spolupracovať s Objednávateľom počas vykonávania Diela alebo jeho časti a vyvinúť maximálne úsilie a súčinnosť z jeho strany tak, aby bolo Dielo alebo jeho časť vykonané v súlade s podmienkami v zmysle tejto Zmluvy o dielo.

### **Článok 12. ZODPOVEDNÉ OSOBY**

- 12.1 Zmluvné strany sa dohodli, že si vzájomne určia osoby, ktoré budú zodpovedné za vecné plnenie tejto Zmluvy o dielo a komunikáciu týkajúcu sa plnenia tejto Zmluvy o dielo.
- 12.2 Prostredníctvom zodpovedných osôb určených podľa tohto Článok 12. tejto Zmluvy o dielo budú Zmluvné strany:
- a) uskutočňovať všetky organizačné záležitosti s ohľadom na všetky aktivity a činnosti súvisiace s plnením tejto Zmluvy o dielo,
  - b) zabezpečovať koordináciu jednotlivých aktivít a činností Zmluvných strán súvisiacich s plnením tejto Zmluvy o dielo,

- c) sledovať priebeh plnenia tejto Zmluvy o dielo,
- d) navrhovať potrebné zmeny technických riešení a iné zmeny technickej povahy týkajúce sa plnenia tejto Zmluvy o dielo, e) zabezpečovať vzájomnú spoluprácu a súčinnosť.

12.3 Za Objednávateľa je zodpovednou osobou podľa tohto Článok 12. tejto Zmluvy o dielo:

- a) meno a priezvisko: **Mgr. Martin Fabian**
  - b) funkcia: referent informatiky
  - c) tel. kontakt: +421 918 248 966
  - d) e-mail: [faby@sala.sk](mailto:faby@sala.sk)
- („Zodpovedná osoba Objednávateľa“).

12.4 Za Zhotoviteľa je zodpovednou osobou podľa tohto Článok 12. tejto Zmluvy o dielo:

- a) meno a priezvisko: Mgr. Jakub Čeles
  - b) funkcia: konateľ spoločnosti
  - c) tel. kontakt: +421 915 493 566
  - d) e-mail: [jakub.celes@airo.sk](mailto:jakub.celes@airo.sk)
- („Zodpovedná osoba Zhotoviteľa“).

12.5 Zodpovedné osoby podľa bodov 12.3 a 12.4 tejto Zmluvy o dielo majú okrem oprávnení podľa bodu 12.2 tejto Zmluvy o dielo tiež ďalšie oprávnenia, ktoré im výslovne vyplývajú z tejto Zmluvy o dielo.

12.6 V prípade, ak má niektorá zo Zmluvných strán záujem zmeniť ňou určenú zodpovednú osobu podľa bodov 12.3 a 12.4 tejto Zmluvy o dielo, je povinná písomne to oznámiť druhej Zmluvnej strane a toto oznámenie jej doručiť osobne alebo formou doporučenej zásielky.

### Článok 13. OCHRANA ZAMESTNANCOV ZHOTOVITEĽA A SUBDODÁVATEĽOV

13.1 Zhotoviteľ zodpovedá za svojich zamestnancov, svojich Subdodávateľov, zamestnancov svojich Subdodávateľov, členov Skupiny dodávateľov, zamestnancov ostatných členov Skupiny dodávateľov a tiež akékoľvek ďalšie osoby, ktoré sa podieľajú na plnení tejto Zmluvy o dielo, najmä ale nielen je Zhotoviteľ povinný zabezpečiť bezpečnosť a ochranu zdravia týchto osôb pri práci, či už sa táto Zmluva o dielo plní v mieste plnenie v zmysle tejto Zmluvy o dielo alebo na inom dohodnutom mieste.

13.2 Zhotoviteľ je povinný vykonať všetky nevyhnutné opatrenia, aby v súvislosti s plnením tejto Zmluvy o dielo zabezpečil bezpečnosť osôb podľa bodu 13.1. tejto Zmluvy o dielo.

13.3 Zhotoviteľ je povinný v súvislosti s plnením tejto Zmluvy o dielo vykonať opatrenia a určiť postupy na zaistenie bezpečnosti osôb podľa bodu 13.1 tejto Zmluvy o dielo a zabezpečiť prostriedky potrebné na ochranu ich života a zdravia na mieste plnenia tejto Zmluvy o dielo pre prípad vzniku bezprostredného a vážneho ohrozenia života alebo zdravia s tým, že Zhotoviteľ je povinný o vykonaných opatreniach informovať Objednávateľa a ďalšie osoby zdržujúce sa na mieste plnenia tejto Zmluvy o dielo.

13.4 Zhotoviteľ je povinný bezodkladne písomne oboznamovať Objednávateľa o nedostatkoch a iných závažných skutočnostiach v priestoroch Objednávateľa tvoriacich miesto plnenia tejto Zmluvy o dielo, o ktorých sa dozvedel v súvislosti s plnením tejto Zmluvy o dielo a ktoré by boli spôsobilé ohroziť bezpečnosť alebo zdravie osôb podľa bodu 13.1 tejto Zmluvy o dielo pri práci.

13.5 Zhotoviteľ je povinný bezodkladne oboznámiť Objednávateľa o mimoriadnej udalosti (napr. nebezpečná udalosť, pracovný úraz a i.), ktorá sa stala v súvislosti s plnením tejto Zmluvy o dielo a ktorá sa týka ochrany osôb podľa bodu 13.1 tejto Zmluvy o dielo. Povinnosť Zhotoviteľa podľa predchádzajúcej vety tohto bodu 13.5 tejto Zmluvy o dielo sa vzťahuje aj na prípady, v ktorých k

mimoriadnej udalosti nedošlo v súvislosti s plnením tejto Zmluvy o dielo, ale došlo k nej na pracoviskách Objednávateľa.

- 13.6 Zhotoviteľ je povinný zaraďovať osoby podľa bodu 13.1 tejto Zmluvy o dielo na výkon práce so zreteľom na ich zdravotný stav, schopnosti, kvalifikačné predpoklady a odbornú spôsobilosť v zmysle všeobecne záväzných právnych predpisov a ostatných predpisov na zaistenie bezpečnosti a ochrany zdravia pri práci a zabezpečiť, aby nevykonávali tie práce, ktoré nezodpovedajú ich zdravotnému stavu, schopnostiam, kvalifikačným predpokladom a odbornej spôsobilosti v zmysle všeobecne záväzných právnych predpisov a ostatných predpisov na zaistenie bezpečnosti a ochrany zdravia pri práci alebo ich veku.

#### **Článok 14. ZODPOVEDNOSŤ ZA ŠKODU A NÁHRADA ŠKODY**

- 14.1 Nebezpečenstvo škody a vlastnícke právo ku všetkým hmotným plneniam Diela alebo jeho časti vytvoreným alebo dodaným na základe tejto Zmluvy o dielo prechádza na Objednávateľa odovzdaním Diela alebo jeho časti Objednávateľovi.
- 14.2 Každá zo Zmluvných strán nesie zodpovednosť za škodu spôsobenú porušením všeobecne záväzných právnych predpisov a tejto Zmluvy o dielo.
- 14.3 Zhotoviteľ zodpovedá za škodu spôsobenú Objednávateľovi osobami podľa bodu 13.1 tejto Zmluvy o dielo, pričom ustanovenia Zákonníka práce o zodpovednosti zamestnancov za škodu ako i ustanovenia Obchodného zákonníka o náhrade škody aplikovateľné na škodu spôsobenú Subdodávateľmi tým nie sú dotknuté.
- 14.4 Zhotoviteľ zodpovedá za škodu, ktorá vznikne Objednávateľovi počas platnosti a existencie tejto Zmluvy o dielo a pôjde o škodu spôsobenú vadou Diela alebo jeho časti. Za takto spôsobenú škodu zodpovedá Zhotoviteľ, ak vznikla v čase platnej záruky na predmet Zmluvy o dielo.
- 14.5 Zmluvné strany sa dohodli, že na vznik zodpovednosti za spôsobenú škodu nie je nevyhnutné, aby bola škoda spôsobená úmyselným konaním Zhotoviteľa alebo osôb podľa bodu 13.1 tejto Zmluvy o dielo, ale postačuje spôsobenie škody z nedbanlivosti.
- 14.6 Obe Zmluvné strany sa zaväzujú vyvinúť maximálne úsilie k predchádzaniu škodám a k minimalizácii vzniknutých škôd.
- 14.7 Zhotoviteľ je povinný postupovať pri plnení pokynov a zadaní zo strany Objednávateľa s odbornou starostlivosťou a na nevhodnosť pokynov Objednávateľa upozorniť. Ak Zhotoviteľ neupozorní Objednávateľa na nevhodnosť pokynov, nemôže sa zbaviť zodpovednosti za vzniknutú škodu, iba ak nevhodnosť nemohol zistiť ani pri vynaložení odbornej starostlivosti. Zhotoviteľ nezodpovedá ani za škodu, ktorá vznikla v dôsledku vadného zadania zo strany Objednávateľa, ak Zhotoviteľ bezodkladne upozornil Objednávateľa na vadnosť tohto zadania a Objednávateľ na tomto zadaní naďalej písomne trval.
- 14.8 Ak nevhodné pokyny alebo podklady dané Objednávateľom prekážajú v riadnom plnení povinností Zhotoviteľa podľa tejto Zmluvy o dielo, Zhotoviteľ je povinný ich plnenie v nevyhnutnom rozsahu prerušiť do doby výmeny nevhodných podkladov alebo zmeny pokynov Objednávateľa alebo písomného oznámenia, že Objednávateľ trvá na poskytnutí plnení podľa tejto Zmluvy o dielo s použitím podkladov a pokynov daných mu Objednávateľom. O dobu, po ktorú bolo potrebné plnenie povinností Zhotoviteľa podľa tejto Zmluvy o dielo prerušiť sa predlžuje lehota určená na ich splnenie.
- 14.9 Zmluvné strany sa zaväzujú bez zbytočného odkladu písomne upozorniť druhú Zmluvnú stranu na vzniknuté okolnosti vylučujúce zodpovednosť, brániace riadnemu plneniu tejto Zmluvy o dielo. Zmluvné strany sa zaväzujú vyvinúť maximálne úsilie na odvrátenie a prekonanie okolností vylučujúcich zodpovednosť.

- 14.10 Zhotoviteľ je oprávnený zabezpečiť plnenie tejto Zmluvy o dielo alebo jeho častí prostredníctvom Subdodávateľov v súlade s podmienkami Verejného obstarávania a touto Zmluvou o dielo. Zhotoviteľ zodpovedá za každé plnenie takéhoto Subdodávateľa v rozsahu, ako keby plnenie poskytoval sám.
- 14.11 V prípade okolností vyššej moci, ktorou sa rozumie prekážka, ktorá nastala nezávisle od vôle Zmluvnej strany a bráni jej v splnení jej zmluvných povinností a zároveň nemožno rozumne predpokladať, že by povinná Zmluvná strana túto prekážku alebo jej následky odvrátila alebo prekonala, a tiež že by v čase vzniku záväzku túto prekážku predvídala, Zmluvná strana, ktorá nesplní svoje povinnosti z tejto Zmluvy o dielo z dôvodu okolností vyššej moci, nebude zodpovedná za žiadne dôsledky neplnenia svojich povinností, vrátane zodpovednosti za škodu, za predpokladu, že vykonala všetky rozumné opatrenia pre ich splnenie. V takýchto prípadoch nesplnenie povinností nezakladá dôvod pre odstúpenie od tejto Zmluvy o dielo alebo vznik nároku na zmluvnú pokutu. Čas pre splnenie povinnosti sa predlžuje o čas trvania akejkoľvek z okolností uvedených v tomto bode 14.11 tejto Zmluvy o dielo a o čas nevyhnutný na odstránenie ich následkov.
- 14.12 Za konanie vylučujúce zodpovednosť sa považuje napr. konanie/nekonanie riadiaceho orgánu, sprostredkovateľského orgánu, certifikačného orgánu, orgánu auditu alebo iného orgánu oprávneného vstupovať do zmluvných vzťahov v zmysle Zákona o EŠIF za predpokladu, že plnenie tejto Zmluvy o dielo je realizáciou projektu financovaného z európskych štrukturálnych a investičných fondov EÚ.

## Článok 15. SUBDODÁVATELIA

- 15.1 Na poskytovanie plnení, ktoré tvoria súčasť Diela alebo jeho častí pre Objednávateľa má Zhotoviteľ, za podmienok v zmysle tejto Zmluvy o dielo právo uzatvárať zmluvy so Subdodávateľmi. Tým nie je dotknutá zodpovednosť Zhotoviteľa za plnenie tejto Zmluvy o dielo v zmysle ust. § 41 ods. 8 Zákona o VO a Zhotoviteľ je povinný odovzdať Objednávateľovi plnenia v zmysle tejto Zmluvy o dielo sám, na svoju zodpovednosť, v dohodnutom čase a v dohodnutej kvalite.
- 15.2 Zoznam subdodávateľov s ich identifikačnými údajmi v rozsahu:
- (i) meno a priezvisko alebo obchodné meno, resp. názov,
  - (ii) adresa pobytu alebo sídlo,
  - (iii) IČO alebo dátum narodenia, ak nebolo pridelené IČO,
  - (iv) podiel plnenia tejto Zmluvy o dielo v percentuálnom vyjadrení, ako aj údaje o osobe oprávnenej konať za Subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia, tvorí neoddeliteľnú súčasť tejto Zmluvy o dielo ako Príloha č. 3.
- 15.3 Zhotoviteľ je povinný písomne oznámiť Zodpovednej osobe Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo akúkoľvek zmenu údajov o Subdodávateľovi bezodkladne po tom, ako sa o takej zmene dozvedel.
- 15.4 Zhotoviteľ je oprávnený zmeniť alebo doplniť Subdodávateľa počas trvania tejto Zmluvy o dielo. V prípade zmeny alebo doplnenia Subdodávateľa musí Subdodávateľ spĺňať podmienky účasti na Verejnom obstarávaní týkajúce sa osobného postavenia v zmysle ust. § 32 ods. 1 Zákona o VO a nesmú u neho existovať dôvody na vylúčenie v zmysle ust. § 40 ods. 6 písm. a) až g) a ust. § 40 ods. 7 a 8 Zákona o VO. Zhotoviteľ je povinný predložiť Objednávateľovi písomné oznámenie o zmene alebo doplnení Subdodávateľa, ktoré bude obsahovať údaje o navrhovanom Subdodávateľovi v rozsahu podľa bodu 15.2 tejto Zmluvy o dielo, a to najneskôr 3 (slovom: tri) pracovné dni pred zmenou Subdodávateľa. Zmena alebo doplnenie Subdodávateľa podlieha písomnému súhlasu Zodpovednej osoby Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo. Po

vzájomnom odsúhlasení zmeny alebo doplnenia Subdodávateľa oboma Zmluvnými stranami uzatvoria Zmluvné strany dodatok k tejto Zmluve o dielo reflektujúci túto zmenu alebo doplnenie Subdodávateľa.

- 15.5 Porušenie povinností vyplývajúcich z bodov 15.2, 15.3 a 15.4 tejto Zmluvy o dielo sa považuje za podstatné porušenie tejto Zmluvy o dielo.

## **Článok 16. KLÚČOVÍ EXPERTI**

- 16.1 Zhotoviteľ je povinný zabezpečiť plnenie tejto Zmluvy o dielo v rozsahu stanovenom v Opise predmetu zákazky – časť I. kľúčovými expertmi, ktorých uviedol vo svojej ponuke predloženej vo Verejnom obstarávaní (ďalej len „Kľúčoví experti“) alebo ďalšími osobami pod odborným vedením týchto Kľúčových expertov. Zoznam Kľúčových expertov je obsahom Prílohy č. 4 k tejto Zmluve o dielo, ktorú je povinný vytvoriť Zhotoviteľ pred podpisom tejto Zmluvy o dielo tak, aby obsahovala všetkých Kľúčových expertov identifikovaných minimálne menom a priezviskom.
- 16.2 Zhotoviteľ je oprávnený zmeniť alebo doplniť Kľúčového experta počas trvania tejto Zmluvy o dielo, avšak len za podmienky, že nový Kľúčový expert bude spĺňať podmienky účasti na Verejnom obstarávaní týkajúce sa odbornej a technickej spôsobilosti v zmysle požiadaviek uvedených vo Výzve na predkladanie ponúk, čo je Zhotoviteľ povinný Objednávateľovi preukázať a len s písomným súhlasom Zodpovednej osoby Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo.
- 16.3 Zhotoviteľ je povinný predložiť Objednávateľovi písomné zamýšľané oznámenie o zmene alebo doplnení Kľúčového experta, ktoré bude obsahovať odôvodnenie tejto zmeny, údaje o navrhovanom Kľúčovom expertovi. K oznámeniu podľa tohto bodu 16.3. tejto Zmluvy o dielo je Zhotoviteľ povinný pripojiť podklady preukazujúce odbornú a technickú spôsobilosť v zmysle požiadaviek uvedených vo Výzve na predkladanie ponúk a písomnú zmluvu, z ktorej vyplýva záväzok osoby, že poskytne svoje kapacity počas celého trvania tejto Zmluvy o dielo. Zodpovedná osoba Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo je povinná vyjadriť sa k oznámeniu podľa tohto bodu 16.3 tejto Zmluvy o dielo najneskôr do 7 (slovom: siedmich) pracovných dní. Po vzájomnom odsúhlasení zmeny alebo doplnenia Kľúčového experta oboma Zmluvnými stranami uzatvoria Zmluvné strany dodatok k tejto Zmluve o dielo reflektujúci túto zmenu alebo doplnenie Kľúčového experta.
- 16.4 Zmena Kľúčového experta v rozpore s týmto Článkom 16. tejto Zmluvy o dielo sa považuje za podstatné porušenie tejto Zmluvy o dielo.

## **Článok 17. SANKCIE A ZMLUVNÉ POKUTY**

- 17.1 Ak bude Zhotoviteľ v omeškaní s plnením povinnosti odovzdať Objednávateľovi Dielo alebo jeho časť včas podľa bodu 4.2 písm. a) tejto Zmluvy o dielo, Zhotoviteľ je povinný zaplatiť Objednávateľovi zmluvnú pokutu vo výške 500,00 EUR (slovom: päťsto eur), a to za každý deň omeškania maximálne však do výšky 5 % (slovom: päť percent) z časti Ceny za Dielo vrátane DPH, za Dielo alebo jeho časť, s ktorej zhotovením a dodaním je Zhotoviteľ v omeškaní.
- 17.2 V prípade omeškania Objednávateľa so splnením peňažného záväzku alebo jeho časti v zmysle tejto Zmluvy o dielo má Zhotoviteľ právo uplatniť si voči nemu z nezaplatenej sumy úroky z omeškania v zmysle ust. § 369a Obchodného zákonníka, a to v sadzbe v zmysle ust. § 1 ods. 2 nariadenia vlády Slovenskej republiky č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení nariadenia vlády Slovenskej republiky č. 303/2014 Z. z.

- 17.3 Celková suma všetkých zmluvných pokút a úrokov z omeškania, ktoré budú Zmluvné strany povinné si vzájomne zaplatiť na základe tejto Zmluvy o dielo nemôže presiahnuť sumu vo výške 100 % (slovom: sto percent) Ceny za Dielo vrátane DPH.
- 17.4 Zhotoviteľ je povinný zaplatiť zmluvné pokuty podľa tohto Článok 17. tejto Zmluvy o dielo najneskôr v lehote 15 (slovom: pätnástich) dní odo dňa doručenia písomnej výzvy Objednávateľa na jej zaplatenie.
- 17.5 Odstúpenie od tejto Zmluvy o dielo ktoroukoľvek Zmluvnou stranou sa nedotýka nároku Objednávateľa na zaplatenie zmluvnej pokuty podľa tohto Článok 17. tejto Zmluvy o dielo.
- 17.6 Zaplatením zmluvnej pokuty podľa tohto Článok 17. tejto Zmluvy o dielo nie je dotknutý nárok Zmluvných strán na náhradu škody spôsobenú porušením povinnosti, na ktorú sa vzťahuje zmluvná pokuta vo výške, ktorá prevyšuje výšku dohodnutej zmluvnej pokuty, t. j. dotknutá Zmluvná strana je oprávnená domáhať sa náhrady škody spôsobenej porušením povinnosti v zmysle tejto Zmluvy o dielo presahujúcej výšku zmluvnej pokuty zabezpečujúcej túto povinnosť.
- 17.7 Zmluvné strany sa dohodli, že ak si Objednávateľ uplatní voči Zhotoviteľovi zmluvnú pokutu podľa tohto Článok 17. tejto Zmluvy o dielo, bude mať Objednávateľ právo započítať si svoju pohľadávku vyplývajúcu z uplatnenej zmluvnej pokuty voči akejkolvek pohľadávke Zhotoviteľa, ktorú má tento voči Objednávateľovi, či už z tejto Zmluvy o dielo alebo z akéhokoľvek iného právneho dôvodu.
- 17.8 V prípade, ak dôjde k omeškaniu Zhotoviteľa podľa bodu 17.1 tejto Zmluvy o dielo o viac ako 1 (slovom: jeden) mesiac, bude takéto konanie považované za podstatné porušenie tejto Zmluvy o dielo.

#### **Článok 18. ZMENY DIELA A ZMENY ZMLUVY O DIELO**

- 18.1 Ak Objednávateľ v budúcnosti zistí, že Dielo ako celok je potrebné rozšíriť o ďalšie časti Diela nad rámec tejto Zmluvy o dielo, ktorých dodanie je nevyhnutným predpokladom funkčnosti a kompatibility Diela ako celku a zároveň pôjde o nevyhnutný prvok za účelom plnenia tejto Zmluvy o dielo, je oprávnený v súlade s relevantnými ustanoveniami Zákona o VO zabezpečiť dodanie takejto ďalšej časti Diela. Zhotoviteľ nemá právo na prednostné dodanie ďalšej takejto časti Diela nad rámec tejto Zmluvy o dielo bez ohľadu na skutočnosť, že predmetom Diela alebo jeho časti môžu byť autorské práva Zhotoviteľa.
- 18.2 Zmena tejto Zmluvy o dielo sa vykoná prostredníctvom obojstranne podpísaného písomného dodatku k tejto Zmluve o dielo.
- 18.3 Objednávateľ je oprávnený v odôvodnených prípadoch v súlade s § 18 Zákona o VO písomne navrhnúť zmenu Diela alebo jeho časti, jeho doplnenie alebo rozšírenie a v súlade s uvedeným aj zmenu a doplnenie tejto Zmluvy o dielo.
- 18.4 Akúkoľvek inú zmenu tejto Zmluvy o dielo možno uskutočniť formou písomného dodatku podpísaného štatutárnymi zástupcami oboch Zmluvných strán postupom v zmysle všeobecne záväzných právnych predpisov.

#### **Článok 19. POVINNOSŤ ZHOTOVITEĽA PRI VÝKONE AUDITU/KONTROLY/OVEROVANIA**

- 19.1 Tento Článok 19. tejto Zmluvy o dielo sa uplatní len v prípade a v rozsahu v akom predstavujú finančné prostriedky Objednávateľa určené na zaplatenie Ceny za Dielo prostriedky z EŠIF.



- 19.2 Zhotoviteľ berie na vedomie, že finančné prostriedky Objednávateľa určené na zaplatenie Ceny za Dielo podľa Článok 9. tejto Zmluvy o dielo sú finančné prostriedky z Európskeho fondu regionálneho rozvoja a zároveň sú finančné prostriedky zo štátneho rozpočtu SR.
- 19.3 Zhotoviteľ berie na vedomie, že podpisom tejto Zmluvy o dielo sa stáva súčasťou Systému riadenia EŠIF a Systému finančného riadenia. Zhotoviteľ zároveň berie na vedomie, že na použitie prostriedkov, kontrolu použitia týchto prostriedkov a vymáhanie ich neoprávneného použitia alebo zadržania sa vzťahuje režim upravený v osobitných všeobecne záväzných právnych predpisoch, napr. v Zákone č. 357/2015 Z. z., Zákone č. 523/2004 Z. z., Zákone o EŠIF, Zákon č. 528/2008 Z. z. a v ďalších príslušných všeobecne záväzných predpisoch SR a právnych aktov EÚ.
- 19.4 Zmluvné strany sa dohodli a súhlasia, že všetky zmeny v Systéme riadenia EŠIF, Systéme finančného riadenia EŠIF, Systéme riadenia EŠIF alebo v právnych dokumentoch vydaných oprávnenými osobami, z ktorých pre Zhotoviteľa vyplývajú práva a povinnosti v súvislosti s plnením podľa tejto Zmluvy o dielo a Zmluvy o poskytnutí NFP, ak boli tieto dokumenty zverejnené, sú pre Zhotoviteľa záväzné dňom ich zverejnenia.
- 19.5 Okrem povinností uvedených v tejto Zmluve o dielo je Zhotoviteľ povinný strpieť výkon kontroly/audit/overovania oprávnenými osobami v súvislosti s vykonaným Dielom alebo jeho časťou v zmysle tejto Zmluvy o dielo a poskytnúť im všetku potrebnú súčinnosť, a to kedykoľvek počas platnosti a účinnosti tejto Zmluvy o dielo, ako v termínoch stanovených pre Objednávateľa v zmluvných vzťahoch s príslušnými orgánmi zapojenými do implementácie fondov EÚ, v rámci ktorých si Objednávateľ nárokuje financovanie výdavkov uhradených Zhotoviteľovi, ktoré vznikli s plnením podľa tejto Zmluvy o dielo.
- 19.6 Zhotoviteľ sa zaväzuje umožniť výkon finančnej kontroly/audit/overovania príslušnými oprávnenými osobami uvedenými v nasledujúcom bode a vytvoriť podmienky pre jej výkon v zmysle príslušných platných a účinných právnych predpisov SR a právnych aktov EÚ a ako kontrolovaný subjekt pri výkone kontroly riadne plniť povinnosti, ktoré mu vyplývajú z uvedených predpisov, a to počas platnosti a účinnosti tejto Zmluvy o dielo a počas platnosti a účinnosti Zmluvy o poskytnutí NFP. Uvedená doba sa predĺži v prípade, ak nastanú skutočnosti predpokladané relevantnými všeobecne záväznými právnymi predpismi EÚ.
- 19.7 Zhotoviteľ sa zaväzuje podrobiť sa aj výkonu kontroly poverenými zamestnancami Objednávateľa. Poverení zamestnanci Objednávateľa vykonávajúci kontrolu majú počas celého programového obdobia OPII prístup ku všetkým obchodným dokumentom Zhotoviteľa súvisiacim s výdavkami a plnením povinností podľa tejto Zmluvy o dielo.
- 19.8 Oprávnenými osobami pre účely tohto Článok 19. tejto Zmluvy o dielo sú najmä:
- Zodpovedná osoba Objednávateľa podľa bodu 12.3 tejto Zmluvy o dielo a ním poverené osoby,
  - zástupcovia príslušného riadiaceho orgánu a sprostredkovateľského orgánu, prípadne iných relevantných orgánov a nimi poverené osoby,
  - Najvyšší kontrolný úrad SR, Úrad pre verejné obstarávanie, Úrad vládného auditu, OLAF, Certifikačný orgán a nimi poverené osoby,
  - orgán auditu, jeho spolupracujúce orgány a nimi poverené osoby,
  - splnomocnení zástupcovia Európskej Komisie a Európskeho dvora audítorov,
  - orgán zabezpečujúci ochranu finančných záujmov EÚ,
  - osoby prizvané alebo poverené orgánmi podľa tohto bodu 19.8 písm. a) až f) tejto Zmluvy o dielo v súlade s príslušnými všeobecne záväznými právnymi predpismi SR a EÚ,
  - vecne príslušná autorita v zmysle Zákona o KB.

- 19.9 Zhotoviteľ berie na vedomie, že sprostredkovateľský orgán operačného programu Integrovaná infraštruktúra prioritná os 7 Informačná spoločnosť pre programové obdobie 2014 – 2020 je pri vykonávaní administratívnej finančnej kontroly v nevyhnutnom rozsahu oprávnený od Objednávateľa alebo od osoby, ktorá je vo vzťahu k finančnej operácii alebo jej časti Zhotoviteľom výkonov, prác alebo služieb alebo akejkoľvek inej osoby, ktorá má informácie, doklady alebo iné podklady, ktoré sú potrebné pre výkon finančnej kontroly, ak ich poskytnutiu nebráni osobitný predpis:
- a) vyžadovať a odoberať, v určenej lehote originály alebo úradne osvedčené kópie dokladov, písomností, záznamy dát na pamäťových médiách prostriedkov výpočtovej techniky, ich výpisov, výstupov, vyjadrenia, informácie, dokumenty a iné podklady súvisiace s administratívnou finančnou kontrolou alebo finančnou kontrolou na mieste,
  - b) vyžadovať od tretej osoby podľa tohto bodu 18.9 tejto Zmluvy o dielo súčinnosť v rozsahu oprávnení v zmysle zákona č. 357/2015 Z. z.,
  - c) osoby poverené na výkon kontroly sú oprávnené v nevyhnutnom rozsahu za podmienok ustanovených v osobitných predpisoch okrem oprávnení uvedených v predchádzajúcich písmenách vstupovať do objektu, zariadenia, prevádzky, dopravného prostriedku, na pozemok tretej osoby, alebo vstupovať do obydľia, ak sa používa aj na podnikanie alebo na vykonávanie inej hospodárskej činnosti,
  - d) oboznámiť sa pri začatí finančnej kontroly na mieste s bezpečnostnými predpismi, ktoré sa vzťahujú na priestory, v ktorých sa vykonáva finančná kontrola na mieste.
- 19.10 Sprostredkovateľský orgán je pri vykonávaní administratívnej finančnej kontroly v zmysle zákona č. 357/2015 Z. z. povinný potvrdiť tretej osobe podľa bodu 19.9 tejto Zmluvy o dielo odobratie poskytnutých originálov alebo úradne osvedčených kópií dokladov, písomností, záznamov dát na pamäťových médiách, prostriedkov výpočtovej techniky, ich výpisov, výstupov, vyjadrení, informácií, dokumentov a iných podkladov súvisiacich s administratívnou finančnou kontrolou alebo finančnou kontrolou na mieste a zabezpečiť ich riadnu ochranu pred stratou, zničením, poškodením a zneužitím (uvedené potvrdenie sa vydáva, ak Sprostredkovateľský orgán žiada o poskytnutie podkladov nad rámec definovaný Zmluvou o poskytnutí NFP); tieto veci Sprostredkovateľský orgán vráti bezodkladne tomu, od koho sa vyžiadali, ak nie sú potrebné na konanie v zmysle Trestného poriadku alebo na iné konanie podľa osobitných všeobecne záväzných právnych predpisov. Zhotoviteľ je povinný zabezpečiť prítomnosť oprávnených osôb zo strany Zhotoviteľa počas vykonávania kontroly u Zhotoviteľa.
- 19.11 Vykonaním kontroly oprávnenej osoby podľa Zmluvy o poskytnutí NFP nie je dotknuté právo riadiaceho orgánu alebo inej oprávnenej osoby na vykonanie novej kontroly/vládneho auditu, a to počas celej doby účinnosti Zmluvy o poskytnutí NFP.
- 19.12 Zmluvné strany sa zaväzujú, že počas vykonávania Diela alebo jeho časti podľa tejto Zmluvy o dielo budú navzájom spolupracovať a vyvinú maximálne úsilie a súčinnosť, aby bol jej predmet zrealizovaný v súlade s touto Zmluvou o dielo. Zhotoviteľ je povinný zabezpečiť prijatie nápravných opatrení a definovanie termínov na odstránenie zistených nedostatkov.
- 19.13 V nadväznosti na vyššie sa Zhotoviteľ zaväzuje sledovať a dodržiavať všetky zmeny prijímané orgánmi EÚ a orgánmi štátnej správy, verejnej správy a samosprávy, a na základe toho realizovať ad hoc konzultácie s Objednávateľom a bez zbytočného odkladu upozorniť Objednávateľa na dôležité skutočnosti vzťahujúce sa na predmet plnenia tejto Zmluvy o dielo.

## **Článok 20. BEZPEČNOSŤ VÝVOJA DIELA ALEBO JEHO ČASTI**

- 20.1 Zhotoviteľ sa v súvislosti s plnením tejto Zmluvy o dielo zaväzuje dodržiavať bezpečnostnú politiku Objednávateľa, ďalšie Objednávateľom vydané bezpečnostné smernice a štandardy,

požiadavky na bezpečnosť definované Zákonom o KB, Zákonom o ITVS, Vyhláškou č. 78/2020 Z. z., Vyhláškou č. 179/2020 Z. z. a bezpečnostné požiadavky uvedené v tejto Zmluve o dielo.

- 20.2 Oprávnené osoby a pracovníci Zhotoviteľa, ktorí budú vykonávať pre Objednávateľa činnosti súvisiace s plnením tejto Zmluvy o dielo musia byť poučení o povinnostiach podľa predchádzajúceho bodu a o tomto poučení musí Zhotoviteľ vytvoriť záznam, ktorý bude podpísaný poučenou osobou a osobou, ktorá poučenie vykonala. Za riadne poučenie zodpovedá Zhotoviteľ.
- 20.3 Zhotoviteľ sa zaväzuje zaistiť bezpečnosť a odolnosť dodávaného riešenia voči aktuálne známym typom útokov a pred jeho odovzdaním vykonať testovanie na prítomnosť známych zraniteľností. V prípade zistenia zraniteľností sa Zhotoviteľ zaväzuje tieto zraniteľnosti odstrániť, vykonať opätovné testovanie a zdokumentovaný výsledok testovania odovzdať Objednávateľovi spolu s dodávaným riešením.
- 20.4 Zhotoviteľ sa zaväzuje dodržiavať nasledovné bezpečnostné opatrenia a zásady:
- je zapnutá len nutne potrebná funkcionálna, porty a IP adresy a všetky ostatné sú vypnuté,
  - v prípade, že je nevyhnutné vykonávať správu Diela alebo jeho časti na diaľku, je to možné vykonávať výhradne prostredníctvom šifrovaných protokolov,
  - všetky pôvodné a administrátorské účty sú zdokumentované a majú unikátne prvotné heslo zložené z náhodnej postupnosti aspoň 8 (slovom: ôsmich) znakov,
  - Dielo alebo jeho časť disponuje funkcionálnosťou pre zmenu používateľských a administrátorských mien a hesiel a funkcionálnosťou vypnutia používateľského účtu,
  - všetky komponenty dodávaného Diela alebo jeho časti sú aktuálne a podporované výrobcom a postup pre aktualizácie a aplikáciu záplat je zdokumentovaný a dodržiavaný,
  - Zhotoviteľ umožní Objednávateľovi vykonať skeny zraniteľností alebo penetračné testy dodávaného Diela alebo jeho časti pred jeho finálnym odovzdaním a Zhotoviteľ sa zaväzuje nedostatky zistené týmto testovaním pred odovzdaním riešenia odstrániť.
- 20.5 Dielo alebo jeho časť musí byť vyvíjaná v bezpečnom vývojovom prostredí s použitím nástrojov, ktoré:
- musia byť získané legálnym spôsobom z dôveryhodných zdrojov,
  - musia byť podporované výrobcom (t. j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané
  - musia byť aktualizované minimálne raz za 6 (slovom: šesť) mesiacov a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.
- 20.6 Pri implementácii by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky / knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb (napr. knižnice a komponenty dodané tretími stranami; systémy, na ktorých bude Dielo postavené alebo ktoré bude využívať pri svojej prevádzke).
- 20.7 V prípade, že implementované Dielo alebo jeho časť potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.
- 20.8 Zhotoviteľ nesmie používať funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v súčasnej dobe zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.

## Článok 21. TRVANIE A UKONČENIE ZMLUVY O DIELO

- 21.1 Táto Zmluva o dielo sa uzatvára na dobu určitú, a to do dňa úplného odovzdania celého Diela, ku ktorému dôjde podpísaním Záverečného akceptačného protokolu s tým, že maximálna lehota na úplné odovzdanie celého Diela je podľa bodu 5.2 tejto Zmluvy o dielo je 12 (slovom: dvanásť) mesiacov odo dňa účinnosti tejto Zmluvy o dielo, a to vrátane skúšobnej prevádzky podľa Článok 6. tejto Zmluvy o dielo.
- 21.2 Táto Zmluva o dielo zaniká:
- uplynutím doby, na ktorú bola uzatvorená,
  - písomnou dohodou Zmluvných strán,
  - odstúpením od tejto Zmluvy o dielo.
- 21.3 Pokiaľ bude táto Zmluva o dielo predčasne ukončená dohodou Zmluvných strán, tvorí stanovenie spôsobu vysporiadania vzťahov vzniknutých na základe tejto Zmluvy o dielo podstatnú náležitosť dohody o ukončení tejto Zmluvy o dielo. V rámci tejto dohody sa vysporiada aj udelenie licencií k odovzdaným častiam Diela alebo Dielu celému a jeho súčasti v súlade s touto Zmluvou o dielo.
- 21.4 Zmluvné strany sú oprávnené odstúpiť od tejto Zmluvy o dielo z dôvodu podstatného porušenia zmluvných povinností druhou Zmluvnou stranou, nepodstatného porušenia zmluvných povinností druhou Zmluvnou stranou v prípadoch, ak to umožňuje zákon alebo táto Zmluva o dielo. Zmluvné strany sú oprávnené tiež odstúpiť od tejto Zmluvy o dielo aj v ďalších prípadoch predpokladaných touto Zmluvou o dielo alebo zákonom.
- 21.5 Odstúpenie od Zmluvy o dielo musí byť vykonané v písomnej forme, riadne odôvodnené a doručené na aktuálnu verejne známu adresu druhej Zmluvnej strany formou doporučenej zásielky.
- 21.6 Zmluvné strany sa dohodli, že každé porušenie tejto Zmluvy o dielo sa považuje za nepodstatné porušenie povinnosti, tej ktorej Zmluvnej strany, ktorá túto Zmluvu o dielo porušila s výnimkou takého porušenia tejto Zmluvy o dielo, ktoré je v tejto Zmluve o dielo výslovne označené ako podstatné porušenie zmluvných povinností.
- 21.7 Zmluvné strany sa dohodli, že okrem prípadov uvedených v iných článkoch tejto Zmluvy o dielo sa považuje za podstatné porušenie zmluvných povinností aj:
- odobratie oprávnenia Zhotoviteľa na predmet podnikania, ktorý ho oprávňuje plniť túto Zmluvu o dielo,
  - skutočnosť, že Zhotoviteľ vstúpi do likvidácie, bude na neho vyhlásený konkurz alebo bude voči nemu zamietnutý návrh na vyhlásenie konkurzu pre nedostatok majetku,
  - nastanú iné dôvody v zmysle ust. § 344 Obchodného zákonníka a nasl.,
  - pri plnení tejto Zmluvy o dielo Objednávateľ zistí, že Zhotoviteľ uviedol v ponuke predloženej vo verejnom obstarávaní, na základe ktorej bola uzatvorená táto Zmluva o dielo nepravdivé alebo skreslené údaje.
- 21.8 V prípade podstatného porušenia tejto Zmluvy o dielo je Zmluvná strana oprávnená od tejto Zmluvy o dielo odstúpiť bez zbytočného odkladu po tom, ako sa o tomto porušení dozvedela. Zmluvné strany sa osobitne dohodli, že porušenie tejto Zmluvy o dielo je podstatné, ak Zmluvná strana porušujúca túto Zmluvu o dielo vedela v čase uzavretia tejto Zmluvy o dielo alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel tejto Zmluvy o dielo, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola táto Zmluva o dielo uzavretá, že druhá Zmluvná strana nebude mať záujem na plnení povinností pri takom porušení tejto Zmluvy o dielo.
- 21.9 V prípade nepodstatného porušenia tejto Zmluvy o dielo je Zmluvná strana oprávnená odstúpiť od tejto Zmluvy o dielo, ak Zmluvná strana, ktorá je v omeškaní s plnením svojej povinnosti, nesplní svoju povinnosť ani v dodatočnej primeranej lehote, ktorá jej na to bola poskytnutá v

pisomnom vyzvaní. To isté platí, ak Zmluvná strana, ktorá spôsobila vznik protiprávneho stavu, tento stav neodstráni ani v dodatočnej lehote určenej vo vyzvaní.

- 21.10 Zmluvné strany sa dohodli, že predtým, ako oprávnená Zmluvná strana využije svoje právo odstúpiť od tejto Zmluvy o dielo z akékoľvek dôvodu, požiada druhú Zmluvnú stranu o písomné vysvetlenie alebo spoločné rokovanie za účelom vzájomného vysvetlenia dôvodov pre odstúpenie; a prípadné písomné odstúpenie od tejto Zmluvy o dielo zašle najskôr po uplynutí 7 (slovom: siedmych) pracovných dní odo dňa doručenia takejto výzvy.
- 21.11 Pre prípady ukončenia tejto Zmluvy o dielo podľa tohto Článok 21. tejto Zmluvy o dielo platí, že Zmluvná strana, ktorá odstúpila od tejto Zmluvy o dielo, si ponechá odovzdané a prevzaté plnenia, ak takéto plnenie má zrejme vzhľadom na svoju povahu pre oprávnenú stranu hospodársky význam bez zvyšku plnenia, pri ktorom nastalo omeškanie, napr. sú objektívne použiteľné za účelom pokračovania dodávky Diela alebo jeho časti, alebo sa jedná o samostatne funkčnú časť Diela alebo jeho časti. V takomto prípade vzniká druhej Zmluvnej strane nárok na dohodnutú pomernú časť Ceny za Dielo v závislosti od miery plnenia časti Diela.
- 21.12 Skončenie tejto Zmluvy o dielo sa nedotýka nároku na náhradu škody vzniknutej porušením tejto Zmluvy o dielo, nároku na zaplatenie zmluvnej pokuty, ktorý vznikol do účinnosti odstúpenia, a ďalej ustanovení, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení tejto Zmluvy o dielo, najmä ustanovenia o povinnosti mlčanlivosti, komunikácii a riešení sporov.

## Článok 22. ZÁVEREČNÉ USTANOVENIA

- 22.1 Táto Zmluva o dielo nadobúda platnosť dňom jej podpisu oboma Zmluvnými stranami.
- 22.2 Táto Zmluva o dielo nadobúda účinnosť v prípade kumulatívneho splnenia nasledujúcich podmienok:
- ukončenie finančnej kontroly doručením správy z tejto kontroly Objednávateľovi, v rámci ktorej riadiaci orgán OPII neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok Verejného obstarávania; za deň splnenia tejto časti odkladacej podmienky sa považuje deň, kedy Objednávateľ písomne oznámi Zhotoviteľovi, že došlo k ukončeniu finančnej kontroly, v rámci ktorej riadiaci orgán neidentifikoval nedostatky, ktoré by mali alebo mohli mať vplyv na výsledok Verejného obstarávania (po doručení správy z kontroly Objednávateľovi),
  - zverejnenie Zmluvy o dielo v súlade s ustanovením § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov v spojení s § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov. Zmluvné strany súhlasia so zverejnením celej zmluvy, okrem osobných údajov kľúčových expertov v rozsahu meno, priezvisko.
- 22.3 Výsledky plnenia tejto Zmluvy o dielo predstavujúce obchodné tajomstvo Zhotoviteľa, ustanovenia týkajúce sa ochrany utajovaných skutočností, ako i technické predlohy, návody, výkresy, projektové dokumentácie, modely, spôsob výpočtu jednotkových cien a vzory (§ 5a ods. 4 zákona o slobode informácií) sa nezverejňujú.
- 22.4 Zmluvné strany sa dohodli, že akékoľvek oznámenie alebo iná formálna komunikácia Zmluvných strán bude uskutočňovaná písomne prostredníctvom kontaktných údajov v zmysle tejto Zmluvy o dielo s tým, že každá zo Zmluvných strán sa zaväzuje oznámiť druhej Zmluvnej strane akúkoľvek ich zmenu.
- 22.5 Ak v priebehu trvania tejto Zmluvy o dielo Zhotoviteľ zmení názov/obchodné meno, prípadne dôjde k jeho rozdeleniu, zlúčeniu, splynutiu alebo úpadku, je povinný o tejto skutočnosti bezodkladne písomne informovať Objednávateľa, spolu s uvedením, ako prechádzajú práva a

záväzky z tejto Zmluvy o dielo na jeho právneho nástupcu. Objednávateľ uzavrie s právnym nástupcom dodatok k tejto Zmluve o dielo v zmysle príslušných ustanovení Zákona o VO, ak k právnemu nástupníctvu nedochádza zo zákona.

- 22.6 Zmluvné strany sa dohodli, že vzťahy neupravené touto Zmluvou o dielo sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatných relevantných všeobecne záväzných predpisov. Rozhodným právom na účely prejednávania a rozhodnutia sporov, ktoré vzniknú z tejto Zmluvy o dielo alebo v súvislosti s ňou je právo SR.
- 22.7 Bez toho, aby tým bolo dotknuté ktorékoľvek ustanovenie tejto Zmluvy o dielo, Zmluvné strany sa dohodli, že použitie akéhokoľvek ustanovenia ktoréhokoľvek všeobecne záväzného predpisu, ktoré nie je kogentné, je výslovne vylúčené v rozsahu, v ktorom by jeho použitie mohlo meniť (či už úplne alebo čiastočne) význam alebo obsah ktoréhokoľvek ustanovenia tejto Zmluvy o dielo.
- 22.8 V prípade vzniku sporu z tejto Zmluvy o dielo alebo v súvislosti s ňou sa Zmluvné strany zaväzujú vyvinúť maximálne úsilie na vyriešenie takéhoto sporu primárne vzájomnou dohodou a zmerom a v prípade neúspechu sú na prejednanie a rozhodnutie takýchto sporov príslušné súdy SR.
- 22.9 Jednotlivé ustanovenia tejto Zmluvy o dielo sú vymáhateľné nezávisle od seba a neplatnosť ktoréhokoľvek z nich nebude mať žiaden vplyv na platnosť ostatných ustanovení, s výnimkou prípadov, kedy je z dôvodu dôležitosti povahy alebo inej okolnosti týkajúcej sa takéhoto neplatného ustanovenia zrejmé, že dané ustanovenie nemôže byť oddelené od ostatných príslušných ustanovení. V prípade, ak niektoré z uvedených ustanovení bude neplatné, Zmluvné strany sa zaväzujú zabezpečiť uskutočnenie všetkých krokov potrebných za tým účelom, aby bolo dohodnuté ustanovenie s podobným účinkom, ktorým sa neplatné ustanovenie v súlade s príslušným právnym predpisom nahradí.
- 22.10 Neoddeliteľnou súčasťou tejto Zmluvy o dielo sú nasledovné prílohy:
- a) **Príloha č. 1:** Opis predmetu zákazky – časť I., podľa súťažných podkladov - v časti B.1 OPIS PREDMETU ZÁKAZKY
  - b) **Príloha č. 2:** Zhotoviteľom vyplnená Príloha č. 3 súťažných podkladov – Návrh na plnenie kritérií pre časť č. I predmetu zákazky
  - c) **Príloha č. 3:** Zoznam subdodávateľov Zhotoviteľom vyplnená Príloha č. 6 súťažných podkladov – Čestné vyhlásenie uchádzača o subdodávateľoch.
  - d) **Príloha č. 4:** Zoznam Kľúčových expertov
- 22.11 Táto Zmluva o dielo je vyhotovená v 4 (slovom: štyroch) vyhotoveniach s platnosťou originálu, z toho 2 (slovom: dve) vyhotovenia obdrží Objednávateľ a 2 (slovom: dve) vyhotovenia obdrží Zhotoviteľ.
- 22.12 Zmluvné strany týmto vyhlasujú, že obsah tejto Zmluvy o dielo im je známy, predstavuje ich vlastnú slobodnú a vážnu vôľu, je vyhotovený v správnej forme, a že tomuto obsahu aj jeho právnym dôsledkom porozumeli a súhlasia s nimi, na znak čoho pripájajú svoje vlastnoručné podpisy.
- 22.13 Vzhľadom na výšku plnenia predmetu zmluvy Zhotoviteľ vyhlasuje, že je zapísaný v registri partnerov verejného sektora v zmysle zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Táto povinnosť zápisu do registra partnerov verejného sektora v zmysle zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov sa vzťahuje aj na subdodávateľov a iné osoby, ktorých kapacity má zhotoviteľ využiť, pokiaľ príslušný právny predpis neustanovuje inak.

Za Zhotoviteľa

V Bratislave dňa: 5.8.2022

Za Objednávateľa

V Šali, dňa:.....

.....  
Mgr. Jakub Čeles  
konateľ spoločnosti

.....  
Mgr. Jozef Belický  
primátor mesta Šaľa

.....  
Ing. Štefan Kopaj  
konateľ spoločnosti

.....  
Ing. Rudolf Törvényi  
konateľ spoločnosti





**OPIS PREDMETU ZÁKAZKY**

**ROZSAH PREDMETU OBSTARÁVANIA:**

**ČASŤ I.: DODÁVKA A IMPLEMENTÁCIA SYSTÉMOVÝCH NÁSTROJOV NA ZABEZPEČENIE KYBERNETICKEJ BEZPEČNOSTI MESTA ŠAĽA**

**1. Centrálny logovací systém (+ 5 ročný premium support)**

*Predmetom zákazky* je dodávka a implementácia systému pre centralizované ukladanie a správa logov s integrovaným systémom analýzy a riešenia bezpečnostných udalostí/incidentov zo systémov a aplikácií verejného obstarávateľa.

Monitorovať bezpečnosť sietí a informačných systémov implementáciou centrálného nástroja na zaznamenávanie činnosti sietí, informačných systémov a ich používateľov pomôže mestu Šaľa zaistiť dodržiavanie požiadaviek zákona č. 69 z 30. januára 2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len ZKB); vyhlášky č. 164 Národného bezpečnostného úradu z 1. júna 2018, ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby). Ide najmä o povinnosti pre prevádzkovateľov základnej služby, plnenie bezpečnostných opatrení, riešenie kybernetických bezpečnostných incidentov a vykonanie auditu kybernetickej bezpečnosti. Okrem nižšie špecifikovaných vlastností na zariadenie všeobecne požadujeme správu protokolov udalostí (logov), poskytujúci jednoduché zobrazenie všetkých strojovo generovaných dát, zhromažďovanie, unifikáciu a dlhodobé uchovávanie protokolov udalostí a záznamov o udalostiach z aktívnych sieťových prvkov, bezpečnostných zariadení, operačných systémov a aplikačného softvéru. v sieti mesta Šaľa. Ukladanie a zhromažďovanie dát musí prebiehať „takmer reálnom čase“ (near real-time) do definovanej výkonnej databázy, ku ktorej môžu IT špecialisti pristupovať prostredníctvom preddefinovaných riadiacich panelov a štruktúrovaného i fulltextového vyhľadávania s grafickým zobrazením výsledkov.

Ďalej požadujeme aj základné SIEM funkcie, ako sú upozornenia s limitmi a jednoduché korelácie. Na nasadenie s cieľom získať súlad so ZKB sú tieto integrované SIEM funkcie dostatočné. V budúcnosti ak budeme požadovať pokročilejšie analytické a korelačné funkcie musí zariadenie zvládnuť jednoduchú integráciu s inými nástrojmi používanými na monitorovanie alebo analýzu dát, dátových tokov, aplikácií a operačných systémov ako aj implementáciu v takých zložitých a komplikovaných prostrediach ako sú IoT a SCADA.

Všetky technické parametre/funkcionality, resp. vlastnosti požadovaného predmetu zákazky predstavujú minimálne požiadavky, ktoré musia byť splnené v ponuke uchádzača. V prípade, že by sa záujemca/uchádzač cítil dotknutý vo svojich právach, t. j., že by týmto opisom dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov/uchádzačov alebo výrobcov, alebo že tento predmet zákazky nie je opísaný dostatočne presne a zrozumiteľne, tak vo svojej ponuke môže uchádzač použiť technické riešenie ekvivalentné, ktoré spĺňa kvalitatívne, technické, funkčné požiadavky na rovnakej a vyššej úrovni, ako je uvedené v tejto časti súťažných podkladov, túto skutočnosť však musí preukázať uchádzač vo svojej ponuke.

## ŠPECIFIKÁCIA HARDWARU

<b>Počet:</b>	1 ks
<b>Základná špecifikácia:</b>	<p>Centrálny logovací systém by mal pracovať ako fyzická appliance s jedným uceleným webovým rozhraním pre všetky administrátorské i operátorské činnosti. Nevyžaduje inštaláciu ďalších systémov a aplikácií okrem podpory zberu na iných lokalitách (mimo centrálu) a agenta pro zber Windows logov. Konfigurácia systému sa musí vykonávať v grafickom rozhraní jednotnej užívateľskej konzoly, Systém poskytuje podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát.</p> <p>Systém má umožňovať doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľom bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému - užívateľsky definované parsery. Dokumentácia systému musí obsahovať prehľadný návod na vytváranie zákaznických parserov a systém musí obsahovať možnosť testovania a ladenia parserov bez vplyvu na ostatné produkčné funkcie systému. Pre vytváranie je požité tzv. vizuálne programovanie, ktoré automaticky opravuje a upozorňuje na chyby.</p> <p>Systém musí umožňovať v grafickom rozhraní vizuálneho programovacieho jazyka jednoducho vykonávať triedenie a značkovanie vstupných dát pre ich ďalšie spracovanie.</p> <p>Systém má prijímať a spracovávať logy, udalosti a ďalšie strojovo generované dáta prostredníctvom minimálne nasledujúcich protokolov: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovane) a TCP 20515 (RELP, šifrovane). Systém musí umožňovať príjem logov i na rozsahu minimálne 50 UDP a TCP portov.</p> <p>Prijaté logy systém má štandardizovať do jednotného formátu a logy sú rozdeľované príslušných polí podľa ich typu. Systém musí zároveň uchovávať originálne verzie správ.</p> <p>Pre hodnoty jednotlivých parsovaných polí musí byť možné v definícii parseru zmeniť typ a štandardizovať minimálne na tieto základné druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými dátami typu číslo je možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšie/najväčšia hodnota a pod.)</p> <p>Centrálny logovací systém musí zachovávať pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, ktorá vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi.</p> <p>Všetky polia a položky prijaté systémom musia byť automaticky indexované. Nad všetkými položkami musí byť možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom.</p> <p>Centrálny logovací systém musí umožňovať zber udalostí vo formátoch RAW, Syslog, CEF, LEEF, JSON RFC7159.</p> <p>Centrálny logovací systém neumožňuje mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log musí mať unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.</p>

Centrálny logovací systém musí umožňovať konfiguráciu filtrácie nerelevantných správ, konsolidáciu logov na vlastnom storage priestore, jednoduché vyhľadávanie udalostí a okamžité vytváranie grafických reportov (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. Reportovací nástroj musí byť integrálnou súčasťou systému a aj súčasťou jednotného rozhrania.

Centrálny logovací systém musí vykonávať ucelenú vizualizáciu logov, udalostí a strojových dát (grafy udalostí). Vizualizácia má byť dynamická, t. j. voľbou v jednom grafe sa ostatné príslušné grafy v pohľade na dáta upravia podľa požadovanej voľby automaticky.

Centrálny logovací systém musí umožňovať jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurácie systému alebo parametrov uložených dát. Historické dáta v požadovanej dĺžke retencie uložené v systéme je možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nevyžaduje manuálnu konfiguráciu a zásahy používateľa.

Centrálny logovací systém musí vykonávať automatické dopĺňovanie reverzných DNS záznamov a GeolIP informácií k udalostiam a v prípade GeolIP ich grafické znázornenie na mape bez nutnosti využívať služby tretích strán či externé aplikácie.

Ďalej musí podporovať natívne získavanie logov z Office365.

V prípade krátkodobého preťaženia systému nemôže dochádzať k strate logov. Všetky prijaté nespracované logy/udalosti sú ukladané do vyrovnávacej pamäte.

Centrálny logovací systém musí umožňovať unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí a musí spĺňať požiadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov.

Centrálny logovací systém má mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie.

Centrálny logovací systém musí obsahovať reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov.

Centrálny logovací systém musí obsahovať predpripravené pohľady na uložené dáta podľa jednotlivých kategórií zdrojových zariadení i podľa logického členenia.

Na základe pohľadu na uložené dáta je možné vykonať export dát v štruktúrovanom formáte tak, ako sú v pohľade skutočne zobrazované.

Konfiguračné a systémové rozhranie a dokumentácia sú identické v anglickom i v slovenskom alebo českom jazyku.

Centrálny logovací systém musí umožňovať kapacitnú i výkonovú škálovateľnosť.

Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP alebo Syslog.

Centrálny logovací systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)

	<p>Centrálny logovací systém musí obsahovať jednotnú centrálna webovú konzolu pre prístup k logom, alertom, reportom a pre správu systému. Z tejto konzoly sa vykonáva kompletná konfigurácia, správa a analýza logov.</p> <p>Centrálny logovací systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému, vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní.</p> <p>Centrálny logovací systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Systém má automaticky zaznamenávať užívateľské meno ku každej akcii užívateľom.</p>
<p><b>HW parametre systému:</b></p>	<p>HW appliance v rackovom prevedení s 1U, vrátane ramena pre organizáciu zapojených káblov umožňujúceho vysunutie zapnutého systému z racku pre servisné účely.</p> <p>HW appliance musí obsahovať všetky potrebné komponenty a musí byť nezávislá na ďalších systémoch.</p> <p><b>Minimálne parametre:</b></p> <ul style="list-style-type: none"> <li>• 1 procesor, 12 jader s podporou HyperThreadingu;</li> <li>• Min. 64GB RAM DDR-4;</li> <li>• Diskový subsystém s čistou dostupnou kapacitou min. 12TB pre integrovanú databázu;</li> <li>• HW akcelerovaný SAS RAID radič s read-write cache min. 8GB;</li> <li>• Min. 4 ks rovnakých RAID edition diskov určených pre použitie v datacentrách, s rýchlosťou 7200 otáčiek/m;</li> <li>• Min. 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pre management HW;</li> <li>• Redundantné ventilátory, vymeniteľné za chodu;</li> <li>• Napájacie zdroje s redundanciou 1+1, vymeniteľné za chodu, účinnosť min. 94%;</li> <li>• Virtuálne KVM, tj. prevzatie textovej i grafickej konzoly serveru a prenos povelov z klávesnice a myši vzdialeného počítača;</li> <li>• Systém pre vzdialenú správu serveru vrátane potrebnej licencie.</li> </ul>
<p><b>Výkonnostné a SW parametre systému:</b></p>	<p>Centrálny logovací systém musí fungovať formou HW appliance (všetky časti systému je možné nastaviť v centrálnej webovej konzole a nie je potrebné upravovať žiadne konfiguračné súbory, scripty, alebo makra v príkazovom riadku).</p> <p>Aktualizácie systému by mali byť distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. Všetky aktualizácie by mali byť vykonávané z webového rozhrania systému bez potreby asistencie výrobcu/dodávateľa.</p> <p>Systém musí podporovať downgrade, napríklad pri problémoch s novou verziou systému po upgrade.</p> <p>Priemerný trvalý príjem by mal byť 2000 udalostí za sekundu pri priemernej veľkosti jednej udalosti 700Byte. Systém by mal vedieť preukázateľne kompletne spracovať prijaté udalosti vrátane vytvorenia očakávaných metadát (DNS-PTR, čísla a mená ASN, geolokácie), zaisťovanie normalizácie, zamedzovania straty prijatých udalostí, alebo posunutiu dôveryhodného časového razítka udalosti.</p>

Špičkový príjem by mal byť 4000 udalostí za sekundu po dobu 10 minút pri priemernej veľkosti jednej udalosti 700Byte. Systém pri špičkovom príjme preukázateľne kompletne spracováva prijaté udalosti vrátane vytvorenia očakávaných metadát (DNS-PTR, čísla a mená ASN, geolokácie), zaisťovanie normalizácie, zamedzovania straty prijatých udalostí, alebo posunutiu dôveryhodného časového razítka udalosti.

Licenčne musí byť neobmedzený počet zariadení pre príjem zasielaných udalostí. Licenčne musí byť neobmedzený počet udalostí v GB za deň. Integrovaná databáza má čistú veľkosť 12 TB a musí podporovať kompresiu ukladaných dát.

Centrálny logovací systém musí podporovať doplňovanie správ o statické informácie z textových tabuliek, napríklad k užívateľskému menu doplniť informáciu o jeho emailovej adrese, členstve v AD skupinách a pod. Pre automatickú aktualizáciu takto uložených doplnkových informácií musí byť možné tieto textové tabuľky doplniť pomocou REST API systému a modifikovateľné cez webové rozhranie systému.

Centrálny logovací systém musí umožňovať on-line ladenia užívateľsky definovaných parserov - pri ich vytváraní je možné vložiť vlastné testovacie správy, pri zmene je okamžite zobrazená výsledná podoba rozparsovaných dát a prípadné chybové hlásenia.

Centrálne správovská konzola musí umožňovať pridávať k jednotlivým zdrojom dát, aplikáciám, zariadeniam alebo IP subnetom tzv. značky, označujúce napríklad umiestnenie zariadenia, typ zariadenia, kritickosť zariadenia a pod. Systém musí obsahovať preddefinované značky, ktoré automaticky pridáva k prijímaným správam (napríklad konfiguračná zmena, úspešné overenie užívateľa, neúspešné overenie užívateľa, správa z Windows, správa generovaná firewallom a pod.)

Všetky pridávané značky sú ukladané s každou prijatou udalosťou, na základe značky je možné filtrovať dáta alebo obmedzovať oprávnenia užívateľov systému k jednotlivým udalostiam.

Centrálny logovací systém by mal byť predpripravený pre zrkadlenie a clustrové zapojenie – 2 nody.

Centrálny logovací systém by mal umožňovať export dát vo formáte vhodnom pre ďalšie strojové spracovanie bez dodatočných obmedzení na časové obdobie, množstvo, alebo obsah exportovaných dát.

Centrálny logovací systém musí podporovať zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém a taktiež musí podporovať zálohovanie dát na externý systém, požadované je plánované aj ad-hoc zálohovanie.

**Alerty:**

Centrálny logovací systém musí byť schopný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert.

Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti.

Centrálny logovací systém by mal obsahovať výrobcom predpripravené sety/vzory alertov a korelácií. Užívateľská konfigurácia alertov musí byť možná pomocou vizuálneho programovacieho jazyka v centrálnej správovskej konzole. Vizuálny programovací jazyk nemôže byť prezentovaný čisto textovo,

	<p>ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie umožňuje okamžitú kontrolu.</p> <p>Ako výstupné pravidlo alertu systém musí vedieť odoslať udalosť, ktorá alert vyvolala na externý systém prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol musí byť možnosť definície formátu dát pre jednoduchšiu integráciu so systémami tretích strán.</p> <p>V alertoch by mala byť možnosť využívať značky. Systém musí podporovať funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel má mať možnosť vloženia testovacej správy a výsledku testu vykonanej akcie.</p>
<p><b>Zber udalostí v prostredí Microsoft:</b></p>	<p>Centrálny logovací systém by mal získavať udalosti z Microsoft prostredia buď pomocou agenta inštalovaného priamo na koncovom zariadení s Windows systémom, alebo iným spôsobom. Agent súčasne musí podporovať monitoring interných Windows logov, a aj monitoring textových súborových logov.</p> <p>Agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovanie auditných informácií.</p> <p>Agent musí podporovať nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.</p> <p>Filtrácia odosielaných udalostí agentom sa musí konfigurovať pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Nerelevantné logy majú byť filtrované na strane agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk nesmie byť prezentovaný textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku.</p> <p>Agent nesmie vyžaduje administrátorské zásahy na koncovom systéme – je centrálné spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizácia agenta sa nevykonáva z Group Policy.</p> <p>Komunikácia Windows agenta a centrálneho logovacieho systému je šifrovaná.</p> <p>Agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale aj zber všetkých ostatných logov v zložke protokoly aplikácií a služieb. Agent musí podporovať centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu.</p> <p>Agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v prehliadači udalostí (Event Viewer) na koncovom systéme.</p> <p>Počet inštalácií agenta nemôže byť licenčne ani časovo obmedzený.</p>
<p><b>Záruka:</b></p>	<p>Hardvérová 5-ročná servisná podpora na hardware appliance s opravou na mieste inštalácie serveru a s garantovanou odozvou nasledujúci pracovný deň od nahlásenia prípadnej závady.</p>

	<p>Systém musí podporovať vygenerovanie TSR (technického support reportu) pre možnosť diagnostiky bez vzdialeného prístupu.</p> <p>Softvérové 5-ročná podpora modulov systému vrátane aktualizácií systému a parserov. Podpora musí obsahovať aktualizáciu SW minimálne 3 x ročne, opravy chýb, telefonickú a emailovú podporu s diagnostikou vzdialeným prístupom.</p>
--	---

## LICENCIA, SUPPORT

<b>Podpora a typ licencie:</b>	5 rokov (60 mesiacov) – hardvér aj softvér
--------------------------------	--

## ZKB

<p>Centrálny logovací systém pomáha všetkým povinným subjektom predovšetkým s dodržiavaním povinností vyplývajúcich z nasledujúcich požiadaviek ZKB:</p> <ul style="list-style-type: none"> <li>• Prijímať organizačné a bezpečnostné opatrenia na riadenie rizík;</li> <li>• Prijímať opatrenia na predchádzanie incidentom narušajúcim bezpečnosť;</li> <li>• viesť bezpečnostnú dokumentáciu;</li> <li>• Hlásiť kybernetické bezpečnostné incidenty;</li> <li>• Poskytovať úradu súčinnosť na posúdenie bezpečnosti;</li> <li>• Zabezpečovať dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní;</li> <li>• Umožňovať a podporovať požiadavky ZKB § 19 Povinnosti prevádzkovateľa základnej služby;</li> <li>• Riadiť bezpečnosť sietí a informačných systémov, prevádzky, prístupov, monitorovania a bezpečnostných auditov;</li> <li>• Sledovať kybernetické bezpečnostné udalosti a zaisťuje ochranu prístupu k vzniknutým záznamom;</li> <li>• Podporovať prevedenie jednorazového aj periodického auditu dodržiavania bezpečnostných politík;</li> <li>• Poskytovať platformu pre rolu audítora kybernetickej bezpečnosti;</li> <li>• Podporovať požiadavky VKB § 10 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. f) zákona;</li> <li>• Predchádzať a riešiť kybernetický bezpečnostný incident;</li> <li>• Dosahovať súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti;</li> <li>• Detekovať a vyhodnocovať bezpečnostné udalosti a incidenty, zlepšovať možnosti koordinácie pri riešení IT incidentov všeobecne a podporovať požiadavky ZKB § 24 Hlásenie kybernetických bezpečnostných incidentov prevádzkovateľom základnej služby;</li> <li>• Preverovať účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti a dopomáhať k súladu požadovaných opatrení tvorbou vhodných reportov a auditov. Umožňovať tak podporovať požiadavky ZKB § 29 Audit;</li> <li>• LOGmanager je nástrojom na centrálny zber a analýzu činností všetkých systémov generujúcich strojové dáta. Umožňuje tak naplniť požiadavky VKB § 15 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. k) zákona.</li> </ul>
---

Na vyššie uvedené povinnosti musí centrálny logovací systém poskytovať mechanizmy protokolovania, upozorňovania a zaisťovať schopnosť spätne dohľadať aktivity systémov aj užívateľov a vykonávať ich priebežný aj nárazový audit. To je kriticky dôležité pre prevenciu, odhaľovanie alebo minimalizáciu vplyvov narušenia (kompromitácie) dát aj systémov. Systém v rámci jednoduchého zobrazenia musí poskytovať prístup ku všetkým strojovým dátam, je možné v prípade, že sa zistí problém, robiť podrobné sledovanie, aktivovať výstrahy a zaisťiť detailnú analýzu. V skratke ide o aplikáciu na zhromažďovanie, ukladanie a analýzu protokolov udalostí, ktorá umožňuje nákladovo efektívnu automatizáciu bezpečnostných opatrení a proaktívnu ochranu informačných systémov a elektronických sietí.

Centrálny logovací systém musí spĺňať bez výhrad požiadavky normy STN EN ISO/IEC 27001:2013 na vytváranie auditných záznamov. Požadujeme tiež potvrdenie normy od autorizovaného audítora výrobcu daného riešenia ktoré bude predmetom ponuky.

## IMPLEMENTÁCIA, TESTOVANIE, NASADENIE

<p><b>Služby:</b></p>	<p>Služby spojené s implementáciou a konfiguráciou systému</p> <p>v rozsahu <b>10 človekodní:</b></p> <ul style="list-style-type: none"> <li>• Zber požiadaviek, nastavenie a konfigurácia systému v IT prostredí obstarávateľa;</li> <li>• Konfigurácia Windows systémov pre zasielanie logov do systému;</li> <li>• Overenie funkčných a výkonových parametrov Windows agentov;</li> <li>• Predvedenie vytvorenia a uloženia vlastného dashboardu a reportu;</li> <li>• Predvedenie nastavenia značkovania udalostí a vytvárania upozornení s limitom alebo koreláciou;</li> <li>• Nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom;</li> <li>• Zaškolenie obsluhy a správy systému pre roly administrátor, supervízor, operátor.</li> </ul>
<p><b>Kľúčový expert</b></p>	<p><b>Špecialista pre infraštruktúry/HW špecialista</b></p> <p>Rozsah: 10 človekodní</p> <ul style="list-style-type: none"> <li>• minimálne 3-ročná preukázateľná odborná prax v oblasti riadenia procesov IT služieb;</li> <li>• minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti implementácie, správy a prevádzky ponúkaného riešenia;</li> <li>• platný certifikát alebo ekvivalent daného certifikátu vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</li> </ul>

<p><b>Služby</b></p>	<p>Služby spojené s implementáciou, nasadením a testovaním v rozsahu <b>2 človekodní</b> pozostávajúce z:</p> <ul style="list-style-type: none"> <li>• prepojenie databáz centrálného logovacieho systému s databázou existujúceho informačného systému verejného obstarávateľa</li> <li>• Konfigurácia</li> </ul>
----------------------	--



	<ul style="list-style-type: none"> <li>• Testovanie;</li> <li>• Zaškolenie</li> </ul>
<b>Kľúčový expert</b>	<b>Špecialista databázy – (2 ČD)</b> <ul style="list-style-type: none"> <li>• minimálne 3-ročná preukázateľná odborná prax v oblasti databázových technológií a systémov;</li> <li>• minimálne dve (2) profesionálne praktické skúsenosti s implementáciou a správou databázovej infraštruktúry a implementácie, správy a prevádzky ponúkaného riešenia</li> <li>• platný certifikát alebo ekvivalent daného certifikátu vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou</li> </ul>
<b>Požiadavky na plnenie:</b>	<ul style="list-style-type: none"> <li>• Dodanie HW na miesto plnenia v lehote do 6 mesiacov, služieb do 12 mesiacov.</li> <li>• Predmet dodania musí byť nový, doposiaľ nepoužitý, zabalený v originálnom balení bez známok poškodenia tovaru a obalu.</li> </ul>

## 2. Firewall Next Generation (Palo Alto Networks) zapojenie redundantne (+ 5 ročný premium support)

**Predmetom zákazky je obstaranie** firewall -hardwaru podpory zariadenia brány firewall novej generácie. V infraštruktúre Mesta Šaľa je vybudovaná segmentácia siete, ktorú zabezpečuje zariadenie Palo Alto Networks firewall. Je to jediné IPS na trhu, ktoré je schopné zastaviť neznámu C2 komunikáciu v reálnom čase. Segmentáciou siete Mesta Šaľa sa rozumie logické oddelenie serverovej siete, klientskej siete a sietí vzdialených lokalít pomocou definovaných pravidiel. Tieto pravidlá obsahujú okrem zdrojových a cieľových IP adries a portov aj definície aplikácií a užívateľských skupín z Active Directory. Všetky pravidlá sú tzv. „application based“. Okrem toho všetky pravidlá kontrolujú komunikáciu pomocou antivírovej, antispymware, DNS-security, IPS a sandbox kontroly. Antivírová kontrola používa okrem AV definícií aj machine learning, ktorý je priamo na FW mesta Šaľa. Tým sa zabezpečuje vysoká efektívnosť pri odchytení tzv. „zero-day“ útokoch. FW je schopný takisto detekovať zneužívanie užívateľských účtov, ktoré je efektívne pri phishing kampaniach. Pri komunikácii s externými sieťami v internete sú okrem iných kontrolované a blokované aj URL kategórie. Kategorizácia URL liniek sa uskutočňuje v reálnom čase. Firewall je teda schopný v reálnom čase detekovať škodlivé URL linky, malware, DNS požiadavky a sieťovej komunikácie bez závislosti od pravidelne sťahovaných signatúr. Z hľadiska infraštruktúry, technického nastavenia, konfigurácie, vypracovanej bezpečnostnej dokumentácie, prevádzky/obsluhy správcu siete a celkového súladu s požiadavkami zákona 95/2018 Z. z. o informačných technológiách vo verejnej správe a zákona 69/2018 o kybernetickej bezpečnosti nie je možné použiť inú alternatívu firewallu.

### ŠPECIFIKÁCIA HARDWARU

<b>Počet:</b>	2 ks
<b>Model, typ:</b>	Palo Alto Networks PA-440

<p><b>Základná špecifikácia:</b></p>	<p>Bezpečnostné zariadenie typu firewall (ďalej tiež len FW) ako celok zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií a pod. Zároveň je týmto jedným výrobcom zaistená podpora minimálne po dobu plánovanej životnosti FW.</p>
<p><b>HW architektúra:</b></p>	<p>Všetky parametre priepustnosti musia byť v real world mix paketoch, tzv. "Application mix".</p> <p>FW je typu HW appliance.</p> <p>Modul pre spracovanie dát je v architektúre firewallu hardwarovo oddelený od ďalších podporných modulov (správa zariadenia a riadiaci modul pre podporné sieťové činnosti), aby nemohlo dôjsť k ich vzájomnému ovplyvneniu.</p> <p>FW musí obsahovať jeden dedikovaný port pre správu pomocou konzoly pre prístup k CLI.</p> <p>FW musí obsahovať 8x dátové rozhrania s rýchlosťou 10/100/1000 RJ45.</p> <p>FW musí obsahovať jeden dedikovaný OOB management port pre plnohodnotnú správu FW.</p> <p>FW musí byť schopný ukladať "logovať" údaje na interný SSD disk s veľkosťou minimálne 128 GB.</p> <p>FW musí podporovať agregáciu portov pomocou protokolu 802.3ad (LACP).</p> <p>FW musí byť rozmerovo kompatibilný s 19 "rozdávčačom.</p> <p>FW musí podporovať dva nezávislé redundantné zdroje napájania AC 230V.</p>
<p><b>High Availability (HA):</b></p>	<p>FW musí podporovať režim HA v móde Active-Active zložený aspoň z dvoch zariadení.</p> <p>FW musí podporovať režim HA v móde Active-Standby zložený aspoň z dvoch zariadení.</p> <p>V oboch typoch HA sú všetky informácie o prebiehajúcej prevádzke synchronizované tak, aby pri výpadku jedného z boxov nedošlo k strate informácií NAT a k prerušeniu aktívnych spojení prevádzky typu TCP aj UDP prechádzajúceho cez FW.</p> <p>FW musí byť schopný vykonať HA failover na základe stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti špecifikovanej IP adresy.</p>
<p><b>Všeobecné výkonové parametre:</b></p>	<p>„Priepustnosť firewallu pri plnej aplikačnej kontrole dosahuje hodnoty aspoň 1,7 Gb/s (app mix)“.</p> <p>Priepustnosť firewallu pri plnej aplikačnej kontrole a zapnutí všetkých dostupných signatúr IPS a AV dosahuje hodnoty 1,0 Gb / s (app mix)</p> <p>Min. počet súbežných spojení je 200 000.</p> <p>Min. počet nových spojení za sekundu je 37 000.</p>

<p><b>Sieťová funkcionálnosť:</b></p>	<p>FW musí plne podporovať IPv4 aj IPv6.</p> <p>FW musí podporovať zapojenie v režimoch L2 (s virtuálnym L3 rozhraním), L3, transparent a TAP.</p> <p>FW musí podporovať preklady adresy typu Static NAT, Dynamic NAT, PAT, NAT64.</p> <p>FW musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)</p> <p>PBR a umožňuje nakonfigurovať na základe všetkých dostupných metrických typov interface, zóna, IP adresa, užívateľ.</p>
<p><b>VPN:</b></p>	<p>FW musí podporovať site-to-site VPN pomocou protokolu IPSec. Počet tunelov nie je licenčne obmedzený.</p> <p>FW musí podporovať Remote Access VPN pomocou protokolov IPSec a SSL (TLS, či DTLS).</p> <p>Priepustnosť IPSec je 1.7 Gb / s.</p> <p>Počet súčasne pripojených užívateľov nie je licenčne obmedzený</p> <p>Riešenie musí obsahovať funkcionálnosť kontroly pripájaných zariadení, ktorá je v súlade s preddefinovanými podmienkami. Napr. verzia OS, nainštalovaný antivírusový nástroj pod.</p> <p>FW pre Remote Access VPN poskytuje pripojenie z klientskych operačných systémov Windows, MacOSX, Linux, Android a iOS</p>
<p><b>Manažment:</b></p>	<p>HW appliance má obsahovať plnohodnotné grafické rozhranie (GUI) pre správu a čítanie logových záznamov bez nutnosti používania centrálného management servera. Pripojenie ku GUI musí podporovať šifrovanie.</p> <p>GUI má obsahovať offline kontextovú nápovedu.</p> <p>HW appliance musí obsahovať plnohodnotné textové rozhranie (CLI) pre správu a čítanie logových záznamov bez nutnosti používania centrálného management servera. Vzdialené pripojenie k CLI musí podporovať šifrovanie.</p> <p>HW appliance musí obsahovať plnohodnotné API rozhranie pre čítanie a konfiguráciu všetkých nastavení, týkajúcich sa bezpečnostných a ďalších pravidiel aj rozhrania a smerovanie.</p> <p>HW appliance musí umožňovať použitie šablón pre bootstrapping nových FW použitím USB flash disku.</p> <p>FW pre autentizáciu a autorizáciu administrátorov musí podporovať protokoly LDAP, Radius, TACACS +, Kerberos a osobný certifikát.</p> <p>FW musí obsahovať natívne nástroje pre debugging problémových situácií v úrovni L2 - L7 ISO / OSI modelu.</p> <p>FW musí podporovať natívny nástroj pre odchytenie prevádzky.</p> <p>FW by mal umožňovať správu z administrátorských staníc s OS Windows a MacOS.</p>



	<p>FW musí podporovať získavanie väzby IP adresa-užívateľské meno prostredníctvom načítania informácie z logového záznamu, získaného pomocou zabezpečeného protokolu Syslog.</p> <p>FW musí podporovať získavanie väzby IP adresa-užívateľské meno z terminálových serverov MS (možné za pomoci nainštalovaného agenta).</p> <p>FW musí podporovať kontrolu klientskych staníc v pravidelných intervaloch cez Windows Management Instrumentation (WMI) alebo Win-RM aby zistil, či je väzba IP adresa-užívateľské meno stále platná.</p>
<p><b>Dešifrovanie:</b></p>	<p>FW musí podporovať dešifrovanie odchádzajúcej SSL / TLS prevádzky, za pomoci "podvrhnutého" serverového certifikátu klientom</p> <p>FW podporuje dešifrovanie prichádzajúcej SSL / TLS prevádzky, za pomoci naimportovaného privátneho kľúča interného servera.</p> <p>FW musí podporovať dešifrovanie Secure Shell (SSH proxy) a kontrolovať tunelované aplikácie.</p> <p>Dešifrovanú prevádzku umožňuje definovať na základe URL kategórií, aj všetkých ďalších typických parametrov, ako sú zdrojová a cieľová IP adresa, port, užívateľská identita.</p> <p>FW musí podporovať dešifrovanie pomocou ECC (Elliptical Curve Cryptography), vrátane DHE a ECDHE pre prichádzajúcu a odchádzajúcu prevádzku.</p>
<p><b>Sandboxing:</b></p>	<p>Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznáme vzorky prechádzajúce protokolom HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB.</p> <p>Sandbox systém musí byť schopný okamžite automaticky vytvoriť IPS / AV signatúry pre FW, v prípade, keď je testovaná vzorka vyhodnotená ako škodlivá.</p> <p>Sandbox musí byť schopný automaticky upraviť kategórie používanej URL databázy ak zistí, že testovaná vzorka je škodlivá a komunikuje na konkrétne URL.</p> <p>Sandbox musí poskytovať aktualizácie signatúr pre AV, Webfiltering, DNS, C &amp; C.</p> <p>Sandbox musí podporovať analýzu vzorky na operačnom systéme inštalovanom priamo na hardvéri, tzn. nie vo virtuálnom prostredí</p> <p>Sandbox a podporovať operačné systémy Windows, Linux, MacOS a Android. Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania FW.</p> <p>Aktualizácia zero-day signatúr je inštalovaná do FW v reálnom čase</p> <p>FW je schopný detekovať a zablokovať prevzatie neznámeho škodlivého súboru v reálnom čase, bez toho, aby bol doručený na koncový bod.</p>

<b>Bezpečnostné funkcionality:</b>	<p>FW musí podporovať zavedenie tzv. Pozitívneho bezpečnostného modelu - povolenie iba vybraných aplikácií a zákaz všetkých ostatných aplikácií, vrátane neznámej prevádzky.</p> <p>FW musí obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (IPS). Databáza IPS signatúr je uložená priamo vo FW. Aplikácia IPS profilu je granulárna, na úrovni bezpečnostného pravidla.</p> <p>FW musí podporovať tvorbu užívateľsky definovaných IPS signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa.</p> <p>FW musí obsahovať integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr je uložená priamo vo FW. Aplikácia AV profilu musí byť granulárna, na úrovni bezpečnostného pravidla.</p> <p>Antivirus musí byť schopný kontrolovať prevádzku v minimálne týchto aplikáciách - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP / 2, FTP a SMB.</p> <p>FW musí podporovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu / dodávateľa.</p> <p>FW musí podporovať možnosť zablokovania útoku využívajúceho známe C&amp;C centrá aj v prípade, že je prevádzka šifrovaná a nie je možné vykonávať SSL dekrypciu.</p> <p>FW v bezpečnostných predpisoch podporuje použitie externých dynamických zoznamov; FW poskytuje možnosť overiť na základe certifikátov pravosť týchto dynamických zoznamov.</p> <p>FW by mal podporovať import Snort signatúr.</p> <p>FW pre prístup ku kritickým aplikáciám by mal poskytovať možnosť vynútiť multifaktorové overenie prostredníctvom webového portálu, bez ohľadu na to, či cieľová aplikácia podporuje viacfaktorovú autentizáciu; táto vlastnosť musí byť konfigurovateľná na úrovni bezpečnostného pravidla.</p> <p>FW musí podporovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu.</p> <p>FW musí podporovať funkciu k ochrane proti tzv. Drive-by downloadom; spôsob ochrany musí byť pre používateľa interaktívny s možnosťou voľby akceptácie rizika a stiahnutia súboru.</p> <p>FW musí podporovať analýzu DNS dopytu tzv. Sinkhole funkciou, ktorá na dopyt malware DNS URL vráti podvrhnutú IP adresu pre detailnejšiu analýzu a zároveň sa stanica na pôvodnú malware stránku nedostane.</p> <p>FW musí podporovať funkcionality pokročilej analýzy DNS dopytov proti technikám používajúcim DGA (domain generation algorithm) v reálnom čase.</p>
--	---

	FW musí podporovať možnosť rozšírenia o funkcionality pokročilej analýzy DNS dotazov proti technikám používajúcim DGA (domain generation algorithm) v reálnom čase.
<b>Ochrana proti DoS:</b>	FW musí podporovať natívnu službu pre ochranu proti útoku typu DoS pomocou limitácie počtu spojení na úrovni zdrojovej a cieľovej IP adresy, užívateľská identita a aplikácia.
<b>QoS:</b>	FW musí podporovať možnosť prioritizácie prevádzky a obmedzenie využívanej šírky pásma na základe zdrojovej a cieľovej IP adresy, portu, užívateľskej identity, aplikácie a času (od - do, deň v týždni + čas a pod.). FW musí podporovať prioritizáciu prevádzky na základe DSCP. FW musí podporovať prioritizáciu prevádzky na základe identifikovanej aplikácie.
<b>URL filtering:</b>	FW musí podporovať natívnu podporu pre využívanie databázy URL. URL databázy sú od toho istého výrobcu ako FW. FW je schopný použiť URL kategóriu v definícii bezpečnostného pravidla. FW musí podporovať vytváranie užívateľsky definovaných kategórií, bez nutnosti využiť externý nástroj a bez nutnosti zásahu výrobcu / dodávateľa. URL databáza je dynamicky aktualizovaná na základe novo zistených URL, vedúcich na škodlivý obsah alebo C & C centra URL databáza musí podporovať možnosť zaradenia do aspoň dvoch kategórií naraz pre jedinú URL. FW musí podporovať požiadať o rekatégorizáciu nevhodne zaradených URL priamo v grafickom rozhraní FW bez nutnosti kontaktovania technickej podpory. Aktualizácia URL databázy je v reálnom čase (real-time) za pomoci využitia machine learning
<b>Logovanie:</b>	FW musí disponovať lokálnym úložiskom logov. FW musí obsahovať nástroj na analýzu logov bez nutnosti využitia ďalšieho systému mimo GUI. FW musí podporovať agregované zobrazenie logov na základe jedného filtrovacieho pravidla, naprieč jednotlivými typmi logov, ako sú prevádzkové logy, logy bezpečnostných incidentov a logy prístupov na URL. FW musí podporovať preposielanie logov na zariadenia tretích strán. FW musí podporovať výber preposielaných logov na úrovni bezpečnostného pravidla.

	<p>Preposielané logy z FW sú automaticky rozpoznané najčastejšie používanými typmi SIEM (uvedených v Leaders kvadrante aktuálneho Gartner MQ).</p> <p>FW musí podporovať vytváranie vlastných reportov priamo z grafického rozhrania FW.</p>
<b>Záruka</b>	<p>5 rokov priamo od výrobcu zariadenia, odozva najneskôr do 4h od nahlásenia, vrátane víkendov a sviatkov. Servis bude poskytovaný v mieste inštalácie. Nahlasovanie poruchy v režime 24x7. Nahlasovanie porúch priamo u výrobcu zariadenia.</p>

#### LICENCIA, SUPPORT

<b>Licencia, typ:</b>	<p>Partner enabled premium support</p> <p>PA-440, Professional Subscription Bundle (Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security), 5 years (60 months) term</p> <p>PA-440, GlobalProtect subscription, for one (1) device in an HA pair, 5 years (60 months), term.</p>
<b>Podpora:</b>	<p>5 rokov (60 mesiacov)</p>

#### IMPLEMENTÁCIA, TESTOVANIE, NASADENIE

<b>Služby:</b>	<p>Služby spojené so zmenou NGFW riešenia v rozsahu <b>9 človekodní</b> pozostávajúce z:</p> <ul style="list-style-type: none"> <li>• Fyzické osadenie HW a upgrade firmvérov;</li> <li>• Konfigurácia vysokej dostupnosti (High Availability – HA);</li> <li>• Migrácia pravidiel z aktuálneho riešenia a ich revízia;</li> <li>• Konfigurácia IPS a app control;</li> <li>• Testovanie;</li> <li>• Zaškolenie v prípade nových funkcií.</li> </ul>
<b>Kľúčový expert:</b>	<p><b>Rozsah implementácie:</b> 7 človekodní</p> <p><b>IT Tester (4 ČD)</b></p> <ul style="list-style-type: none"> <li>• minimálne 3-ročná preukázateľná odborná prax v oblasti testovania softvérových riešení;</li> <li>• minimálne dve (2) profesionálne praktické skúsenosti s testovaním ponúkaného softvérového riešenia;</li> <li>• platný certifikát alebo ekvivalent daného certifikátu vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</li> </ul> <p><b>Špecialista pre bezpečnosť informačných systémov (3 ČD)</b></p> <ul style="list-style-type: none"> <li>• minimálne 3-ročná odborná prax v oblasti informačnej bezpečnosti, konkrétne v oblasti sieťovej bezpečnosti;</li> <li>• minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti implementácie a podpory ponúkaných nástrojov na zabezpečenie sieťovej bezpečnosti;</li> </ul>



	<ul style="list-style-type: none"> <li>• platný certifikát alebo ekvivalent daného certifikátu vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</li> </ul>
--	--

<b>Požiadavky na plnenie:</b>	<ul style="list-style-type: none"> <li>• Dodanie HW na miesto plnenia v lehote do 6 mesiacov, služby do 12 mesiacov</li> <li>• Predmet dodania musí byť nový, doposiaľ nepoužitý, zabalený v originálnom balení bez známok poškodenia tovaru a obalu.</li> </ul>
-------------------------------	--

### 3. Security riešenie na koncových zariadeniach (+ 5 ročný support)

**Predmetom zákazky je obstaranie** podpory licencie antivírusového softvéru, ktoré slúžia na zabezpečenie kompletnej ochrany koncových zariadení (pracovných staníc, notebookov, serverov, mobilných zariadení, virtuálnych servery a počítačov, hypervizorov) proti vírusom, spyware, ransomware, exploit blockerom a sandboxom, UEFI skenerom v jednom balíku. EDR bude slúžiť na ochranu koncových staníc pred škodlivým kódom a prienikom útočníka. Všetky technické parametre/funkcionality, resp. vlastnosti požadovaného predmetu zákazky predstavujú minimálne požiadavky, ktoré musia byť splnené v ponuke uchádzača. V prípade, že by sa záujemca/uchádzač cítil dotknutý vo svojich právach, t. j., že by týmto opisom dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov/uchádzačov alebo výrobcov, alebo že tento predmet zákazky nie je opísaný dostatočne presne a zrozumiteľne, tak vo svojej ponuke môže uchádzač použiť technické riešenie ekvivalentné, ktoré spĺňa kvalitatívne, technické, funkčné požiadavky na rovnakej a vyššej úrovni, ako je uvedené v tejto časti výzvy, túto skutočnosť však musí preukázať uchádzač vo svojej ponuke.

## ŠPECIFIKÁCIA

<b>Počet</b>	110 ks
<b>Základná špecifikácie:</b>	<p>Riešenie musí detekovať a blokovať škodlivý softvér v reálnom čase, vrátane vírusov, červov, trójskych koní, spyware, Adware a rootkitov.</p> <p>Technológia bezpečnosti koncových bodov musí zahŕňať technológiu založenú na správaní, poskytovanie signatúr pre známe hrozby, prístup založený na detekcii zraniteľnosti a heuristike.</p> <p>Riešenie musí byť schopné zaznamenať dobré aj zlé správanie neznámych aplikácií, zlepšiť detekciu a znížiť falošné poplachy bez toho, aby bolo nutné vytvárať konfigurácie založené na pravidlách, ktoré poskytujú ochranu pred neviditeľnými hrozbami, t. j. HZero-Day Threats.</p> <p>Súčasťou riešenia má byť aj firewall, ktorého engine má možnosť povoliť alebo blokovať podporu sieťových protokolov, vrátane Ethernetu, Token Ring, IPX/SPX, AppleTalk a NetBEUI. Môže blokovať ovládače protokolu (napríklad: VMware, WinPcap) a má osobitné pravidlá pre adaptér - napr. Ethernet, Wireless, VPN.</p>

Riešenie má podporovať Android, Apple IOS, Windows na zariadeniach ARM, Windows v režime S, Windows 7 32/64b, Windows 8 32/64b, Windows 8.1 32/64b, Windows 10 32/64b, Windows Server 2019 a staršie min. do verzie 2008R2, MacOS 10.15 a staršie min. do verzie 10.10, distribúcie linuxu Amazon Linux, CentOS, Debian, Fedora, Oracle, red Ha, SUSE a Ubuntu.

Požadujeme podporu týchto virtuálnych prostredí:

Microsoft Azure, Amazon AWS, VMware ESXi 5.5 a novší, MS Windows Server (Hyper-V) 2008R2 a novší, Citrix XenServer 5.6 a novší, Oracle Virtual Box.

Riešenie IPS v prípade potreby musí umožňovať úpravy a vytvorenie podpisu IPS pomocou formátu Snort.

Riešenie musí vedieť blokovať zariadenia na základe ID triedy Windows a má zahŕňať USB, infračervené rozhranie, Bluetooth, sériové, paralelné, Firewire, SCSI a PCMCIA. Súčasne umožňovať definíciu vlastných špecifických zariadení.

Riešenie musí byť schopné blokovať a udeliť povolenie na čítanie /zápis/ spustenie pre uvedené zariadenia.

Riešenie musí poskytovať analýzu aplikácií, riadenie procesov, riadenie prístupu k súborom a registrom a riadenie modulov a DLL.

Riešenie IPS má mať možnosť kombinácie NIPS (sieť) a HIPS (hostiteľ) s generickým blokovaním zneužitia, aby sa proaktívne chránilo proti všetkým variantom, granulárnu kontrolu prístupu aplikácií a vyššie uvedené technológiu založenú na správaní.

Riešenie Anti Spyware musí byť schopné obísť súborový systém Windows a vie mať priamy prístup ku zväzku NTFS, aby poskytovalo prvotnú kontrolu disku pre vyššiu ochranu proti rootkitom.

System Lock Down - je schopné "uzamknúť" systém odtlačkom (hash) všetkých spustiteľných súborov v systéme. Potom môže sledovať všetky spustené aplikácie a terminovať všetky aplikácie, pre ktoré agent nemá zodpovedajúci hash.

Riešenie musí chrániť systém pred niekoľkými formami neobvyklého správania siete, ktoré je navrhnuté tak, aby narušilo dostupnosť a / alebo stabilitu systému.

Riešenie musí chrániť prenos dát pred odoslaním hackerskému systému, ktorý spoofoval ich IP alebo MAC adresu.

Agent má mať schopnosť detekovať a blokovať reťazce implementácie procesov. Má byť schopný zistiť, kedy sa škodlivá aplikácia pokúsi zaviesť dôveryhodnú aplikáciu a potom použiť oprávnenia dôveryhodnosti tejto aplikácie pre prístup k sieti.

Riešenie musí zabraňovať škodlivým aplikáciám vo vkladaní kódu do dôveryhodnej aplikácie, aby obišli výstupný firewall aplikácií.

Zabraňovať škodlivým aplikáciám v používaní ich vlastného sieťového adaptéra k obchádzaniu výstupného firewallu.

Antivírusové a antispýwarové politiky riešenia v predvolenom nastavení majú mať možnosť zvoliť Vysoká bezpečnosť a Vysoký výkon, aby bola zaistená správna rovnováha pri nasadení v produkčnej sieti.

Antivírus riešenia má mať technológiu založenú na správaní, ktorá by skenovala trójske kone, červy a zaznamenávanie stlačení klávesnice, aby bola chránená pred hrozbami nulového dňa.

Navrhované riešenie má možnosť skenovať prílohy e-mailových pluginov, vrátane súborov.zip, odstraňovať malware skôr, než sa dostane do doručenej pošty, a je schopné skenovať e-mailovú prevádzku POP3 vrátane e-mailových klientov Microsoft Outlook a Outlook Express.

Pravidlá lokálnej brány firewall majú byť konfigurovateľné v závislosti na adaptéroch, vrátane ethernetu, bezdrôtovej siete, telefonického pripojenia, VPN (Microsoft PPTP, Nortel, Cisco).

Riešenie musí mať pripravené politiky vrátane: všetky vymeniteľné jednotky len na čítanie, blokovať spustenie programu z vymeniteľných jednotiek, chrániť súbory klientov a kľúče Registry, zaprotokolovať súbory zapísané na disky USB, blokovať úpravy hostiteľských súborov

Server pre správu má mať schopnosť pridávať viac domén a je možné priradovať rôznych administrátorov iným umiestneniam. Každá doména zdieľa rovnaký server pre správu a databázu. Toto oddelenie bráni správcovi v jednej doméne v prezeraní dát v iných doménach. Títo správcovia môžu zobraziť a spravovať obsah svojej vlastnej domény, ale nemôžu zobraziť a spravovať obsah iných domén.

Z dôvodu zachovania šírky pásma siete je umožnené konfigurovať klientov pre upload maximálnych záznamov protokolov na server pre správu.

Riešenie má umožňovať nastavenie zabezpečenia, ktoré blokuje všetku prevádzku, kým sa nespustí brána firewall a potom, čo sa brána firewall zastaví, okrem počiatočného prenosu DHCP a NetBIOS.

Riešenie AV má mať schopnosť detekovať súbory podľa počtu užívateľov, ktorí tento súbor používajú po celom svete.

Prevenencia vniknutia do prehliadača (Browser intrusion prevention): AV musí byť schopná blokovať sťahovanie škodlivého obsahu pomocou web prehliadačov.

Riešenie AV musí súbory radiť na základe digitálneho podpisu, veku súboru a atribútov prevalencie

AV klient má mať viditeľnú indikáciu, kedykoľvek sa pripojí k AV konzole.

AV konzola musí vedieť zobrazovať hodnotu, ktorá indikuje stav vírusov vo verejnej sieti.

	<p>Riešenie má mať funkciu Deception ako súčasť Endpoint Agentu.</p> <p>Riešenie musí mať ochranu zneužitia pamäti ako súčasť rovnakého agenta.</p> <p>Riešenie má mať funkciu EDR s použitím rovnakého agenta.</p> <p>Riešenie má mať funkciu Host Integrity, identifikovať a napraviť nevyhovujúce koncové body.</p> <p>Riešenie má mať efektívne strojové učenie v analýze súborov a behaviorálnej analýze.</p> <p>Riešenie má mať hostiteľský IPS, ktorý dokáže blokovať a detekovať interné alebo odchádzajúce sieťové útoky a komunikáciu a hrozby na úrovni prehliadača a siete, než sa dostanú na disk a sú spustené.</p> <p>Agent koncového bodu je chránený pred manipuláciou alebo deaktiváciou.</p> <p>Riešenie má mať voliteľnú konzolu pre správu v cloude.</p>
<p><b>Detekcia a reakcia na koncovom bode (Endpoint Detection and Response):</b></p>	<p>Riešenie bude schopné zistiť, vyhľadávať, izolovať a eliminovať prieniky do systému na zariadeniach pomocou AI analytiky, investigačných postupov a threat intelligence. Všetko má byť integrované do jednotného klienta.</p> <p>Musí plniť nasledujúce funkcie:</p> <p>Detekovať a napraviť - skrátenie času na zistenie narušenia a rýchle odhalenie rozsahu nákazy.</p> <p>Aplikovať strojové učenie a analýzu správania k odhaleniu podozrivej aktivity, detekovať a uprednostniť vážne incidenty.</p> <p>Automaticky identifikovať a vytvárať incidenty pre podozrivé skripty a zneužitia pamäte.</p> <p>Odhaľovať pamäťové útoky s analýzou procesnej pamäte.</p> <p>Zvýšenie produktivity osôb reagujúcich na incidenty a zaistenie obmedzenia hrozieb:</p> <p>Zabezpečiť úplné prehrávanie incidentov s nepretržitým záznamom aktivity koncových bodov, zobrazíť konkrétne procesy koncových bodov.</p> <p>Vyhľadávanie hrozieb pomocou indikátorov kompromitácie naprieč všetkými koncovými bodmi v reálnom čase.</p> <p>Izolovanie potencióálne ohrozených koncových bodov počas vyšetrovania pomocou karantény koncových bodov.</p> <p>Odstraňovať škodlivé súbory a súvisiace artefakty na všetkých ovplyvnených koncových bodoch.</p> <p>Blacklisting a súbory na zozname povolených v koncovom bode.</p>

Reporting, ktorý umožňuje exportovať správy o riešení incidento. Replikovať osvedčené postupy a analýzy kvalifikovaných vyšetrovateľov pomocou playbooks.

Podrobný prehľad o aktivite pomocou automatizovaného zberu informácií..

Ako súčasť platformy požadujeme riešenie koncového bodu, ktoré umožňuje detekciu, overenie a karanténu. Všetky funkcie musia fungovať v podnikovej sieti alebo mimo nej a bez požiadavky na VPN do podnikovej siete.

Riešenie musí byť schopné podporovať viac detekčných a ochranných technológií v rámci ich riešenia a malo by obsahovať základný signatúrny engine, ktorý využíva databázu známych súborov a ich správanie na určenie, či je súbor nebezpečný, bez ďalšej záťaže pri overení súboru k detekcii zraniteľností nultého dňa a hrozieb.

Riešenie má mať dvojstupňový proces karantény a sanácie.

Riešenie musí byť schopné aktualizovať nové verzie agenta na koncovom bode.

Riešenie musí byť schopné sa dozvedieť o hrozbách nultého dňa z iných bezpečnostných zariadení rovnakého výrobcu vykonávajúcich detonáciu vzorky.

Riešenie koncových bodov je schopné prijímať vstupy indikátorov kompromitácie.

Agent koncového bodu má mať schopnosť chrániť pred hrozbami, ako sú adware, vírusy a softvérové chyby zabezpečenia, ktoré na koncovom riešení existujú.

Riešenie musí mať schopnosť plne forenzne analyzovať identifikovaný malware a poskytnúť zodpovedným zamestnancom nasledovné informácie:

Súhrnnú správu o zmenách vykonaných na hostiteľovi; Poskytnúť kópiu binárneho kódu škodlivého softvéru;

Celú cestu URL identifikujúcu všetky umiestnenia, na ktoré sa malware pokúša komunikovať;

Súhrnné správy o udalostiach podnikového malwaru rozdeľujúce malware podľa typu, hostiteľa a aktivity;

Okamžitú analýzu toho, či sa malware mapuje na predtým známu alebo neznámu hrozbu;

Informácie o závažnosti ilustrujúce ako efektívne by boli ostatné ochranné mechanizmy proti tejto hrozbe.

Riešenie musí dynamicky generovať požadované pravidlá/zásady blokovania/blacklist škodlivého súboru na všetkých klientoch koncových bodov bez nutnosti nasadenia / integrácia s ďalšími agentmi.

Riešenie má byť schopné automaticky vložiť do karantény podozrivé súbory.

Riešenie má byť schopné odovzdať indikátory kompromitácie (IOC), ako je hash súboru riešeni koncového bodu, aby riešenie koncového bodu mohlo blokovať súčasnú aj budúcu detekciu podobných súborov.

Riešenie musí byť schopné detekovať rootkity na úrovni jadra, identifikovať metódy DLL injection, identifikovať naprieč koncovými bodmi, ak má škodlivý súbor rôzne názvy.

Riešenie musí poskytovať jediný pohľad na podozrivé alebo škodlivé súbory naprieč koncovými bodmi.

Riešenie musí poskytovať reputáciu súborov na základe informácií Intelligence zhromaždených po celom svete, aby pomohli procesom vyšetrovania a nápravy.

Riešenie musí poskytovať správcovi možnosť odosielať súbory pre dynamickú analýzu malwaru.

Riešenie musí poskytovať možnosť pridávať na zoznam povolených alebo zakázať súbory naprieč koncovými bodmi.

Agent koncového bodu podporuje vyhľadávanie reputácie súboru na serveroch riešenia, podporuje blokovanie, mazanie a karanténu hrozieb, neovplyvňuje výkon AV agenta, poskytuje schopnosti IPS na hostiteľovi, aby sa chránil pred sieťovými hrozbami zameranými na koncové body, poskytuje koncovým bodom funkcie prevencie narušenia pomocou webovej prevádzky.

Riešenie koncového bodu musí podporovať vyhľadávanie IOC zo všetkých koncových bodov. Súbory, kľúče Registry aj domény a adresy URL.

Riešenie koncového bodu majú mať možnosť Blacklisting a vymazať škodlivé súbory z jedného riadiaceho bodu.

Riešenie má byť schopné umiestniť koncové body do karantény z centrálnej konzoly, aby sa zabránilo ďalšej infekcii.

Riešenie koncového bodu má korelovať informácie o hrozbe a malware s existujúcim riešením proti malwaru a uprednostniť alebo zrušiť prioritu incidentov na základe stavu ochrany pomocou riešenia proti malwaru.

Riešenie má podporovať aktuálnu ochranu koncového bodu ako súčasť platformy, ktorá umožňuje detekciu, overenie, obmedzenie a nápravu koncového bodu.

Riešenie koncového bodu musí byť schopné napraviť koncový bod pomocou existujúcej ochrany koncového bodu alebo vlastných nástrojov.

Riešenie koncového bodu má byť schopné detekovať neznámy škodlivý malware a malo by byť schopné odoslať malware na detekciu z koncových bodov, nezávisle na riešení sieťového riešenia.

Riešenie koncového bodu má byť schopné detekovať, overovať a napraviť koncové body, keď je používateľ v podnikovej sieti aj mimo nej a bez požiadavky na VPN.

	<p>Riešenie má podporovať prístupy na základe definovaných rolí.</p> <p>Riešenie pre koncový bod má byť schopné dynamicky prijímať informácie o IOC a hrozbách zo zariadení vykonávajúcich analýzu virtuálneho spustenia v sieti (napr. riešenie nech je založené na integrácii s e-mailom).</p> <p>Riešenie má mať možnosť vyhľadávania IOC a Threat Hunting dopytov priamo na klientovi.</p> <p>Riešenie koncového bodu má byť schopné detekovať prítomnosť súborov, ktoré boli uložené do systému, ale neboli spustené.</p> <p>Riešenie koncového bodu nemá zasahovať do bežných operácií na koncovom bode bez ohľadu na to, ako je systém zaneprázdnený.</p> <p>Riešenie pre koncový bod má poskytovať pravidelné aktualizácie informácií o hrozbách, aby zahŕňali ukazovatele zahŕňajúce vysoko pokročilé skupiny hrozieb v sponzorovaných cieľených útokoch.</p> <p>Upgrady riešenia koncového bodu sú podporované štandardnými mechanizmami nasadenia podnikového softvéru (napr. SCCM, Altiris).</p> <p>Riešenie má umožňovať odoslanie podozrivej vzorky na analýzu kliknutím na tlačidlo z konzoly, aby sa zabránilo potenciálne falošne pozitívnemu varovaniu.</p> <p>Riešenie má podporovať izolovanú exekúciu vzorky v cloude vo virtuálnom aj fyzickom prostredí v rámci zakúpenej licencie.</p> <p>Požadované riešenie má podporovať zapisovanie dát do systému "za letu".</p>
<p><b>Riadenie a kontrola aplikácií:</b></p>	<p>Riešenie má zahŕňať komplexné zisťovanie a inventár aplikácií na skenovanie a inventarizáciu všetkých aplikácií a súborov zhromaždených zo všetkých koncových bodov v prostredí a poskytuje podrobné informácie o každej aplikácii a súbore, vrátane názvu, skóre rizika, skóre zraniteľnosti, vydavateľa, reputácie, počet zariadení, na ktorých je prítomná atď.</p> <p>Riešenie má obsahovať komplexné zásady riadenia aplikácií a jednoduché vytváranie zásad pomocou logického zobrazenia, ktoré pridá akúkoľvek aplikáciu z objavených aplikácií na bielu alebo čiernu listinu.</p> <p>Aplikačná kontrola musí umožňovať dôverovať aplikácii na základe rôznych atribútov aplikácie, povolenie alebo blokovanie aplikácií na základe jednej alebo kombinácie ľubovoľného počtu statických (napr. hash, cesta, vydavateľ a certifikát) a dynamických (napr. riziko a skóre reputácie) atribútov.</p> <p>Zásady musia umožňovať vytváranie pravidiel pre širokú škálu parametrov, ktoré zahŕňajú názov aplikácie, cestu a hash, reputáciu, vydavateľa, používateľa, skupinu užívateľov a parametre príkazového riadku.</p> <p>Zásady majú mať možnosť vynútenia režimu "len monitorovať".</p> <p>Riešenie musí dokázať analyzovať rozdiel medzi tým, aké aplikácie sú povolené v prostredí a aké aplikácie v prostredí bežia.</p>

	<p>Riešenie by malo umožňovať definovať dôveryhodné aplikácie, ktoré pochádzajú z dôveryhodného zdroja, vydavateľa, adresára, súborov, používateľov a skupín užívateľov, ktoré môžu inštalovať alebo aktualizovať softvér v koncových bodoch.</p> <p>Riešenie musí vedieť zabrániť zneužitiu dôveryhodných aplikácií a zabrániť nedôveryhodným aplikáciám v infikovaní systémov.</p>
<p><b>Aplikačná izolácia:</b></p>	<p>Riešenie má mať funkcie pravidiel izolácie správania aplikácie k ochrane samotého zariadenia, tieto pravidlá umožňujú alebo blokujú určité správanie aplikácie, ako nasledujúce typy izolácie: izolácia web prehliadača (Google Chrome, Firefox, Internet Explorer, Microsoft Edge); izolácia Office dokumentov; izolácia PDF prehliadača; izolácia neznámych procesov, ktorá zahŕňa ochranu nastavenia OS a všeobecné nastavenie izolačnej úrovne (minimálne 3 úrovne); nastavenie OS; všeobecné nastavenie aplikačného sandboxingu (vysoká, stredná a nízka izolácia)</p> <p>Aplikačná izolácia musí poskytovať pravidlá na ochranu registrov, súborov, interakcie procesov, volanie a púšťanie procesov, prístupu k sieti, systémových volaní.</p> <p>Riešenie má detegovať akékoľvek podozrivé súbory na základe úrovni intenzity a umožniť pridať detegované súbory do zoznamu whitelist alebo na blacklist a umožniť izolovať podozrivú aplikáciu pomocou zásad izolácie.</p> <p>Riešenie musí byť schopné vyhľadávať, inventarizovať a izolovať prenosné aplikácie na základe hodnotenia rizika.</p>
<p><b>Deception:</b></p>	<p>Riešenie má mať funkciu Deception s nasadením širokej škály "pascí" - falošných súborov, poverení, zdieľaných položiek v sieti, záznamov vo vyrovnávacej pamäti.</p> <p>Riešenie má mať funkciu pascí ako súčasť jediného agenta.</p> <p>Riešenie má využívať deception techniky na sledovanie a upozorňovanie na správanie škodlivých aplikácií.</p>
<p><b>Ochrana mobilných zariadení:</b></p>	<p>Riešenie musí byť podporované na zariadenia IOS a Android.</p> <p>Riešenie musí proaktívne chrániť mobilné zariadenia pred malwarom, sieťovými hrozbami a zneužitím zraniteľnosti aplikácií / OS, s pripojením k internetu aj offline.</p> <p>Riešenie má mať schopnosť umožniť rýchlejšiu reakciu a neustálu ochranu, aj keď sú zariadenia odpojené od internetu.</p> <p>Riešenie musí aktívne zmariť útoky, okamžite a automaticky, keď je detekovaná hrozba.</p> <p>Riešenie musí zabezpečiť ochrannú akciu proti rizikovým hrozbám aplikácií, okrem iného blokovanie komunikácie, zabránenie inštalácie, blokovanie komunikácie so škodlivými servermi C&amp;C a blokovanie prístupu k citlivým prostriedkom.</p>



Riešenie musí zabezpečiť ochrannú akciu proti sieťovým hrozbám, okrem iného sieťové automatické spustenie tunela VPN pri zistení sieťovej hrozby, blokovanie prístupu k citlivým podnikovým zdrojom a blokovanie prístupu k falošným podnikovým hotspotom wi-fi.

Riešenie musí zabezpečiť ochrannú akciu proti hrozbám obsahu, okrem iného tunelovanie kompletnej prevádzky prostredníctvom zabezpečenej webovej brány, blokovanie prístupu k nežiaducemu obsahu a blokovanie phishingových správ SMS.

Riešenie musí zabezpečiť ochrannú akciu k automatickému odpojeniu škodlivých sietí VPN.

Riešenie musí obsahovať VPN technológiu pre elimináciu manipulácie prevádzky. Technológia VPN má schopnosť fungovať ako šifrovaný tunel, ktorým bezpečne prechádza prevádzka medzi zariadením a sieťou a ako selektívny blokátor prevádzky (konkrétna prevádzka prechádzajúca sieťou VPN je zrušená a nikdy neopustí zariadenie). Každá z týchto implementácií môže byť na vyžiadanie.

Riešenia má mať viacvrstvovú mobilnú obranu proti známym útokom a útokom nulového dňa naprieč všetkými mobilnými hrozbami.

Riešenia má mať ochranu pred podozrivými sieťami, aplikáciami a správaním.

Riešenie musí chrániť súkromie a produktivitu, bez toho, aby to negatívne ovplyvnilo chod ostatných aplikácií alebo výdrž batérie.

Riešenie má mať automatizované vynucovanie politík IT a integráciu so všetkými významnými súčasnými podnikovými EMM / MDM, SIEM, e-mailovými servermi a VPN.

Riešenie má mať možnosť integrácie s bezpečnostnými riešeniami, okrem iného vrátane ochrany WSS, CASB, DLP a Endpoint.

Riešenie má umožňovať hĺbkovú analýzu podozrivých aplikácií a mať pri tom nulový dopad na produktivitu, výkon a súkromie.

Riešenie má mať odozvu v reálnom čase a ochranu pred rôznymi známymi, neznámymi a cielenými útokmi malwaru z akýchkoľvek podozrivých aplikácií a sietí.

Riešenie má mať automatickú ochranu podnikových aplikácií, keď je napadnuté.

Riešenie má mať schopnosť kontroly reputácie pomocou strojového učenia pre aplikácie, siete a OS.

Riešenie má mať komplexné protokoly aktivít pre integráciu s akýmkoľvek riešením SIEM. Riešenie má schopnosť analýzy aplikácií na základe podpisu, statickej/dynamickej analýzy, správania, štruktúry, oprávnení, zdroja a ďalších.

Riešenie má obsahovať detekciu, blokovanie a nápravu škodlivých profilov iOS.

	<p>Riešenie má mať schopnosť identifikovať útoky typu Man-in-the-Middle, downgrading SSL a manipulácia s obsahom bez narušenia súkromia.</p> <p>Riešenie má mať schopnosť monitorovať zariadenia kvôli nevyriešeným známym zraniteľnostiam a odhaľovať zraniteľnosti nulového dňa v aplikáciách a operačných systémoch.</p> <p>Riešenie musí poskytovať ochranu pred mobilnými hrozbami pre moderné operačné systémy bez spoliehania sa na tretiu stranu</p>
<p><b>Monitoring a ochrana Active Directory:</b></p>	<p>Riešenie musí riešiť tajné útoky alebo APT (Advanced Persistent Threat) s účinnou obranou služby Active Directory z koncového bodu, aby poskytovalo autonómne obmedzenie narušenia, reakciu na incidenty a hodnotenie zabezpečenia domény.</p> <p>Riešenie má mať autonómnu schopnosť naučiť sa štruktúru služby Active Directory organizácie ako celok (servery, koncové body, aplikácie, používatelia, pobočky, konvencie pomenovania, konfigurácie, atribúty atď.)</p> <p>Riešenie musí byť schopné vytvoriť autentické maskovanie (obfuscation).</p> <p>Riešenie musí umožňovať priebežné vyhodnotenie procesov, kontextu a aktivity služby Active Directory.</p> <p>Riešenie má mať vysoko citlivú detekciu a schopnosť blokovať útok automaticky. riešenie má vedieť poskytovať forenzné hlásenia v reálnom čase, ktoré zachytáva skutočné prieskumné operácie, krádeže poverenia a pohybu, ktoré vykonal útočník a odklady reťazca útokov.</p> <p>Riešenie musí byť schopné automaticky vyriešiť zastavenie škodlivého procesu na koncovom bode, aby narušenie obsiahlo v reálnom čase, odstrániť jeho schopnosť vytvárať ďalšie procesy, prepísať inú časť pamäte, spustiť prieskumné príkazy alebo komunikovať do siete.</p> <p>Riešenie má mať schopnosť nepretržite skúmať nesprávnu konfiguráciu domény, zraniteľné miesta a perzistenciu, prezentovať doménu z pohľadu útočníka a umožniť okamžité riešenie rizika.</p> <p>Riešenie musí vedieť zabrániť zneužitiu údajov AD s pomocou technológie deception založenú na strojovom učení.</p> <p>Riešenie má mať automatizovaný proces hodnotenia, ktorý využíva simulácie útoku na zhromažďovanie podrobných informácií o konfigurácii domény, privilegovaných účtoch, nastavení zabezpečenia, GPO, koncových bodoch, radičoch domény a Kerberose.</p> <p>Riešenie má mať autonómnu analýzu každej komponenty domény a štruktúry služby Active Directory na nesprávnu konfiguráciu a zadné vrátka v AD a v celom prostredí domény.</p>
<p><b>Reporting a správa AV riešenia:</b></p>	<p>Riešenie má byť nasadené, spravované a aktualizované v balíčku jedného agenta a aktualizáčného mechanizmu.</p>

	<p>Riešenie zabezpečenia koncových staníc má možnosť na nasadenie v možnostiach Cloud, On-Prem a Hybrid.</p> <p>Riešenie musí umožňovať vyhľadávanie nespravovaných koncových bodov a nasadenie jediného agenta pre úplnú ochranu.</p> <p>Kontrola zabezpečenia a dodržiavanie predpisov sú spravované jediným management serverom a konzolou.</p> <p>Integrácia s LDAP, Syslog a Active Directory.</p> <p>Servery pre správu nainštalované na rôznych miestach majú mať schopnosť replikovať dáta, protokoly a obsah v definovanom intervale v architektúre Multi-Server Architecture pomocou zásad a replikácie protokolov. Súčasne podporovať clustering centrálnych konzol.</p> <p>Agent musí umožňovať ochranu heslom, heslo pre deaktiváciu služby a heslo pre otvorenie grafického používateľského rozhrania klienta, aby užívatelia nemohli odinštalovať agenta.</p> <p>Agent má mať schopnosť chrániť službu pred zastavením aj keď sa prihlási administrátor.</p> <p>Mechanizmus aktualizácie musí zahŕňať aktualizácie obsahu klienta zo servera pre správu, interných aktualizáčnych serverov, externých serverov pre aktualizáciu dodávateľov, tiež od klienta, ktorý funguje ako proxy medzi serverom pre správu a klientov v skupine a pomocou nástrojov tretích strán, ako je Microsoft SMS.</p> <p>Riešenie má mať jedného agenta pre všetky vymenované funkčné moduly - ochrana koncových bodov, aplikačná kontrola, aplikačná izolácia, Deception, ochrana AD a spoločnú správu a aplikovanie politík tak pre zariadenia typu PC, notebook, Mac, server a mobilné zariadenia iOS a Android.</p> <p>Riešenie AV má jedného a toho istého agenta pre fyzické i virtuálne klientske stanice.</p>
<b>Záruka:</b>	5 rokov priamo od výrobcu softvéru. Nahlasovanie poruchy v režime 24x7. Nahlasovanie porúch priamo u výrobcu softvéru.

#### LICENCIA, SUPPORT

<b>Podpora a typ licencie:</b>	5 rokov (60 mesiacov)
--------------------------------	-----------------------

#### IMPLEMENTÁCIA, TESTOVANIE, NASADENIE

<b>Služby:</b>	
----------------	--

	<p>Služby spojené so zmenou Security riešenie na koncových zariadeniach v rozsahu <b>15 človekodní</b> pozostávajúce z:</p> <ul style="list-style-type: none"> <li>• Úplné nasadenie všetkých modulov ochrany koncových bodov, EDR a ochrany AD na všetky určené zariadenia a systémy;</li> <li>• Migrácia pravidiel a politík zo stávajúceho riešenia ochrany koncových bodov;</li> <li>• Testovanie;</li> <li>• Základné zaškolenie.</li> </ul>
<b>Kľúčový expert</b>	<p>IT programátor/vývojár</p> <ul style="list-style-type: none"> <li>• minimálne 3-ročná preukázateľná odborná prax v oblasti informačných technológií;</li> <li>• minimálne dve (2) profesionálne praktické skúsenosti v oblasti implementácie informačných systémov;</li> <li>• platný certifikát alebo ekvivalent daného certifikátu vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou</li> </ul>

#### 4. SIEM/SOC ako služba

**Predmetom verejného obstarávania** je dodanie SIEM riešenia ako monitorovacieho nástroja na zaistenie a garanciu úrovne bezpečnosti a SOC ako služby. Všetky technické parametre/funkcionality, resp. vlastnosti požadovaného predmetu zákazky predstavujú minimálne požiadavky, ktoré musia byť splnené v ponuke uchádzača. V prípade, že by sa záujemca/uchádzač cítil dotknutý vo svojich právach, t. j., že by týmto opisom dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov/uchádzačov alebo výrobcov, alebo že tento predmet zákazky nie je opísaný dostatočne presne a zrozumiteľne, tak vo svojej ponuke môže uchádzač použiť technické riešenie ekvivalentné, ktoré spĺňa kvalitatívne, technické, funkčné požiadavky na rovnakej a vyššej úrovni, ako je uvedené v tejto časti výzvy, túto skutočnosť však musí preukázať uchádzač vo svojej ponuke.

#### ŠPECIFIKÁCIA

<b>Rozsah:</b>	<b>18 človekodní</b>
<b>Základná špecifikácia:</b>	<ul style="list-style-type: none"> <li>• Zber údajov a udalostí – zber bezpečnostných a prevádzkových záznamov z rôznych zariadení nachádzajúcich sa v IT infraštruktúre organizácie.</li> <li>• Normalizácia zozbieraných údajov – predspracovanie údajov za účelom zjednotenia rôznych formátov.</li> <li>• Korelácia – posúdenie vzťahov medzi jednotlivými údajmi a udalosťami.</li> <li>• Log management – uchovávanie log/auditných záznamov, ich komprimácia a indexácia.</li> <li>• Monitoring používateľov a jednotlivých častí IT infraštruktúry – sledovanie neobvyklého správania sa používateľov a administrátorov, detekcia potenciálnych a reálnych bezpečnostných incidentov a neobvyklých aktivít voči pravidlám a/alebo minulému stavu.</li> <li>• Audit a reporting – generovanie reportov o činnosti a bezpečnostnej kondícii IT infraštruktúry.</li> </ul>

<p><b>Špecifikácia zberu údajov:</b></p>	<ul style="list-style-type: none"> <li>• bezpečnostné udalosti z firewallov, VPN, IDS, IPS a databáz,</li> <li>• sieťové udalosti zo switchov, routerov, serverov a ďalších zariadení,</li> <li>• sieťové aktivity a komunikáciu až na úrovni Layer 7,</li> <li>• aktivity v cloude, Informácie zo SaaS a IaaS prostredia, ako sú Office365, Salesforce.com, Amazon Web Services (AWS), Azure a Google Cloud,</li> <li>• dáta o používateľoch a aktívach, teda informácie zo systémov na riadenie prístupov a identít,</li> <li>• informácie zo skenerov zraniteľností,</li> <li>• udalosti koncových zariadení, ako je Windows event Log, Sysmon a podobne,</li> <li>• aplikačné logy, či už ide o štandardné ERP, alebo vlastné aplikácie,</li> <li>• informácie o hrozbách, ako je napríklad IBM X-Force®.</li> </ul>
<p><b>SOC ako služba:</b></p>	<ul style="list-style-type: none"> <li>• Security Operations Center – SOC bude zaisťovať komplexnú centralizáciu riadenia bezpečnostných udalostí a incidentov, s cieľom minimalizovať reakčnú dobu na incident a škody z nej vyplývajúce.</li> <li>• Pomocou SIEM budú konzultanti SOC nepretržite monitorovať bezpečnostné incidenty a budú zodpovední za reakciu, ak sa zistí.</li> <li>• Detekcia - identifikuje sa, prípadne sa prijme, notifikácia o potenciálne škodlivom chovaní v chránenej infraštruktúre.</li> <li>• Analýza - určí sa, či sa jedná o bezpečnostnú udalosť alebo o bezpečnostný incident, ktorý môže mať negatívny dopad na nami chránenú infraštruktúru – analýza.</li> <li>• Investigácia - cieľom skúmania daného bezpečnostného incidentu bude zistiť konkrétne dopady a cestu, ktorou sa útočníkovi podarilo preniknúť do infraštruktúry.</li> <li>• Reakcia - Okamžitou reakciou sa minimalizuje dopad bezpečnostných incidentov.</li> <li>• Kontrola a zavedenie nápravných opatrení a reporting zistených skutočností na zvýšenie informovanosti – post incident aktivity.</li> </ul>
<p><b>Kľúčoví experti:</b></p>	<p><b>IT konzultant / Expert pre SIEM riešenie</b></p> <p>Rozsah: 17 človekodní</p> <ul style="list-style-type: none"> <li>• minimálne 3-ročná preukázateľná odborná prax na projektoch v oblasti implementácií, správy a prevádzky bezpečnostných riešení na centralizované monitorovanie bezpečnosti informačných systémov;</li> <li>• minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti implementácií, správy a prevádzky ponúkaného bezpečnostného riešenia centralizovaného monitorovania bezpečnosti siete, súčasťou ktorých bolo poskytovanie služieb monitorovania bezpečnosti v reálnom čase s požadovanou funkcionalitou na automatické vyhodnocovanie súladu s definovanými kritériami, funkcie sieťovej analýzy a na automatizovanú notifikáciu o podozrivých udalostiach;</li> <li>• platný technický certifikát v oblasti správy a prevádzky bezpečnostných riešení centralizovaného monitorovania bezpečnosti siete (SIEM) alebo ekvivalent daného certifikátu, vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</li> </ul>

### **Školiteľ pre IT systémy**

Rozsah: 1 človekodeň

- minimálne 3-ročná odborná prax v oblasti školenia informačných systémov;
- minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v školenia informačných systémov a školenia bezpečnostných riešení;
- platný technický certifikát v oblasti školenia bezpečnostných riešení alebo ekvivalent daného certifikátu, vydaný výrobcom ponúkaného riešenia alebo medzinárodne uznávanou akreditačnou a certifikačnou autoritou.

Príloha č. 2: Návrh na plnenie kritérií pre časť č. I predmetu zákazky

**Návrh na plnenie kritérií**

**Názov zákazky:** Zabezpečenie informačnej a kybernetickej bezpečnosti mesta Šaľa

Identifikačné údaje uchádzača:

Názov uchádzača: airo, s. r. o.

Sídlo uchádzača: Ivanská cesta 30/B, 821 04 Bratislava

IČO uchádzača: 48286621

E-mail kont. osoby: jakub.celes@airo.sk

Telefón kont. osoby: +421915493566

Mikropodnik, malý alebo stredný podnik: **áno – nie<sup>1</sup>** (neplatný údaj prečiarknuť)

**Návrh na plnenie kritérií Časť I.:** Dodávka a implementácia systémových nástrojov na zabezpečenie kybernetickej bezpečnosti mesta Šaľa

P.č. (1)	Popis položky (služba) (2)	Merná jednotka (MJ) (3)	Cena v € bez DPH za 1 MJ (4)	Výška DPH za 1 MJ (sadzba 20%) (5)	Celková (konečná) cena v € s DPH za 1 MJ (6)	Množstvo MJ počas platnosti zmluvy (7)	Cena v € bez DPH za celý predmet obstarávania (8)	Výška DPH za celý predmet obstarávania (sadzba 20%) (9)	Celková (konečná) cena v € s DPH za celý predmet obstarávania (10)
1)	Centrálny logovací systém (+ 5 ročný premium support) podľa špecifikácie uvedenej v opise časti I.	kus	24139,5	4 827,90	28 967,40	1	24 139,50	4 827,90	28 967,40

<sup>1</sup> **Mikropodniky:** podniky, ktoré zamestnávajú menej než 10 osôb s ktorých ročný obrat a/alebo celková ročná súvaha neprekačuje 2 milióny EUR.

**Malé podniky:** podniky, ktoré zamestnávajú menej ako 50 osôb a ktorých ročný obrat a/alebo celková ročná súvaha neprekačuje 10 miliónov EUR.

**Stredné podniky:** podniky, ktoré nie sú mikropodnikmi ani malými podnikmi a ktoré zamestnávajú menej ako 250 osôb a ktorých ročný obrat nepresahuje 50 miliónov EUR a/alebo celková ročná súvaha nepresahuje 43 miliónov EUR.





P.č. (1)	Popis položky (služba) (2)	Merná jednotka (MJ) (3)	Cena v € bez DPH za 1 MJ (4)	Výška DPH za 1 MJ (sadzba 20%) (5)	Celková (konečná) cena v € s DPH za 1 MJ (6)	Množstvo MJ počas platnosti zmluvy (7)	Cena v € bez DPH za celý predmet obstarávania (8)	Výška DPH za celý predmet obstarávania (sadzba 20%) (9)	Celková (konečná) cena v € s DPH za celý predmet obstarávania (10)
	IT konzultant/Expert pre SIEM riešenie	človekoden	650	130,00	780,00	17	11 050,00	2 210,00	13 260,00
	Školiteľ pre IT systémy	človekoden	650	130,00	780,00	1	650,00	130,00	780,00
Cena celkom						-	123 795,24	24 759,05	148 554,29

Ak je uchádzač platcom DPH uvedie cenu bez DPH a cenu vrátane DPH, ak uchádzač nie platcom DPH v ponuke na to upozorní.

**CENA ZA KAŽDÚ POLOŽKU PREDMETU OBSTARÁVANIA MUSÍ BYŤ NENULOVÁ A NESMIE MAŤ ZÁPORNÚ HODNOTU!**

**CENA ZA PREDMET TEJTO ZÁKAZKY JE KONEČNÁ. V CENE ZA PREDMET ZÁKAZKY MUSIA BYŤ ZAHRNUTÉ VŠETKY NÁKLADY NA PREDMET OBSTARÁVANIA VRÁTANE PREPRAVNÝCH NÁKLADOV.**

Vyplnené dňa:	5.8.2022
---------------	----------

---

Mgr. Jakub Čeles, Ing. Štefan Kopaj, Ing. Rudolf Törvényi -  
konatelia



Príloha č. 3: Čestné vyhlásenie uchádzača o subdodávateľoch

Obchodné meno uchádzača: airo, s. r. o.  
Sídlo: Ivanská cesta 30/B, 821 04 Bratislava  
IČO: 48286621

Predmet zákazky: **Zabezpečenie informačnej a kybernetickej bezpečnosti mesta Šaľa**

Vyhlasujem na svoju česť, že nebudem pri realizácii uvedeného predmetu zákazky zadávať akýkoľvek podiel zákazky subdodávateľom a celý predmet zákazky zrealizujem vlastnými kapacitami.

V Bratislave dňa 5.8.2022

.....  
Mgr. Jakub Čeles, konateľ

.....  
Ing. Štefan Kopaj, konateľ

.....  
Ing. Rudolf Törvényi, konateľ



#### Príloha č. 4: Zoznam Kľúčových expertov

Kľúčový expert č.1 (Špecialista pre infraštruktúry/HW špecialista):	Ing. Rudolf Törvényi
Kľúčový expert č.2 (Špecialista databázy):	Ing. Rudolf Törvényi
Kľúčový expert č.3 (IT Tester):	Ing. Rudolf Törvényi
Kľúčový expert č.4 (Špecialista pre bezpečnosť informačných systémov):	Ing. Rudolf Törvényi
Kľúčový expert č.5 ( IT programátor/vývojár):	Ing. Rudolf Törvényi
Kľúčový expert č.6 (IT konzultant/Expert pre SIEM riešenie):	Ing. Rudolf Törvényi
Kľúčový expert č.7 (Školiteľ pre IT systémy):	Ing. Rudolf Törvényi

V Bratislave dňa 5.8.2022

.....  
Mgr. Jakub Čeles, konateľ

.....  
Ing. Štefan Kopaj, konateľ

.....  
Ing. Rudolf Törvényi, konateľ