Zmluva o dielo a poskytnutí služieb

uzatvorená v súlade s § 269 ods. 2 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov (ďalej len „**Obchodný zákonník**")

(ďalej len „**Zmluva**")

medzi zmluvnými stranami:

Názov:	**Národná transfúzna služba SR**
Sídlo:	Ďumbierska 3/L, 831 01 Bratislava
IČO:	30 853 915
DIČ:	2021764371
IČ DPH:	SK2021764371
Štatutárny orgán:	Ing. Ivan Oleár, MBA, riaditeľ
Osoba oprávnená na rokovanie	
vo veciach zmluvy:	Ing. Ivan Oleár, MBA
vo veciach odborných:	Ing. Jozef Macko
e-mail:	jozef.macko@ntssr.sk
web:	www.ntssr.sk

(ďalej len „**Objednávateľ**" alebo „**NTS SR**")

a

Obchodné meno:	KOLAS s. r. o.
Sídlo/miesto podnikania:	Tomášikova 10/G, 821 03 Bratislava
IČO:	47060476
IČ DPH:	SK2023758495
DIČ:	2023758495
Bankové spojenie:	VÚB, a. s.
č. účtu:	SK3902000000003653927456
Štatutárny orgán:	Mgr. Iveta Gaľová – konateľ
Registrovaný:	Obchodný register Okresného súdu Bratislava I, oddiel: Sro, vložka č. 87961/B

(ďalej len „**Dodávateľ**")

(ďalej Objednávateľ alebo Dodávateľ aj ako „**zmluvná strana**" alebo spoločne „**zmluvné strany**")

Preambula

Podkladom pre uzatvorenie tejto Zmluvy sú súťažné podklady a ponuka Dodávateľa ako úspešného uchádzača predložená v rámci verejného obstarávania zákazky „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR" postupom podľa § 112 zákona č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej lej „**zákon o verejnom obstarávaní**"), ktorej plnenie zo strany Objednávateľa bude realizované zo štrukturálnych fondov Európskej únie v rámci projektu „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR", s kódom výzvy: OPII-2022/7/20-DOP, ktorými je táto zmluva limitovaná.

Táto Zmluva sa uzatvára aj na základe výsledkov a nálezov auditu kybernetickej bezpečnosti zo dňa 20.01.2022 u Objednávateľa (ďalej len „**Audit**").

Článok I.
Predmet Zmluvy

1.1 Predmetom tejto Zmluvy je záväzok Dodávateľa vykonať pre Objednávateľa dielo spočívajúce v rozvoji governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR (ďalej aj ako „**dielo**") a poskytnúť Objednávateľovi služby podpory a údržby v rozsahu a za podmienok stanovených v tejto Zmluve a jej prílohách (ďalej spolu aj „**predmet plnenia**") a záväzok Objednávateľa riadne vykonané dielo prevziať a zaplatiť Dodávateľovi dojednanú cenu predmetu plnenia.

1.2 Predmet plnenia pozostáva z nasledovných častí:

- 1.2.1 Vypracovanie návrhov a smerníc na základe odporúčaní Auditu v rozsahu a za podmienok uvedených v Prílohe č. 1 k Zmluve
- 1.2.2 Dodanie softvérového a hardvérového zabezpečenia v rozsahu a za podmienok uvedených v Prílohe č. 2 k Zmluve
- 1.2.3 Implementácia riešenia na jednotlivé lokality v rozsahu a za podmienok uvedených v Prílohe č. 3 k Zmluve
- 1.2.4 Poskytnutie služieb údržby a podpory (SLA) na služby a produkty po dobu 1 roka od dodania diela v rozsahu a za podmienok uvedených v Prílohe č. 4 k Zmluve
- 1.2.5 Dvojfaktorová autentifikácia v rozsahu a za podmienok uvedených v Prílohe č. 5 k Zmluve.

1.3 Dodávateľ sa týmto zaväzuje dodať predmet plnenia v súlade s požiadavkami Objednávateľa uvedenými v tejto Zmluve, ako aj technickými a inými špecifikáciami a požiadavkami v rozsahu uvedenom v prílohách tejto Zmluvy.

Článok II.
Práva a povinnosti zmluvných strán

2.1 Dodávateľ sa zaväzuje dodať predmet plnenia v rozsahu, v lehotách a za podmienok stanovených touto Zmluvou. Dodávateľ je povinný dodať predmet plnenia s najvyššou možnou odbornou starostlivosťou.

2.2 Dodávateľ sa najmä zaväzuje, že predmet plnenia bude z hľadiska technologických parametrov plne v súlade s aplikovateľnými právnymi predpismi, a to najmä zákonom č. 95/2019 Z.z.o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Vyhláškou Úradu podpredsedu vlády SRpre investície a informatizáciu č. 78/2020 Z.z. o štandardoch pre informačné technológie verejnej správy a zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Prípadný nesúlad diela s podmienkami vyplývajúcim z uvedených právnych predpisov sa považuje za vadu diela a Dodávateľ bude povinný odstrániť takýto nesúlad bezodplatne bez zbytočného odkladu.

2.3 Dodávateľ sa zároveň zaväzuje poskytovať služby podpory a údržby tak ako sú definované v Prílohe č. 4 k tejto Zmluve tak, aby bola zabezpečená najmä bezporuchovosť a prevádzkyschopnosť diela.

2.4 Hardvérové vybavenie dodávané v rámci vykonávania diela podľa Prílohy č. 2 k Zmluve musí byť nové, nepoužité, nerepasované, v originálnom balení od výrobcu a zodpovedajúce minimálnym technickým a funkčným parametrom uvedeným v Prílohe č. 2 k Zmluve.

2.5 Popis riešenia obsiahnutý v analytických výstupoch musí byť podrobný, aby bolo na jeho základe možné zhodnotiť funkcie implementovaného riešenia.

2.6 V prípade ak Dodávateľ poverí vykonávaním predmetu plnenia subdodávateľov, zodpovedá, ako keby plnil sám. Dodávateľ je povinný zabezpečiť, aby všetci jeho zamestnanci, spolupracujúce osoby a subdodávatelia podieľajúci sa na plnení tejto Zmluvy mali potrebné odborné schopnosti, vedomosti a skúsenosti na plnenie tejto Zmluvy.

2.7 Dodávateľ je povinný dodržiavať pri plnení Zmluvy právny poriadok Slovenskej republiky, príslušné technické normy ako aj vnútorné normy, predpisy, usmernenia a pokyny Objednávateľa (najmä vo vzťahu k bezpečnostnej politike), s ktorými bol oboznámený a je povinný zabezpečiť ich dodržiavanie aj zo strany jeho zamestnancov a spolupracujúcich tretích osôb.

2.8 Objednávateľ je povinný počas trvania tejto Zmluvy poskytnúť Dodávateľovi nevyhnutnú súčinnosť potrebnú na vykonávanie predmetu plnenia, najmä je povinný mu poskytnúť všetky informácie a podklady, ktoré môžu súvisieť s vykonávaním predmetu plnenia a sú na jeho vykonanie potrebné a oznamovať Dodávateľovi skutočnosti nevyhnutné k riadnemu plneniu tejto Zmluvy.

2.9 Dodávateľ zodpovedá za to, že dodané dielo nebude obsahovať Objednávateľom nevyžiadané alebo neschválené funkcie a vlastnosti, ktoré súčasne nie sú potrebné. Porušenie tejto povinnosti je podstatným porušením Zmluvy.

2.10 Dodávateľ sa zaväzuje minimalizovať pri vykonávaní diela také systémové prvky, resp. zabezpečovacie prostriedky, ktoré by v budúcnosti mohli viesť pri používaní diela k obmedzeniu konkurenčného prostredia.

2.11 Porušenie ktorejkoľvek povinnosti Dodávateľa uvedenej v tomto článku Zmluvy sa považuje za podstatné porušenie Zmluvy.

Článok III.
Čas a miesto plnenia

3.1 Zmluvné strany sa dohodli, že Dodávateľ odovzdá Objednávateľovi riadne vykonané dielo najneskôr do 31.10.2023. Riadnym odovzdaní diela sa rozumie dodanie predmetu zmluvy v rozsahu podľa Čl. I. bod 1.2 sub. 1.2.1, 1.2.2, 1.2.3 a 1.2.5, ktoré spĺňa požiadavky stanovené v tejto Zmluve a jej prílohách.

3.2 V prípade, ak riadne vykonané dielo nebude odovzdané ani do 31.12.2023, Objednávateľ je oprávnený od tejto Zmluvy bez ďalšieho odstúpiť.

3.3 Dodávateľ je povinný predložiť Objednávateľovi pri podpise tejto Zmluvy vyplnený harmonogram prác, ktorý bude tvoriť Prílohu č. 7 tejto Zmluvy (Harmonogram prác). Dodávateľ je povinný v priebehu plnenia tejto Zmluvy Objednávateľa priebežne informovať o aktuálnom stave dodržiavania Harmonogramu prác. V prípade ak sa Dodávateľ dostane do časového sklzu alebo má vedomosť o takej skutočnosti, ktorej dôsledkom môže byť nedodržanie Harmonogramu prác, je povinný o tejto skutočnosti bezodkladne informovať Objednávateľa a Harmonogram prác upraviť; vždy však tak, aby nedošlo k omeškaniu s odovzdaním diela ako celku. Upravený Harmonogram prác musí byť odsúhlasený Objednávateľom a stane sa neoddeliteľnou súčasťou tejto Zmluvy.

3.4 Miestom vykonávanie diela je sídlo Objednávateľa a jeho pracoviská podľa Prílohy č. 10 (Miesta realizácie). Miestom odovzdania diela je sídlo Objednávateľa.

Článok IV.
Odovzdanie a prevzatie diela

4.1 Dodávateľ berie na vedomie, že je oprávnený odovzdať dielo po častiach.

4.2 Časť diela podľa Článku I., bod 1.2 sub. 1.2.1 Zmluvy odovzdá Dodávateľ Objednávateľovi v tlačenej aj elektronickej podobe.

4.3 Pred odovzdaním diela podľa Článku I. bod 1.2 sub. 1.2.2, 1.2.3 a 1.2.5 Zmluvy je Dodávateľ povinný vykonať testovanie prevádzkyschopnosti a správnosti fungovania diela, čím sa overí splnenie funkčných, výkonnostných a bezpečnostných požiadaviek diela a zároveň je povinný tieto výsledky zdokumentovať (ďalej len „**skúšobná prevádzka**").

4.4 O odovzdaní každej časti diela spíšu zmluvné strany Protokol o odovzdaní a prevzatí časti diela, ktorý bude podpísaný oboma zmluvnými stranami.V Protokole o odovzdaní a prevzatí časti diela bude vyznačený dátum odovzdania a prevzatia časti diela, meno a priezvisko osôb poverených na odovzdanie a prevzatie diela a ich podpis, ktorým potvrdzujú, že časť diela bola vykonaná riadne a v súlade so Zmluvou. Príslušná časť diela sa považuje za odovzdanú dňom podpísania Protokolu o odovzdaní a prevzatí časti diela. Protokol bude vyhotovený v dvoch

rovnopisoch, pričom každá zo strán obdrží jeden rovnopis.

4.5 Po dodaní poslednej časti diela spíšu zmluvné strany finálny Protokol o odovzdaní diela s náležitosťami ako sú uvedené v bode 4.4 vyššie. Súčasťou Protokolu o odovzdaní a prevzatí diela bude aj zoznam licencií, ktoré Dodávateľ udeľuje Objednávateľovi, záznam o zaškolení zamestnancov a vyhlásenie o dodržaní štandardov pre informačné systémy verejnej správy. Dodávateľ sa zaväzuje Objednávateľovi odovzdať do užívania kompletné dielo, ktoré bude plne funkčné pre účely a potreby Objednávateľa, spôsobilé na spustenie do prevádzky podľa podmienok dohodnutých v tejto Zmluve a bude spĺňať špecifikácie podľa tejto Zmluvy a všeobecne záväzných právnych predpisov.

4.6 V prípade, ak má dielo alebo jeho časť vady, ktoré však nebránia užívaniu diela alebo jeho časti na účel, na ktorý je určený, môže Objednávateľ dielo prevziať. V takomto prípade zmluvné strany spíšu zoznam chýb, vád a nedostatkov v protokole o odovzdaní a prevzatí predmetu zmluvy spolu so stanovením lehoty na ich odstránenie. Po odstránení chýb, vád a nedostatkov zmluvné strany spíšu protokol o odstránení vád diela.

4.7 Objednávateľ je oprávnený odmietnuť prevzatie diela alebo jeho časti, najmä v prípade zjavných vád, dodania nedostatočnej dokumentácie, v prípade, ak dielo nespĺňa požadované špecifikácie alebo kvalitatívne vlastnosti, ak dielo nie je kompletné alebo bolo dodané v rozpore s touto Zmluvou alebo všeobecne záväznými právnymi predpismi, ak neprebehla skúšobná prevádzka alebo ak zo skúšobnej prevádzky vyplynuli vady, ktoré podľa posúdenia Objednávateľa bránia riadnemu užívaniu diela.V prípade, ak Objednávateľ odmietne dielo prevziať, oznámi túto skutočnosť Dodávateľovi písomne spolu s uvedením dôvodov odmietnutia a stanovením lehoty na odstránenie vád diela. Dodávateľ sa zaväzuje v dodatočnej primeranej lehote určenej Objednávateľom tieto vady bezodkladne odstrániť. V prípade, ak k odovzdaniu a prevzatiu riadne vykonaného diela nedôjde najneskôr do 31.12.2023, Objednávateľ je oprávnený od odstúpiť od Zmluvy.

4.8 Po odstránení vád, z dôvodov ktorých, Objednávateľ dielo neprevzal, je Dodávateľ povinný vykonať opätovne skúšobnú prevádzku, s výnimkou prípadov, kedy sa objektívne skúšobná prevádzka nevyžaduje.

4.9 Dodávateľ sa spolu s dielom zaväzuje odovzdať Objednávateľovi všetku dokumentáciu, ktorá je potrebná na riadne užívanie diela.

Článok V.
Cena za predmet plnenia

5.1 Cena za predmet plnenia je stanovená v eurách na základe ponuky Dodávateľa ako úspešného uchádzača vo verejnom obstarávaní v súlade s § 2 ods. 3 zákona č. 18/1996 Z.z. o cenách a súvisiacich právnych predpisov.

5.2 Kalkulácia ceny a špecifikácia jednotlivých položiek je uvedená v Prílohe č. 6 k tejto Zmluve.

5.3 Cena za predmet plnenia sa skladá z dvoch častí:

a) cena počas implementácie diela a podpora počas prvého roka realizácie projektu Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR
b) cena za služby podpory počas jedného roka doby udržateľnosti projektu Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR

5.4 Cena za predmet plnenia je pevne určená, maximálna a konečná, ktorá zahŕňa všetky položky požadovaného rozsahu predmetu plnenia vrátane súvisiacich služieb, poplatkov a odmien za udelenie licencií, cestovných a ubytovacích nákladov a pod.

5.5 V cene za predmet plnenia sú zahrnuté všetky náklady Objednávateľa pri dodávaní diela a poskytovaní služieb údržby a podpory počas jedného roka.

5.6 Objednávateľ vyhlasuje a Dodávateľ berie na vedomie, že cena za predmet plnenia bude uhradená zo štrukturálnych fondov Európskej únie v rámci projektu „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR", s kódom výzvy: OPII-2022/7/20-DOP.

5.7 Objednávateľ je oprávnený bez akýchkoľvek sankcií odstúpiť od Zmluvy v prípade, kedy ešte nedošlo k plneniu z tejto Zmluvy a výsledky finančnej kontroly poskytovateľa nenávratného finančného príspevku neumožňujú financovanie výdavkov vzniknutých z obstarávania predmetu tejto Zmluvy.

Článok VI.
Platobné podmienky

6.1 Zmluvné strany sa dohodli že Objednávateľ uhradí Dodávateľovi ceny za predmet plnenia čiastkovo v súlade s Harmonogramom prác uvedeným v Prílohe č. 7 Zmluvy. Jednotlivé položky Harmonogramu prác predstavujú tzv. fakturačné míľniky.

6.2 Nárok Dodávateľa na úhradu ceny za každú časť diela vzniká po riadnom odovzdaní príslušnej časti diela na základe podpísaného Protokolu o odovzdaní a prevzatí časti diela.

6.3 Daňovým dokladom je pre zmluvné strany faktúra. Dodávateľ je povinný vystaviť faktúru a doručiť ju Objednávateľovi na adresu jeho sídla najneskôr do 5 dní od podpisu Protokolu o odovzdaní a prevzatí časti diela.

6.4 Faktúra musí obsahovať všetky náležitosti daňového dokladu podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov. Faktúra musí obsahovať aj odkaz na číslo tejto Zmluvy a jej prílohou musí byť podpísaný Protokol o odovzdaní a prevzatí časti diela. Za správne vyhotovenie faktúry zodpovedá v plnom rozsahu Dodávateľ.

6.5 Ak faktúra nebude obsahovať ustanovené náležitosti alebo v nej nebudú správne uvedené údaje, Objednávateľ ju vráti v lehote piatich (5) pracovných dní od jej obdržania Dodávateľovi s odôvodnením, že vo faktúre sú chýbajúce náležitosti alebo nesprávne údaje. V takomto prípade nová lehota splatnosti začne plynúť doručením opravenej faktúry Objednávateľovi.

6.6 Faktúry sú splatné v lehote 60 dní odo dňa ich doručenia Objednávateľovi.

6.7 Zmluvné strany sa dohodli na spôsobe platenia prostredníctvom bezhotovostného platobného styku, ktorý sa bude realizovať výhradne prevodným príkazom.

6.8 Faktúry sa považujú za uhradené v celom rozsahu dňom odpísania splatnej sumy z účtu Objednávateľa.

6.9 V prípade omeškania Objednávateľa s úhradou faktúry má Dodávateľ právo na uplatnenie zákonného úroku z omeškania.

Článok VII.
Zodpovednosť za vady a záruka

7.1 Dodávateľ zodpovedá za vady predmetu plnenia v súlade s § 560 a nasl. Obchodného zákonníka, pokiaľ v tomto článku Zmluvy nie je dohodnuté inak.

7.2 Dodávateľ zodpovedá za vady diela, ktoré ma dielo v čase protokolárneho odovzdania Objednávateľovi a to aj v prípade, ak sa takáto vada stane zjavnou až neskôr a za vady, ktoré sa na diele vyskytnú počas záručnej doby.

7.3 Za vady diela sa podľa tejto Zmluvy považujú najmä vykonanie diela v rozpore s touto Zmluvou a špecifikáciami, nedostatky alebo odchýlky vkvalitatívnych, technologických a technických parametroch, nedostatok iných parametrov požadovaných Objednávateľom, akékoľvek chyby a nesprávne funkcie diela, právne vady diela.

7.4 Dodávateľ poskytuje Objednávateľovi zmluvnú záruku na dielo najmenej v trvaní 12 mesiacov. Záručná doba začína plynúť momentom protokolárneho odovzdania a prevzatia časti diela. Záručná doba neplynie po dobu od nahlásenia vady po jej odstránenie, počas ktorej Objednávateľ nemôže dielo užívať riadne pre jeho vady, za ktoré zodpovedá Dodávateľ.

7.5 V prípade, ak má dielo vady, za ktoré zodpovedá Dodávateľ, Dodávateľ sa zaväzuje tieto vady odstrániť v lehotách a v súlade s podmienkami uvedenými v Prílohe č. 4 k tejto Zmluve.

7.6 Dodávateľ nezodpovedá za vady diela spôsobené použitím nevhodných podkladov a vecí poskytnutých Objednávateľom, pri ktorých nemohol ani pri vynaložení odbornej starostlivosti zistiťich nevhodnosť, alebo ak na ich nevhodnosť upozornil Objednávateľa a ten na ich použití napriek tomu trval. Dodávateľ nezodpovedá ani za vady a poruchy spôsobené neodborným alebo násilným zachádzaním s časťami diela (hardvérové vybavenie) a za vady spôsobené neoprávneným zásahom do diela Objednávateľom alebo tretími osobami.

7.7 V prípade zistenia neodstrániteľných vád alebo nedostatkov diela počas trvania zmluvnej záruky je Dodávateľ má Objednávateľ podľa vlastného výberu nárok:

a) na zľavu z ceny diela v prípade, ak takáto vada zásadným spôsob neobmedzuje užívanie predmetu zmluvy a/alebo
b) na odstúpenie od Zmluvy ak takáto vada zásadným spôsob obmedzuje alebo znemožňuje užívanie diela.

7.8 Uplatnením nárokov z vád predmetu zmluvy sa dodávateľ nezbavuje povinnosti nahradiť objednávateľovi škodu, ktorá mu vznikla a povinnosti zaplatiť zmluvnú pokutu.

Čl. VIII.
Autorské práva

8.1 Ak bude výsledkom vykonávania diela autorské dielo platí, že ide o dielo vytvorené Dodávateľom na objednávku Objednávateľa v zmysle § 91 zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov (ďalej len „*Autorský zákon*"). Ak dielo bude počítačovým programom alebo databázou platí, že sa na vytváranie diela vzťahujú ustanovenia o zamestnaneckom diele (§ 90 Autorského zákona).

8.2 Ak sa dielo alebo jeho časť vytvorené podľa tejto Zmluvy riadi ustanoveniami o zamestnaneckom diele (§ 90 Autorského zákona), majetkové práva k dielu vykonáva výlučne Objednávateľ, a to vo svojom mene a na svoj účet. Dodávateľ nie je oprávnený udeliť súhlas tretej osobe na použitie diela, ani ho sám používať alebo vykonávať k dielu majetkové práva bez predchádzajúceho písomného súhlasu Objednávateľa. Objednávateľ je oprávnený použiť dielo na akýkoľvek účel, ktorý umožňuje povaha diela, najmä na zverejnenie, verejné rozširovanie, zaradenie diela do databázy, označenie názvom Objednávateľa, spracovanie diela, spojenie diela s iným dielom, vyhotovenie rozmnoženiny, zmeny alebo iný zásah do diela a je oprávnený udeliť súhlas na použitie diela (licenciu) tretej osobe, a to bez potreby súhlasu Dodávateľa. Právo vykonávať majetkové práva k dielu prechádzajú aj na právneho nástupcu Objednávateľa. Objednávateľ je oprávnený výkon majetkových práv k dielu postúpiť tretej osobe bez predchádzajúceho súhlasu Dodávateľa.

8.3 Ak dielo alebo jeho časť vytvorené na základe tejto Zmluvy nebude počítačovým programom alebo databázou, Dodávateľ udeľuje Objednávateľovi súhlas na použitie diela (licenciu) na použitie diela akýmkoľvek spôsobom, ktorý umožňuje povaha diela, a to najmä na spracovanie diela, jeho spojenie s iným dielom, zaradenie diela do databázy, vyhotovenie rozmnoženiny, verejné rozširovanie originálu diela alebo rozmnoženiny diela, uvedenie diela na verejnosti, vykonanie zmien a zásah do diela, ako aj akýmkoľvek iným spôsobom, najmä vyplývajúcim z účelu tejto Zmluvy. Dodávateľ nie je sám oprávnený vytvorené dielo použiť alebo udeliť súhlas na jeho použitie tretej osobe. Odmena za udelenie licencie je už zahrnutá v cene za predmet plnenia. Dodávateľ udeľuje Objednávateľovi licenciu na dobu trvania majetkových práv k dielu. Licencia udelená Dodávateľom Objednávateľovi je výhradná a územne a vecne neobmedzená. Objednávateľ nie je povinný výhradnú licenciu použiť. Zánikom Objednávateľa prechádzajú práva a povinnosti z licencie na právneho nástupcu Objednávateľa. Objednávateľ je oprávnený udeliť tretej osobe súhlas na použitie diela (sublicenciu) aj bez predchádzajúceho súhlasu Dodávateľa, s čím Dodávateľ výslovne súhlasí. Objednávateľ je oprávnený licenciu postúpiť tretej osobe (previesť) aj bez predchádzajúceho súhlasu Dodávateľa, s čím Dodávateľ výslovne súhlasí. Pokiaľ nebude Dodávateľ informovaný o osobe postupníka, nezakladá to neplatnosť postúpenia licencie. Udelenie sublicencie ako aj postúpenie licencie nemusí mať písomnú formu.

8.4 Dodávateľ sa aj po dobu trvania tejto Zmluvy ako aj po skončení tejto Zmluvy zaväzuje bezodkladne po výzve Objednávateľa poskytnúť Objednávateľovi súčinnosť potrebnú pre riadne vykonávanie práv k dielu, spočívajúcu najmä v podpise osobitnej zmluvy, ktorej predmetom bude udelenie licencie na dielo v rozsahu špecifikovanom v tomto Článku Zmluvy, podpisu vyhlásenia

alebo potvrdenia potvrdzujúceho výkon majetkových práv k dielu Objednávateľom, ďalej sa zaväzuje odovzdať Objednávateľovi bezodkladne po výzve Objednávateľa akékoľvek doklady, dokumenty, zariadenia alebo softvérové riešenia potrebné pre vykonávanie práv k dielu Objednávateľom.

8.5 Dodávateľ netrvá na označení diela svojím menom alebo menom osôb, ktoré na vytvorenie diela použil. Dodávateľ sa zaväzuje vysporiadať akékoľvek nároky zamestnancov alebo iných osôb, ktoré použil na vytvorenie diela.

8.6 Ak bude súčasťou vytvorenia diela podľa tejto Zmluvy dodávka softvéru tretích strán (tzv. podporný softvér) alebo databázy, Dodávateľ sa zaväzuje po dobu trvania licencie k dielu alebo po dobu výkonu majetkových práv k dielu Objednávateľom zabezpečiť pre Objednávateľa licenciu na použitie takéhoto softvéru alebo databázy vo forme, v ktorej túto licenciu poskytuje výrobca alebo distribútor tohto softvéru alebo databázy. Objednávateľ má právo túto licenciu nevyužiť a žiadať od Dodávateľa zníženie ceny za predmet plnenia o časť predstavujúcu náklad na licenciu na softvér alebo databázu tretej strany.

8.7 Dodávateľ vyhlasuje a zodpovedá, že dodané dielo nebude zaťažené právom tretej osoby a bude bez právnych vád. V prípade zistenia právnej vady je Dodávateľ povinný bezodkladne upraviť dielo tak, aby nenarušovalo práva tretích osôb. Pokiaľ vznikne Objednávateľovi škoda z dôvodu práv tretích osôb k dielu, Dodávateľ sa zaväzuje Objednávateľa odškodniť v plnej výške, a to vrátane trov právneho zastúpenia.

8.8 Dodávateľ vyhlasuje a zodpovedá, že pri plnení predmetu tejto Zmluvy nebudú porušené právne normy, najmä práva duševného vlastníctva tretích osôb a že nie sú tretie osoby, ktoré by mohli oprávnenie uplatňovať akékoľvek svoje nároky z týchto práv voči Objednávateľovi.

8.9 Ustanovenia tohto Článku Zmluvy zostávajú platné a účinné aj po zániku tejto Zmluvy.

8.10 Objednávateľ podpisom Zmluvy akceptuje udelenie licencie v rozsahu, v akom mu bola udelená v tomto Článku Zmluvy.

Článok IX.
Povinnosť mlčanlivosti

9.1 Objednávateľ výslovne upozorňuje Dodávateľa, že je súčasťou kritickej infraštruktúry štátu a subjektom hospodárskej mobilizácie, v dôsledku čoho sú akékoľvek informácie týkajúce sa informačnej a kybernetickej bezpečnosti Objednávateľa striktne dôverné.

9.2 Dodávateľ sa zaväzuje považovať všetky skutočnosti a informácie (vrátane dát, know-how, materiálov, podkladov a zariadení poskytnutých Objednávateľom), ktoré mu boli poskytnuté Objednávateľom alebo v mene Objednávateľa, alebo ktoré sa mu stali inak známe na základe tejto Zmluvy alebo v súvislosti s touto Zmluvou za dôverné a zaväzuje sa zachovávať mlčanlivosť o takýchto skutočnostiach a informáciách (ďalej len "**Dôverné informácie**"). Dôvernými informáciami sa rozumejú aj informácie o Objednávateľovi, o jeho informačných systémoch, bezpečnostnej politike, pracovných postupoch a organizačných opatreniach. Povinnosť mlčanlivosti trvá aj po skončení tejto Zmluvy bez časového obmedzenia.

9.3 Dodávateľ sa zaväzuje najmä že Dôverné informácie neoznámi, neposkytne ani inak nesprístupní ani neumožní získať tretej osobe, nezverejní, nezahrnie do žiadnej publikácie ani nepoužije vo svoj prospech alebo v prospech tretej osoby bez predchádzajúceho písomného súhlasu Objednávateľa. Zároveň sa Dodávateľ zaväzuje, že nesprístupní Objednávateľovi informácie, ktoré sú vo výhradnom vlastníctve tretej osoby a na ktoré sa vzťahuje povinnosť mlčanlivosti podľa zákona alebo podľa osobitnej dohody s treťou osobou bez predchádzajúceho súhlasu tejto osoby.

9.4 Povinnosť mlčanlivosti sa nevzťahuje na Dôverné informácie, ktoré (i) boli Dodávateľovi známe pred ich prijatím zo strany Objednávateľa, čo musí byť zdokumentované písomným záznamom, alebo (ii) boli v čase poskytnutia Dodávateľovi verejne známe a dostupné, alebo sa stali verejne známymi a dostupnými po ich poskytnutí Dodávateľovi, za predpokladu, že sa tak nestalo porušením povinnosti mlčanlivosti, alebo (iii) boli poskytnuté Dodávateľovi treťou osobou na to oprávnenou, na ktorú sa nevzťahovala povinnosť mlčanlivosti, alebo (iv) ktoré je Dodávateľ povinný sprístupniť na základe zákona alebo právoplatného rozhodnutia súdu alebo iného orgánu verejnej správy. V prípadoch uvedených v tomto bode Zmluvy je však Dodávateľ povinný bezodkladne informovať Objednávateľa o požiadavke alebo povinnosti sprístupniť Dôverné informácie a umožniť Objednávateľovi pred sprístupnením Dôverných informácií využiť všetky existujúce prostriedky v súlade s právnymi predpismi, ktoré má Objednávateľ k dispozícii.

9.5 Porušením povinnosti mlčanlivosti nie je poskytnutie Dôverných informácií odborným poradcom Dodávateľa (najmä právni, daňoví, účtovní poradcovia), ktorí sú viazaní povinnosťou mlčanlivosti najmenej v rovnakom rozsahu, aký vyplýva z tohto Článku Zmluvy.

9.6 Povinnosť zachovávať mlčanlivosť o Dôverných informáciách sa v rovnakom rozsahu vzťahuje aj na osoby, ktoré Dodávateľ použil na plnenie povinností z tejto Zmluvy.

9.7 Zmluvné strany vyhlasujú, že Dodávateľ nebude mať pri vykonávaní diela prístup k osobným údajom dotknutých osôb, ktoré spracováva Objednávateľ vo svojich informačných systémoch. V prípade, ak pri vykonávaní diela alebo v súvislosti s ním Dodávateľ príde výnimočne do styku s osobnými údajmi spracovávanými Objednávateľom v jeho informačných systémoch, zaväzuje sa Dodávateľ zachovávať mlčanlivosť o takýchto osobných údajoch a bez súhlasu prevádzkovateľa informačného systému ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Dodávateľ je povinný zabezpečiť, že túto povinnosť mlčanlivosti budú v rovnakom rozsahu dodržiavať aj jeho zamestnanci a iné osoby, ktoré Dodávateľ použil na plnenie povinností z tejto Zmluvy.

9.8 Dodávateľ zodpovedá Objednávateľovi za škodu spôsobenú porušením mlčanlivosti. Porušenie povinnosti mlčanlivosti Dodávateľom sa považuje za podstatné porušenie Zmluvy.

Článok X.
Sankcie a náhrada škody

10.1 V prípade omeškania Objednávateľa s úhradou ceny za predmet plnenia alebo jej časti je Dodávateľ oprávnený uplatniť si u Objednávateľa nárok na úrok z omeškania vo výške podľa § 369 ods. 2 Obchodného zákonníka v spojení s § 1 ods. 1 nariadenia vlády SR č. 21/2013 Z.z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka.

10.2 V prípade omeškania Dodávateľa s dodaním riadne vykonaného diela v lehote podľa Článku III. bod 3.1 tejto Zmluvy je Objednávateľ oprávnený uplatniť si voči Dodávateľovi nárok na zaplatenie zmluvnej pokuty vo výške 0,03% z ceny za nedodaný predmet plnenia bez DPH za každý aj začatý deň omeškania.

10.3 V prípade nedodržania reakčného času (lehota nástupu na odstránenie chyby) vymedzeného v Tabuľke 1 Prílohy č. 4 tejto Zmluvy je Objednávateľ oprávnený uplatniť si voči Dodávateľovi nárok na zaplatenie zmluvnej pokuty vo výške 1.000,- EUR za každé jedno porušenie povinnosti Dodávateľa.

10.4 V prípade omeškania Dodávateľa s odstránením kritickej alebo naliehavej vady podľa 1 Prílohy č. 4 tejto Zmluvy je Objednávateľ oprávnený uplatniť si voči Dodávateľovi nárok na zaplatenie zmluvnej pokuty vo výške 1.000,- EUR za každé jedno porušenie povinnosti Dodávateľa.

10.5 V prípade porušenia povinnosti mlčanlivosti vymedzenej v Článku IX. Zmluvy Dodávateľom je Objednávateľ oprávnený uplatniť si voči Dodávateľovi zmluvnú pokutu vo výške 5.000,- EUR za každý prípad porušenia.

10.6 Zmluvnú pokutu je Dodávateľ povinný zaplatiť Objednávateľovi do 10 dní od doručenia výzvy Objednávateľa na jej úhradu. Objednávateľ je oprávnený právo na zmluvnú pokutu podľa tohto bodu Zmluvy započítať voči právu Dodávateľa na zaplatenie ceny za predmet plnenia, a to aj vtedy, ak splatnosť ceny za predmet plnenia ešte nenastala.

10.7 Zmluvné strany zhodne vyhlasujú, že dojednaná výška zmluvných pokút je primeraná významu zabezpečovanej povinnosti a následkom jej porušenia.

10.8 Zaplatením zmluvnej pokuty nie je dotknuté právo Objednávateľa požadovať splnenie porušenej povinnosti, právo Objednávateľa na odstúpenie od Zmluvy, ako ani nárok Objednávateľa na náhradu škody v plnej výške.

10.9 Dodávateľ sa nedostane do omeškania s plnením povinností podľa tejto Zmluvy, pokiaľ Objednávateľ neposkytne Dodávateľovi súčinnosť potrebnú pre plnenie záväzkov Dodávateľa.

10.10 V prípade, ak Dodávateľ spôsobí Objednávateľovi zavineným porušením svojich povinností vyplývajúcich mu z právnych predpisov alebo Zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. Za škodu sa pre účely tejto Zmluvy rozumejú aj pokuty a iné majetkové sankcie uložené Objednávateľovi v dôsledku porušenia povinností zo strany Objednávateľa.

10.11 Dodávateľ zodpovedá za škodu aj vtedy, pokiaľ bola táto spôsobená jeho zamestnancami alebo inými osobami, prostredníctvom ktorých Dodávateľ plnil svoje záväzky podľa tejto Zmluvy.

10.12 Zmluvné strany nezodpovedajú za škodu, pokiaľ bola spôsobená okolnosťami vylučujúcimi zodpovednosť podľa § 374 Obchodného zákonníka. Zodpovednosť zmluvnej strany nevylučuje prekážka, ktorá vznikla až v čase, keď povinná strana bola v omeškaní s plnením svojej povinnosti. Vylúčenie zodpovednosti za škodu pre okolnosť vylučujúcu zodpovednosť sa vzťahuje len pokiaľ trvá prekážka zakladajúca okolnosť vylučujúcu zodpovednosť. Zmluvná strana, ktorej sa prekážka týka, je povinná vyvinúť maximálne úsilie na odstránenie a prekonanie okolnosti vylučujúcej jej zodpovednosť a bezodkladne na takúto prekážku upozorniť druhú zmluvnú stranu a spolupracovať s druhou zmluvnou stranou na predchádzaní vzniku škody.

Článok XI.
Doručovanie

11.1 Zmluvné strany sa dohodli, že všetky písomnosti, oznámenia, žiadosti a prejavy vôle podľa tejto Zmluvy sa doručujú osobne, prostredníctvom elektronických prostriedkov na prenos dát a informácií (e-mail) alebo poštou, pokiaľ nie je v tejto Zmluve dohodnuté inak.

11.2 Pri osobnom doručovaní (patrí sem aj doručovanie kuriérom, inou treťou osobou, osobné preberanie písomností medzi zmluvnými stranami) sa písomnosť považuje za doručenú okamihom jej odovzdania adresátovi; za doručenie písomnosti sa považuje aj okamih, keď adresát odmietol prevziať písomnosť, a to okamihom tohto odmietnutia.

11.3 Pri doručovaní poštou, pokiaľ nepôjde o doporučenú zásielku, sa zásielka považuje za doručenú piaty deň po jej odoslaní. Pri doporučenej zásielke sa zásielka považuje za doručenú tretí pracovný deň po dni podania zásielky.

11.4 Zmluvné strany sa dohodli, že akékoľvek prejavy Zmluvných strán smerujúce k skončeniu platnosti tejto Zmluvy musia byť doručované osobne alebo vo forme doporučenej zásielky.

11.5 Pre doručovanie písomností medzi Zmluvnými stranami platia kontaktné údaje Zmluvných strán uvedené v záhlaví tejto Zmluvy alebo iné kontaktné údaje, ktoré adresát uviedol v písomnom oznámení doručenom druhej Zmluvnej strane.

11.6 Zmluvné strany sa zaväzujú oznamovať si navzájom bez zbytočného odkladu zmeny kontaktných osôb a kontaktných údajov uvedených v záhlaví tejto Zmluvy, inak zodpovedajú za škodu, ktorá tým druhej zmluvnej strane vznikla.

Článok XII.
Subdodávky

12.1 Dodávateľ môže zabezpečiť časť plnenia predmetu Zmluvy prostredníctvom svojich subdodávateľov.

12.2 Dodávateľ garantuje spôsobilosť subdodávateľov pre plnenie predmetu Zmluvy.

12.3 Dodávateľ má právo na zmenu subdodávateľa, prostredníctvom ktorého nepreukazoval splnenie podmienok účasti podľa § 27, resp. § 28 zákona o verejnom obstarávaní vo vzťahu k plneniu, ktorého sa táto Zmluva týka.

12.4 Dodávateľ má právo na doplnenie nového subdodávateľa vo vzťahu k plneniu, ktorého sa táto Zmluva týka.

12.5 Dodávateľ je povinný do piatich pracovných dní odo dňa uzatvorenia zmluvy so subdodávateľom, alebo v deň nástupu subdodávateľa (podľa toho, ktorá skutočnosť nastane neskôr), preukázať Objednávateľovi, že tento subdodávateľ spĺňa podmienky účasti podľa § 26 ods. 1 zákona o verejnom obstarávaní. Zároveň je Dodávateľ povinný aktualizovať zoznam subdodávateľov, ktorý je Prílohou č. 8 tejto Zmluvy.

12.6 Ak sa na subdodávateľa vzťahuje povinnosť zapisovať sa do Registra partnerov verejného sektora podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Dodávateľ je sa zaväzuje zabezpečiť splnenie tejto povinnosti všetkými jeho subdodávateľmi po celú dobu trvania tejto Zmluvy. V prípade, ak počas plnenia tejto Zmluvy dôjde k právoplatnému výmazu niektorého subdodávateľa z registra partnerov verejného sektora, je Dodávateľ povinný okamžite ukončiť plnenie tejto Zmluvy prostredníctvom takéhoto subdodávateľa.

12.7 Porušenie povinností Dodávateľa uvedených v tomto článku Zmluvy sa považuje za podstatné porušenie zmluvných povinností.

Článok XIII.
Osobitné ustanovenia o výkone kontroly

13.1 Dodávateľ je povinný strpieť a umožniť výkon kontroly/auditu súvisiaceho s dodávaným predmetom plnenia, ako aj s ostatnými ustanoveniami tejto zmluvy zo strany osôb oprávnených na výkon kontroly, kedykoľvek po uzavretí tejto Zmluvy a počas platnosti a účinnosti Zmluvy o nenávratnom finančnom príspevku č. Z311071CLH1 (cez NTS SR č. 8/23; cez MIRRI SR: 181/2023) uzavretej medzi poskytovateľom nenávratného finančného príspevku a Objednávateľom dňa 08.02.2023, pričom oprávnenými osobami sú najmä:

a) Poskytovateľ nenávratné finančného príspevku a ním poverené osoby,
b) Útvar vnútorného auditu Riadiaceho orgánu alebo Sprostredkovateľského orgánu a nimi poverené osoby,
c) Najvyšší kontrolný úrad SR a ním poverené osoby,
d) Orgán auditu, jeho spolupracujúce orgány (Úrad vládneho auditu) a osoby poverené na výkon kontroly/auditu,
e) Splnomocnení zástupcovia Európskej Komisie a Európskeho dvora audítorov,
f) Orgán zabezpečujúci ochranu finančných záujmov EÚ,
g) Osoby prizvané orgánmi uvedenými v písmenách a) až f) v súlade s príslušnými právnymi predpismi SR a právnymi aktmi EÚ.

13.2 Dodávateľ sa zaväzuje poskytnúť osobám oprávneným na výkon kontroly špecifikovaným v bode 13.1 tohto Článku Zmluvy, všetku potrebnú súčinnosť. V prípade, že v dôsledku kontroly vykonanej oprávneným orgánom, dôjde zavinením Dodávateľa k uznaniu plnenia predmetu zmluvy ako neoprávneného výdavku, t.j. výdavku, ktorý nezodpovedá cenám bežným na trhu v čase ich vzniku a v mieste ich vzniku, a ktorý preto nebude Objednávateľovi uznaný ako oprávnený, je Dodávateľ povinný nahradiť kupujúcemu v plnom rozsahu škodu, ktorá mu v dôsledku tejto skutočnosti vznikne.

13.3 Dodávateľ bude rešpektovať právo osôb oprávnených na výkon kontroly podľa bodu 13.1 tohto Článku Zmluvy vstupovať do objektov, ak to súvisí s predmetom tejto Zmluvy a požadovať od Dodávateľa predloženie originálnych dokladov a inú potrebnú dokumentáciu, alebo iné ďalšie doklady súvisiace s touto Zmluvou.

13.4 Dodávateľ za zaväzuje prijať opatrenia na nápravu nedostatkov zistených kontrolou, overovaním na mieste v zmysle Správy z kontroly, v lehote stanovenej osobami oprávnenými na výkon kontroly podľa bodu 13.1 tohto Článku Zmluvy, a zároveň zaslať kupujúcemu informáciu o splnení opatrení prijatých na nápravu zistených nedostatkov bezodkladne po ich splnení.

Článok XIV.
Skončenie zmluvy

14.1 Pred splnením Zmluvy je možné Zmluvu ukončiť:
a) písomnou dohodou Zmluvných strán,
b) odstúpením v prípadoch uvedených vo všeobecne záväzných právnych predpisoch a v tejto Zmluve.

14.2 Objednávateľ je oprávnený odstúpiť od Zmluvy okrem iného v prípade, ak Dodávateľ podá na seba návrh na vyhlásenie konkurzu alebo návrh na povolenie reštrukturalizácie, alebo ak bude na majetok Dodávateľa vyhlásený konkurz alebo povolená reštrukturalizácia na základe návrhu ktorejkoľvek tretej osoby, alebo ak je zamietnutý návrh na vyhlásenie konkurzu pre nedostatok majetku, alebo pokiaľ sa stane zrejmým, že Dodávateľ nie je ďalej schopný plniť túto Zmluvu z dôvodu straty oprávnenia potrebného na plnenie tejto Zmluvy. Uvedené skutočnosti je Dodávateľ bezodkladne povinný oznámiť druhej zmluvnej strane.

14.3 Zmluvné strany sa dohodli, že za podstatné porušenie Zmluvy budú považovať najmä:
14.3.1 na strane Objednávateľa:
a) omeškanie s poskytnutím potrebnej súčinnosti potrebnej pre plnenie povinností Dodávateľa podľa tejto Zmluvy a túto súčinnosť neposkytne ani v dodatočnej lehote poskytnutej Dodávateľom v dĺžke najmenej 30 dní,
b) opakované omeškanie s úhradou splatných faktúr Dodávateľa o viac ako 120 dní odo dňa splatnosti faktúry,
14.3.2 na strane Dodávateľa:
a) také porušenie povinností Dodávateľa, ktoré je v Zmluve výslovne označené ako podstatné porušenie Zmluvy,
b) opakované porušenie povinnosti Dodávateľa dodržať reakčný čas alebo odstrániť kritickú alebo naliehavú vadu podľa Tabuľky 1 Prílohy č. 4 tejto Zmluvy, ktoré nastane najmenej päťkrát v priebehu troch (3) kalendárnych mesiacov nasledujúcich po sebe,

c) porušenie povinnosti mlčanlivosti,
d) skončenie Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

14.4 Odstúpenie od Zmluvy musí byť písomné, s uvedením dôvodu odstúpenia v súlade so všeobecne záväznými právnymi predpismi alebo touto Zmluvou a zaslané formou doporučeného listu druhej zmluvnej strane. Účinky odstúpenia od Zmluvy nastávajú dňom jeho doručenia druhej zmluvnej strane.

14.5 V prípade odstúpenia od Zmluvy sú zmluvné strany povinné vrátiť si všetky poskytnuté plnenia do 10 dní od účinnosti odstúpenia od Zmluvy; uvedené neplatí v prípade, ak dôjde k odstúpeniu od Zmluvy po dodaní diela v časti poskytovania služieb podpory a údržby, pri ktorom je Dodávateľ povinný vrátiť časť ceny za predmet plnenia zodpovedajúcu týmto službám.

14.6 Zánik tejto Zmluvy nemá vplyv na platnosť ustanovení tejto Zmluvy pri ktorých je výslovne uvedené, že zostávajú v platnosti aj po skončení tejto Zmluvy alebo u ktorých z povahy a účelu alebo zo všeobecne záväzných právnych predpisov vyplýva, že majú zostať v platnosti aj po skončení tejto Zmluvy, najmä, nie však výlučne, ustanovení o náhrade škody, zmluvnej pokute, autorských právach alebo mlčanlivosti.

Článok XV.
Spoločné a záverečné ustanovenia

15.1 Táto Zmluva je platná dňom jej podpisu oboma zmluvnými stranami. Táto Zmluva nadobúda účinnosť po splnení odkladacej podmienky nadobudnutia účinnosti Zmluvy podľa bodu 15.2 nižšie, nie však skôr ako dňom nasledujúcim po dni jej prvého zverejnenia v súlade so zákonom č. 546/2010 Z.z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

15.2 Odkladacia podmienka nadobudnutia účinnosti zmluvy: Zmluva nadobudne účinnosť až po schválení procesu verejného obstarávania poskytovateľom nenávratného finančného príspevku – dňom vydania správy z kontroly procesu verejného obstarávania. Ak výsledok predmetnej kontroly verejného obstarávania nebude kladný, nie je splnená podmienka k nadobudnutiu účinnosti Zmluvy. Z uvedeného dôvodu k plneniu Zmluvy nemôže dôjsť skôr, ako sa Zmluva stane účinnou. Po doručení správy z kontroly verejného obstarávania Objednávateľ bezodkladne upozorní na túto skutočnosť Dodávateľa.

15.3 Ak v momente uzatvorenia Zmluvy nemá Dodávateľ v Registri partnerov verejného sektora vedenom Ministerstvom spravodlivosti SR zapísaných svojich konečných užívateľov výhod, pričom v súlade s príslušnými ustanoveniami zákona č. 315/2016 Z.z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov má takúto povinnosť, Zmluva nadobudne účinnosť najskôr v deň zápisu konečných užívateľov výhod Dodávateľa do tohto registra. Ak zápisu do tohto registra nedôjde ani do 30 dní odo dňa uzatvorenia Zmluvy, Objednávateľ je oprávnený od tejto Zmluvy odstúpiť. Dodávateľ je povinný byť zapísaný v Registri partnerov verejného sektora po celú dobu trvania Zmluvy.

15.4 Dodávateľ nie je oprávnený postúpiť akúkoľvek svoju pohľadávku z tejto Zmluvy na tretiu osobu bez predchádzajúceho písomného súhlasu Objednávateľa. Písomný súhlas Objednávateľa s týmto úkonom je zároveň platný len za podmienky, že bol na tento úkon udelený predchádzajúci písomný súhlas Ministerstva zdravotníctva SR. Právny úkon, ktorým budú postúpené pohľadávky Dodávateľa v rozpore s týmto ustanovením je podľa § 39 zákona č. 40/1964 Zb. – Občiansky zákonník v znení neskorších predpisov neplatný.

15.5 Zmluvné strany sa zaväzujú uzatvoriť spoločne s touto Zmluvou aj Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností uvedenú v Prílohe č. 9 k tejto Zmluve.

15.6 Meniť alebo dopĺňať obsah tejto Zmluvy je možné iba formou písomných dodatkov, ktoré budú platné, ak budú riadne potvrdené a podpísané oprávnenými zástupcami oboch Zmluvných strán.

15.7 Zásady ochrany osobných údajov sú uvedené na webovej stránke: http://www.ntssr.sk/zasadyochranyudajov/ochrana-osobnych-udajov-zmluvnych-partnerov-osob-opravnenych-konat-v-mene-zmluvnych-partnerov-a-zastupcov-zmluvnych-partnerov.

15.8 Právne vzťahy touto Zmluvou neupravené sa riadia slovenským právom, najmä príslušnými ustanoveniami zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

15.9 Táto Zmluva nahrádza každú písomnú alebo ústnu dohodu medzi zmluvnými stranami ohľadne predmetu tejto Zmluvy.

15.10 Neoddeliteľnou súčasťou tejto Zmluvy sú jej prílohy:

a) Príloha č. 1 – Špecifikácia predmetu plnenia vo vzťahu k vypracovaniu návrhov a smerníc na základe odporúčaní Auditu
b) Príloha č. 2 – Špecifikácia predmetu plnenia vo vzťahu k dodávke softvérového a hardvérového zabezpečenia
c) Príloha č. 3 – Špecifikácia predmetu plnenia vo vzťahu k implementácii riešenia pre jednotlivé lokality
d) Príloha č. 4 – Podmienky poskytovania služieb podpory a údržby (SLA)
e) Príloha č. 5 – Špecifikácia predmetu plnenia vo vzťahu k dvojfaktorovej autentifikácii
f) Príloha č. 6 – Štruktúra ceny za predmet plnenia
g) Príloha č. 7 – Harmonogram prác
h) Príloha č. 8 – Zoznam subdodávateľov
i) Príloha č. 9 – Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
j) Príloha č. 10 – Miesta realizácie

15.11 Táto Zmluva je vyhotovená v štyroch vyhotoveniach s platnosťou originálu. Dodávateľ aj Objednávateľ obdržia každý po dve vyhotovenia tejto Zmluvy.

15.12 Zmluvné strany vyhlasujú, že si túto Zmluvu prečítali, jej obsahu porozumeli a súhlasia s ním a že Zmluvu uzatvárajú slobodne, vážne a bez nátlaku, na znak čoho pripájajú svoje podpisy.

V Bratislave, dňa _

Národná transfúzna služba SR
Ing. Ivan Oleár, MBA,
riaditeľ

V Bratislave, dňa

Mgr. Iveta Gáľová
konateľ

Špecifikácia predmetu plnenia vo vzťahu k vypracovaniu návrhov a smerníc na základe odporúčaní Auditu

Požiadavka č.:	Vyhl. 362/2018 Z.z.	Opatrenie z auditu KB	Popis výstupu
O-0002	§ 2 Obsah a štruktúra bezpečnostnej dokumentácie	Zadefinovať vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení	vypracovanie plánu implementácie bezpečnostných opatrení podľa požiadaviek ZoKB a ZoITVS a príslušných vyhlášok
O-0017	§ 6 Riadenie aktív, hrozieb a rizík	Dopracovať do výstupného listu checklist, aby neprišlo k opomenutiu niektorých položiek a tiež písomne spracovať proces vrátenia aktív a odobratia prístupov pre dodávateľa.	vypracovanie návrhu smernic Požiadavky pre tretie strany - Bezpečnostné opatrenia
O-0023	§ 7 Personálna bezpečnosť	Dopracovať do výstupného listu checklist, aby neprišlo k opomenutiu niektorých položiek a tiež písomne spracovať proces vrátenia aktív a odobratia prístupov pre dodávateľa.	
O-0020	§ 7 Personálna bezpečnosť	Doplniť poučenie o podstatné povinnosti z oblasti informačnej a kybernetickej bezpečnosti alebo doplniť poučenie o oboznámenie so Smernicou o informačnej a kybernetickej bezpečnosti	-----
O-0021	§ 7 Personálna bezpečnosť	Stanoviť stratégiu vzdelávania v oblasti informačnej a kybernetickej bezpečnosti a zabezpečiť je zavedenie do praxe	vypracovanie plánu rozvoja bezpečnostného povedomia zamestnancov, návrh obsahu vzdelávania pre vstupné a periodické školenia pre bežných užívateľov a administrátorov
O-0022	§ 7 Personálna bezpečnosť	Zabezpečiť v nadväznosti na pravidelné preškolenie zamestnancov overenie efektívnosti vzdelávania	vypracovanie vzorového testu pre overovanie znalostí a bezpečnostného povedomia zamestnancov
O-0055	§ 13 Systém správy kryptografických kľúčov a certifikátov	Určiť pravidlá kryptografickej ochrany v kryptografickom štandarde podľa výsledkov analýzy rizík a technických možností komponentov v infraštruktúre. Na základe štandardu následne vyžadovať a implementovať opatrenia súvisiace s kryptografiou. Osobitnú pozornosť odporúčame venovať protokolom, ktoré prenášajú užívateľské identifikátory a heslá v cleartexte (TELNET, FTP, HTTP atď.).	vypracovanie návrhu smernice Správa a prevádzka IS_admin
O-0056	§ 13 Systém správy kryptografických kľúčov a certifikátov	Do zoznamu interných kontrol zaviesť povinnosť kontroly nastavenia systému správy kryptografických kľúčov a certifikátov ako na internej CA, tak na certifikátoch inštalovaných externými partnermi.	Vypracovanie vzorového Audit check listu pre interné audity/kontroly
O-0003	§ 3 Bezpečnostná stratégia kybernetickej bezpečnosti	Vypracovanie bezpečnostnej stratégie kybernetickej bezpečnosti.	vypracovanie návrhu Stratégie kybernetickej bezpečnosti

O-0009	§ 5 organizácie kybernetickej bezpečnosti	Stanoviť formu a periodicitu pravidelného informovania vedenia a štatutárneho orgánu a využívať ju na pravidelné alebo jednorazové informovanie alebo predkladanie návrhov	vypracovanie návrhu Politiky informačnej bezpečnosti
O-0010	§ 5 organizácie kybernetickej bezpečnosti	Rozpracovať spôsob napĺňania povinností vyplývajúcich z dekrétu a zavedených bezpečnostných politík	
O-0011	§ 5 organizácie kybernetickej bezpečnosti	Zaviesť kompenzačné opatrenia, ktoré zabezpečia primeranú nezávislosť alebo vyčleniť pozíciu manažéra pre kybernetickú bezpečnosť mimo odboru informatiky	
O-0012	§ 5 organizácie kybernetickej bezpečnosti	Zadefinovať politiku kontrolných činností, vypracovať plán ich vykonávania a proces vyhodnocovania efektívnosti vykonávaných činností a prijatých opatrení	
O-0004	§ 3 Bezpečnostná stratégia kybernetickej bezpečnosti	Spracovať zoznam aktív a vypracovať nad ním analýzu rizík so zohľadnením hodnoty aktíva pre základnú službu. Odporúčanie: spracovať Zoznam aktív a vypracovať nad ním analýzu rizík so zohľadnením hodnoty aktíva pre základnú službu	Vypracovanie návrhu smernice Klasifikácia, kategorizácia informačných aktív a Metodiky
O-0007	§ 4 Klasifikácia informácií a kategorizácia sietí a informačných systémov	Vykonať klasifikáciu informácií a kategorizáciu sietí a informačných systémov podľa § 20 ods. 2. pre všetky informačné systémy, ktoré majú priamy alebo nepriamy vplyv na prevádzkovanú základnú službu	Konzultácie, zaškolenie, vykonanie klasifikácie infirmácií a kategorizácii IS a sietí (vyplnenie katalógu aktív)
O-0013	§ 6 Riadenie aktív, hrozieb a rizík	Spracovať zoznam aktív a vypracovať nad ním analýzu rizík so zohľadnením hodnoty aktíva pre základnú službu	
O-0013	§ 6 Riadenie aktív, hrozieb a rizík	Spracovať zoznam aktív s uvedením požadovaných parametrov a u jednotlivým aktív identifikovať , či sa podieľajú na poskytovaní základnej služby alebo sa jedná o podporné služby alebo ostatné aktíva	
O-0016	§ 6 Riadenie aktív, hrozieb a rizík	Spracovať zoznam aktív a u jednotlivým aktív identifikovať vlastníka rizika a vlastníka aktíva	
O-0018	§ 6 Riadenie aktív, hrozieb a rizík	Dopracovať proces riadenia rizík o hrozby, zraniteľnosti a ich ohodnotenie, a vykonať nad nimi analýzu rizík v súlade s prijatou metodikou, ale zameranú podrobne na IS	Vypracovanie Metodiky riadenia rizík, Vykonanie analýzy rizík na základe katalógu aktív, Konzultácie a navrhnutie procesných a technických bezpečnostných opatrení na zníženie rizík (Plán zvládania rizík)
O-0019	§ 6 Riadenie aktív, hrozieb a rizík	Dopracovať proces riadenia rizík o hrozby, zraniteľnosti a ich ohodnotenie, a vykonať nad nimi analýzu funkčného dopadu (BIA).	Vypracovanie Analýzy funkčného dopadu (BIA) na vyhodnotenie dopadu na činnosť prevádzkovateľa základnej služby
O-0059	§ 14 Riešenie kybernetických bezpečnostných incidentov	Príprava a vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov.	vypracovanie návrhu smernice o Riešení bezpečnostných incidentov
O-0062	§ 14 Riešenie kybernetických bezpečnostných incidentov	Stanovenie opatrení na odvrátenie alebo zmiernenie dopadu kybernetického bezpečnostného incidentu	

O-0063	§ 14 Riešenie kybernetických bezpečnostných incidentov	Vedenie záznamov o kybernetických bezpečnostných incidentoch vrátane použitých riešení v service desk nástroji resp. ticketovacom systéme.	
O-0064	§ 14 Riešenie kybernetických bezpečnostných incidentov	Formalizovať postup prešetrovania a určenia príčin vzniku kybernetického bezpečnostného incidentu.	
O-0065	§ 14 Riešenie kybernetických bezpečnostných incidentov	Doplnenie definície primeranosti pri prijímaní bezpečnostných opatrení, ktoré zamedzujú opakovanému výskytu vzniku kybernetického bezpečnostného incidentu.	
O-0038	§ 11 Riadenie bezpečnosti prevádzky siete a informačného systému	Zadefinovanie postupov riadenia záplat a aktualizácií pre všetky prevádzkované informačné systémy, vrátane podpornej infraštruktúry.	vypracovanie návrhu smernice o Správe a prevádzke informačných systémov_administráror
O-0039	§ 11 Riadenie bezpečnosti prevádzky siete a informačného systému	Zadefinovať formálne pravidlá riadenia kapacít, monitoring kapacít naprieč informačnými systémami a implementácia monitorovacieho nástroja	
O-0041	§ 11 Riadenie bezpečnosti prevádzky siete a informačného systému	Zadefinovanie pravidiel a postupov ochrany pred škodlivým kódom na všetkých informačných systémoch a technologických celkoch ak to daná technológia umožňuje. Odobratie administrátorských práv koncovým používateľom.	
O-0042	§ 11 Riadenie bezpečnosti prevádzky siete a informačného systému	Zadefinovanie pravidiel a postupov na inštaláciu software na zariadeniach, odobratie nadbytočných admin práv užívateľov	
O-0043	§ 11 Riadenie bezpečnosti prevádzky siete a informačného systému	Zadefinovanie pravidiel a postupov na inštaláciu zariadení v sieťach a informačných systémoch, vynucovanie týchto pravidiel u dodávateľov. Zváženie dodatočných opatrení vo forme deaktivovania nepoužívaných portov na switchoch, prípadne port-sčeríte či 802.1X.	
O-0040,	§ 11 Riadenie bezpečnosti prevádzky siete a informačného systému	Zadefinovanie pravidiel a postupov pravidelného zálohovania, implementácia software na zálohovanie všetkých informačných systémov podľa požadovaného parametru RPO pre všetky informačné systémy a podporné aktíva, pravidelné testovanie obnovy informácií zo záloh	Vypracovanie návrhu smernice pre Zálohovanie a archivácia, vypracovanie návrhu smernice Stratégie zálohovania, vypracovanie vzoru zálohovacej matice, Konzultácie k vyplneniu zálohovacej matice
O-0047	§ 12 Riadenie prístupov osôb k sieti a informačnému systému	Zadefinovanie pravidiel riadenia prístupu k sieťam, implementácia segmentácie siete, vypnutie nepoužívaných portov na manažovaných LAN switchoch, zváženie implementácie L2 bezpečnostných prvkov (port security, DHCP snooping, Dynamic ARP inspection atď.).	vypracovanie návrhu smernice o Riadení prístupových práv
O-0024	§ 8 Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov	Pri rokovaní s dodávateľmi pri akvizícii IS alebo jeho vývoja rokovať súčasne aj o zmluve o plnení povinností vyplývajúcich so ZoKB	vypracovanie návrhu zmluvy pre dodávateľa základnej služby
O-0025	§ 8 Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov	Vykonať kontrolu jednotlivých zmluvných vzťahov s dodávateľmi, identifikovať všetkých dodávateľov, s ktorými je potrebné uzatvoriť zmluvy o plnení povinností vyplývajúcich so ZoKB a dorokovať ich	Konzultácia k identifikácii dodávateľov, s ktorými je potrebné uzatvoriť zmluvy o plnení bezpečnostných opatrení vyplývajúcich zo ZoKB.

O-0071	§ 17 Zabezpečenie kontinuity riadenia kybernetickej bezpečnosti	Spracovať politiku pre BCM. Podľa analýzy funkčného dopadu (BIA) vypracovať BCP, DRP a ich pravidelné testovanie a aktualizáciu	Vypracovanie návrhu smernice pre Riadenie kontinuitu činnosti (BCM Plány kontinuty činnosti), Vypracovanie Stratégia a plánu obnovy (DRP Plány obnovy),
O-0073	§ 17 Zabezpečenie kontinuity riadenia kybernetickej bezpečnosti	Stanoviť frekvenciu a rozsah zálohovania pre každý informačný systém.	Vypracovanie Smernice pre zálohovanie a obnovu IS, Požiadavky na obnovu IS zo záloh - vzor Záznam o vykonaní testu obnovy IS z prevádzkovej zálohy - vzor Vypracovanie Stratégie kontinuity a obnovy Konzultácie k určenie cieľovej doby a cieľového bodu obnovy (RTO,RPO), MTO
O-0073	§ 17 Zabezpečenie kontinuity riadenia kybernetickej bezpečnosti	Určenie osoby zodpovednej za zálohovanie pre každý informačný systém.	
O-0075	§ 17 Zabezpečenie kontinuity riadenia kybernetickej bezpečnosti	Stanoviť časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní pre každý informačný systém	
O-0076	§ 17 Zabezpečenie kontinuity riadenia kybernetickej bezpečnosti	Vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.	

V Bratislave, dňa

.....

podpis (štatutár alebo splnomocnená osoba)
Mgr. Iveta Gaľová – konateľ

Špecifikácia predmetu plnenia vo vzťahu k dodávke softvérového a hardvérového zabezpečenia

Implementácia firewallow a dvojfaktorovej autentifikácie do siete NTSSR

Tento návrh sa zaoberá nasadením firewallow vo všetkých lokalitách za účelom celkového zvýšenia bezpečnosti siete a zabezpečením súladu so ZoKB a odporúčaniami auditu. Prostredníctvom firewallow sa vykoná segmentácia sietí na všetkých lokalitách a riadenie prístupov medzi jednotlivými segmentami s centrálnou správou. Ich dôslednou konfiguráciou budú naplnené nasledovné odporúčania auditu:

O-0008 - § 4 - Dôsledná segmentácia siete, kategorizácia a určenie bezpečnostných zón na firewalle.
O-0028 - § 10 - Implementácia segmentácie prostredníctvom VLAN v každej lokalite, oddelenie jednotlivých typov zariadení (server, klientska stanica, tlačiareň...) do samostatných sieťových segmentov, nastavenie riadených prestupov prostredníctvom firewallu a granulárne nastavených pravidiel.
O-0029 - § 10 - Dôsledná segmentácia siete a umiestňovanie serverov so službami priamo prístupnými z externých sietí do dedikovaných DMZ segmentov.
O-0030 - § 10 - Implementácia segmentácie siete a umiestňovanie serverov do segmentov v závislosti od bezpečnostných požiadaviek a účelov.
O-0031 – § 10 - Implementácia segmentácie siete vo všetkých lokalitách a zabezpečenie prepojenia jednotlivých segmentov prostredníctvom firewallu.
O-0032 – § 10 - Segmentácia siete a povoľovanie spojní na základe princípu zásady najnižších privilégií
O-0033 - § 10 - Implementácia segmentácie a povoľovanie len špecifikovaných služieb na firewalle

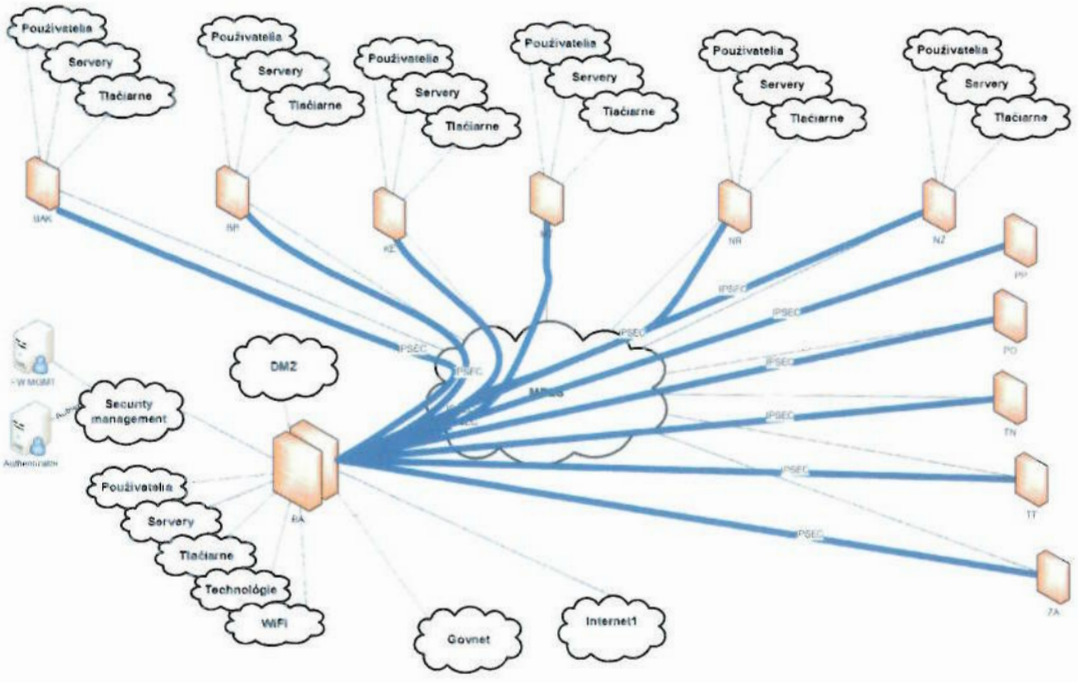
Čiastočne pokryté bude aj opatrenie č 44, nakoľko všetky sieťové spojenia budú zaznamenávané firewallmi a záznamy budú centrálne ukladané na logserveri.
O-0044 - § 11 - Implementácia centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systém

Do siete bude implementovaný systém pre silnú dvojfaktorovú autentifikáciu a tento bude integrovaný so vzdialeným prístupom. Nasadením 2FA a následnou rekonfiguráciou pristupov budú naplnené nasledovné odporúčania auditu:

O-0035 - § 10 - Implementácia dvojfaktorovej autentizácie pri vzdialenom prístupe do internej siete.
O-0036 - § 10 - Identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti
O-0050 - § 12 - Riadenie vzdialeného prístupu formou zriadenia VPN prístupov pre dodávateľov.

Návrh riešenia

Navrhované riešenie počíta s využitím a rozšírením existujúceho riešenia. Súčasne používané firewally na riaditeľstve budú nahradené výkonnejšími modelmi. Existujúce zariadenia sa použijú na lokalitách. Ostatné lokality budú osadené tiež rovnakými modelmi. Riaditeľstvo bude mať firewally vo vysokodostupnom zapojení, na lokalitách budú bez vysokej dostupnosti, dostupnosť bude zabezpečená dodávateľskou SLA. High level dizajn navrhovanej topológie je na nasledujúcom obrázku. Presný zoznam segmentov vrátane IP plánu bude predmetom detailného dizajnu.



Požiadavky na HW zariadenie a manažment:

Počet zariadení: 2

Požiadavka č.	Parameter	Hodnota (áno/nie)
1	Požadované funkcionality: Firewall, IPS, Aplikačná kontrola+URL filtering, Malware a Botnet ochrana, HTTPs inšpekcia, DLP a ochrana proti Zero-day malware	áno
2	Okamžite použitelné preddefinované IPS politiky	áno
3	Možnosť definície IPS výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
4	Možnosť nastavenia monitorovacieho alebo blokovacieho režimu IPS globálne, na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry	áno
5	Možnosť konfigurácie a ladenia IPS engine priamo z log výstupov firewallu	áno
6	Nové signatúry IPS musia byť viditelne označené a musia byť aktivované iba v detekčnom režime	áno
7	Detekcia/blokovanie šírenia škodlivého kódu (malware)	áno
8	Minimálne podporované typy súborov pre dynamickú sandbox emuláciu:powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z, rar)	áno
9	Podporovaná veľkosť emulovaných súborov v sandbox, min. 80MB	áno
10	Možnosť definície Antivirus výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
11	Riadenie politky na základe užívateľských skupín z Active Directory	áno
12	Ochrana proti SNI spoofing v rámci HTTPs inspekce	áno
13	Podpora plnohodnotné HTTPS inspekce pre HTTPS, IMAPS,POP3S	áno
14	Možnosť granulárneho riadenie HTTPs (inšpekcia spojenia alebo bypass) - podľa kombinácie: aplikácia / URL / URL kategória	áno
15	Možnosť vypnutie HTTPS inspekcie pre Wifi	áno
16	Zariadenie musí byť schopné vyčítať identity priamo z doménového kontroleru bez nutnosti inštalovať akúkoľvek externú komponentu	áno
17	Podpora IPSec VPN tunelov	áno
18	VPN IPSec musí podporovať nasledujúce šifrovacie protokoly: AES-128, AES-256, CAST, DES	áno
19	VPN IPSec musí podporovať dátovú integritu pre MD5, SHA1, SHA-256, AES-XCBC	áno
20	Riešenie musí podporovať IP compression pre S2S VPN	áno
21	Podpora Remote Access VPN pre 500 používateľov - vrátane licencie	áno
22	Priepustnost Firewallu, minimálne 17000 Mbps (RFC 3511, 2544, 2647, 1242)	áno
23	Priepustnost Threat prevention, minimálne 2 Gbps (FW, IPS, Threat ochrana, APPC)	áno
24	Počet nových spojení za sekundu (CPS) minimálne 65.000	áno
25	Počet súčasných spojení, min. 2.400.000	áno
26	Fanless - bez aktivných chladiacich komponent.	áno
27	Maximálna hodnota BTU 320 za hodinu	áno
28	Počet fyzických sieťových rozhraní, mín. 16x 10/100/1000	áno
29	min. 2x 2.5GbE optický port	áno
	duálne WAN porty - 2x1Gbps	áno
30	podpora alespon 1x 10Gbps SFP+	áno
31	Dedikovaný management port RJ45 1x1Gbps	áno
32	Duálne zdroje napájenia	áno
33	Storage min 250GB SSD	áno
34	2x USB port 3.0	áno
35	1x USB-C vrátane RJ-45 console port	áno
36	Podpora slotu pre formát microSD memory karet do velkosti 64 GB	áno

37	Maximálna spotreba energie 36W	áno
38	Riešenie musí byt uvedené v Gartner Enterprise Firewall Magic Quandrant, každý rok za posledné 3 roky (2019,2020,2021) v kvadrante Leader	áno
39	Podpora vysokej dostupnosti Active-Standby	áno
40	Failover cluster time maximálne 1s	áno
41	Podpora debuggovania problémových scenárov na úrovni L2 - L7	áno
42	Podpora linux nástrojov (min. SCP, BASH, VI, TOP), spúšťania linuxových BASH skriptov a nástrojov tretích stran	áno
43	Riešenie musí podporovať možnosť obnovenia predchádzajúceho OS image (revert) a z lokálneho úložiska	áno
44	Inštalácia dvoch zariadení do standardného 19" kabinetu 1U (velikosť boxu maximálně desktop standard size - 210 x 170 x 45mm)	áno
45	Zero touch deployment (nastavenie prvotnej konfigurácie z USB flash)	áno
46	Dodávaná firewall platforma musia byt vo forme samostatnej fyzickej hardware appliance	áno
47	Podpora lokálného aj centrálného managementu jednotného pre oba typy zariadení	áno
48	Podpora mobilné aplikácie pro remote management	áno
49	Podpora DynDNS a reach my device.	áno
50	Cloud management v cene zariadení	áno
51	Remote Access licencie musí byť súčasťou licencie zariadení.	áno

V Bratislave, dňa

.....

podpis (štatutár alebo splnomocnená osoba)
Mgr. Iveta Gaľová – konateľ

Špecifikácia predmetu plnenia vo vzťahu k implementácii riešenia pre jednotlivé lokality

Počet zariadení: 2

Požiadavka č.	Parameter	Hodnota (áno/nie)
1	Požadované funkcionality: Firewall, IPS, Aplikačná kontrola+URL filtering, Malware a Botnet ochrana, HTTPs inšpekcia, DLP a ochrana proti Zero-day malware	áno
2	Okamžite použitelné preddefinované IPS politiky	áno
3	Možnosť definície IPS výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
4	Možnosť nastavenia monitorovacieho alebo blokovacieho režimu IPS globálne, na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry	áno
5	Možnosť konfigurácie a ladenia IPS engine priamo z log výstupov firewallu	áno
6	Nové signatúry IPS musia byť viditelne označené a musia byť aktivované iba v detekčnom režime	áno
7	Detekcia/blokovanie šírenia škodlivého kódu (malware)	áno
8	Minimálne podporované typy súborov pre dynamickú sandbox emuláciu:powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z, rar)	áno
9	Podporovaná veľkosť emulovaných súborov v sandbox, min. 80MB	áno
10	Možnosť definície Antivirus výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
11	Riadenie politky na základe užívateľských skupín z Active Directory	áno
12	Ochrana proti SNI spoofing v rámci HTTPs inspekce	áno
13	Podpora plnohodnotné HTTPS inspekce pre HTTPS, IMAPS,POP3S	áno
14	Možnosť granulárneho riadenie HTTPs (inšpekcia spojenia alebo bypass) - podľa kombinácie: aplikácia / URL / URL kategória	áno
15	Možnosť vypnutie HTTPS inspekcie pre Wifi	áno
16	Zariadenie musí byť schopné vyčítať identity priamo z doménového kontroleru bez nutnosti inštalovať akúkoľvek externú komponentu	áno
17	Podpora IPSec VPN tunelov	áno
18	VPN IPSec musí podporovať nasledujúce šifrovacie protokoly: AES-128, AES-256, CAST, DES	áno
19	VPN IPSec musí podporovať dátovú integritu pre MD5, SHA1, SHA-256, AES-XCBC	áno
20	Riešenie musí podporovať IP compression pre S2S VPN	áno
21	Podpora Remote Access VPN pre 500 používateľov - vrátane licencie	áno
22	Priepustnost Firewallu, minimálne 17000 Mbps (RFC 3511, 2544, 2647, 1242)	áno
23	Priepustnost Threat prevention, minimálne 2 Gbps (FW, IPS, Threat ochrana, APPC)	áno
24	Počet nových spojení za sekundu (CPS) minimálne 65.000	áno
25	Počet súčasných spojení, min. 2.400.000	áno
26	Fanless - bez aktivných chladiacich komponent.	áno
27	Maximálna hodnota BTU 320 za hodinu	áno
28	Počet fyzických sieťových rozhraní, mín. 16x 10/100/1000	áno
29	min. 2x 2.5GbE optický port	áno
	duálne WAN porty - 2x1Gbps	áno
30	podpora alespon 1x 10Gbps SFP+	áno
31	Dedikovaný management port RJ45 1x1Gbps	áno
32	Duálne zdroje napájenia	áno
33	Storage min 250GB SSD	áno
34	2x USB port 3.0	áno
35	1x USB-C vrátane RJ-45 console port	áno

36	Podpora slotu pre formát microSD memory karet do velkosti 64 GB	áno
37	Maximálna spotreba energie 36W	áno
38	Riešenie musí byt uvedené v Gartner Enterprise Firewall Magic Quandrant, každý rok za posledné 3 roky (2019,2020,2021) v kvadrante Leader	áno
39	Podpora vysokej dostupnosti Active-Standby	áno
40	Failover cluster time maximálne 1s	áno
41	Podpora debuggovania problémových scenárov na úrovni L2 - L7	áno
42	Podpora linux nástrojov (min. SCP, BASH, VI, TOP), spúšťania linuxových BASH skriptov a nástrojov tretích stran	áno
43	Riešenie musí podporovať možnosť obnovenia predchádzajúceho OS image (revert) a z lokálneho úložiska	áno
44	Inštalácia dvoch zariadení do standardného 19" kabinetu 1U (velikosť boxu maximálně desktop standard size - 210 x 170 x 45mm)	áno
45	Zero touch deployment (nastavenie prvotnej konfigurácie z USB flash)	áno
46	Dodávaná firewall platforma musia byt vo forme samostatnej fyzickej hardware appliance	áno
47	Podpora lokálného aj centrálného managementu jednotného pre oba typy zariadení	áno
48	Podpora mobilné aplikácie pro remote management	áno
49	Podpora DynDNS a reach my device.	áno
50	Cloud management v cene zariadení	áno
51	Remote Access licencie musí byť súčasťou licencie zariadení.	áno

Počet zariadení: 10

Požiadavka č.	Parameter	Hodnota (áno/nie)
1	Požadované funkcionality: Firewall, IPS, Aplikačná kontrola+URL filtering, Malware a Botnet ochrana, HTTPs inšpekcia, DLP a ochrana proti Zero-day malware	áno
2	Okamžite použitelné preddefinované IPS politiky	áno
3	Možnosť definície IPS výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
4	Možnosť nastavenia monitorovacieho alebo blokovacieho režimu IPS globálne, na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry	áno
5	Možnosť konfigurácie a ladenia IPS engine priamo z log výstupov firewallu	áno
6	Nové signatúry IPS musia byť viditelne označené a musia byť aktivované iba v detekčnom režime	áno
7	Detekcia/blokovanie šírenia škodlivého kódu (malware)	áno
8	Minimálne podporované typy súborov pre dynamickú sandbox emuláciu:powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z, rar)	áno
9	Podporovaná veľkosť emulovaných súborov v sandbox, min. 80MB	áno
10	Možnosť definície Antivirus výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
11	Riadenie politky na základe užívateľských skupín z Active Directory	áno
12	Ochrana proti SNI spoofing v rámci HTTPs inspekce	áno
13	Podpora plnohodnotné HTTPS inspekce pre HTTPS, IMAPS,POP3S	áno
14	Možnosť granulárneho riadenie HTTPs (inšpekcia spojenia alebo bypass) - podľa kombinácie: aplikácia / URL / URL kategória	áno
15	Možnosť vypnutie HTTPS inspekcie pre Wifi	áno
16	Zariadenie musí byť schopné vyčítať identity priamo z doménového kontroleru bez nutnosť inštalovať akúkoľvek externú komponentu	áno
17	Podpora IPSec VPN tunelov	áno
18	VPN IPSec musí podporovať nasledujúce šifrovacie protokoly: AES-128, AES-256, CAST, DES	áno
19	VPN IPSec musí podporovať dátovú integritu pre MD5, SHA1, SHA-256, AES-XCBC	áno

20	Riešenie musí podporovať IP compression pre S2S VPN	áno
21	Podpora Remote Access VPN pre 200 používateľov integrovana v ramci licence boxu.	áno
22	Priepustnost Firewallu, minimálne 6 Gbps (RFC 3511, 2544, 2647, 1242)	áno
23	Priepustnost Threat prevention, minimálne 500 Mbps (FW, IPS, Threat ochrana, APPC)	áno
24	Počet nových spojení za sekundu (CPS) minimálne 15.000	áno
25	Počet súčasných spojení, min. 500.000	áno
26	Fanless - bez aktivných chladiacich komponent.	áno
27	Maximálna hodnota BTU 90 za hodinu	áno
28	Počet fyzických sieťových rozhraní, mín. 10x 10/100/1000	áno
29	Moznost SFP optickeho portu na WAN rozhranie	áno
30	Externý zdroj so závitom na ochranu proti nechtěnému odpojení.	áno
31	1x USB port 3.0	áno
32	1x USB-C console port	áno
33	Podpora slotu pre formát microSD memory karet	áno
34	Maximálna spotreba energie 25W	áno
35	Riešenie musí byt uvedené v Gartner Enterprise Firewall Magic Quandrant, každý rok za posledné 3 roky (2019,2020,2021) v kvadrante Leader	áno
36	Podpora vysokej dostupnosti Active-Standby	áno
37	Failover cluster time maximálne 1s	áno
38	Podpora debuggovania problémových scenárov na úrovni L2 - L7	áno
39	Podpora linux nástrojov (min. SCP, BASH, VI, TOP), spúšťania linuxových BASH skriptov a nástrojov tretích stran	áno
40	Riešenie musí podporovať možnosť obnovenia predchádzajúceho OS image (revert) a z lokálneho úložiska	áno
41	Inštalácia dvoch zariadení do standardného 19" kabinetu 1U (velikosť boxu maximálně desktop standard size - 210 x 160 x 38mm)	áno
42	Zero touch deployment (nastavenie prvotnej konfigurácie z USB flash)	áno
43	Dodávaná firewall platforma musia byt vo forme samostatnej fyzickej hardware appliance	áno
44	Podpora lokálneho aj centrálneho managementu jednotného pre oba typy zariadení	áno
45	Podpora mobilné aplikácie pro remote management	áno
46	Podpora DynDNS a reach my device.	áno
47	Cloud management v cene zariadení	áno
48	Remote Access licencie musí byť súčasťou licencie zariadení.	áno

Security manažment softvér počet: 25

Požiadavka č.	Parameter	Hodnota (áno/nie)
1	Management musí byť fyzicky oddelený od firewall platformy	áno
2	Jednotný centrálny management: správa politík a analýza logov na jednej konsolidovanej virtuálnej appliance (Hyper-V, ESXi) alebo hardware	áno
3	Management musí ukladať a zpracovávať logy zo všetkých firewallov, objem logov za deň min. 15 GB/deň	áno
4	Management log server musí spracovať min. 40.000 logov/sekundu	áno
5	Dlhodobé ukladanie historických log záznamov, min. interná kapacita úložiska 8TB	áno
6	Podpora administrátorských profilov pre delegáciu oprávnení (čítanie, zápis)	áno
7	Možnosť pridelenia práv administrátorom alebo API účtu len pre definovayný zoznam prístupných firewall pravidiel	áno

8	Zoskupovanie firewall pravidiel do logických skupín a pod-skupín na základe zdroja, cieľa, služby/aplikácie pre dlhodobú konzistenciu pravidiel	áno
9	Ochrana vzájomného ovplyvňovania alebo kolízie pri súčasnom pripojení viacero administrátorov pomocou zamykania individuálnych pravidiel a objektov	áno
10	Policy Tracer - vyhľadávanie firewall pravidla podľa kombinácie definovaných atribútov (min. zdrojová IP, cieľová IP, užívateľ, služba, aplikácia...)	áno
11	Kontrola politík proti chybám a duplicitám.	áno
12	Vizualizácia a prehľadávanie logov priamo v politike na vybranom pravidle (min. zdroj, cieľ, služba, aplikácia, užívateľ, čas)	áno
13	Zobrazenie histórie a zmien priamo v politike na vybranom pravidle (min,. Kto, aká zmena a kedy bola na pravidle uskutočnená)	áno
14	Prehľadávanie logov, min. podpora: "keyword" prehľadávanie, "field" prehľadávanie a "wildcard" prehľadávanie	áno
15	Práca s bezpečnostnými logmi - možnosť prehľadávania všetkých typov logov (fw, ips, malware) v jednej záložke s definovaním vlastných permanentných filtrov	áno
16	Rekonfigurácia a ladenie threat engine priamo z logov výstupov firewallu	áno
17	Logovaynie a historické prehľadávanie TCP stavových informácií k jednotlivým spojeniam v rámci centrálneho log servera (min. SYN, SYN.ACK, Established, FIN, FIN.ACK, RST)	áno
18	Intzegrovaný monitoring musí poskytovať grafické rozhranie pre sledovanie parametrov v reálnom čase a histórii aspoň 30 dní (využitie pamäti, CPU, počet naviazaných spojení, počet novo otvorených spojení za sekundu, priepustnosť, atď...).	áno
19	Podpora služby vlastnej certifikačnej autority pro vydávanie PKI certifikátov pre bezpečné prihlasovanie užívateľov a administrátorov a pre VPN klientský prístup	áno
20	Kontrola politiky podľa štandardov, min. ISO 27000 a GDPR (môže byť dodané produktom tretej strany)	áno
21	Integrácia na Cisco ISE cez rozhranie pxGrid	áno
22	Integrácia na Vmware vSphere, min. dynamické získavanie VM objektov a ich aplikácie vo firewalle politike	áno
23	Ak je management licencia obmedzená počtom riadených objektov bezpečnostných brán, musí podporovať riadenie min. 25 objektov brán	áno
24	Ak je management licencia obmedzená doskovou kapacitou, licencia pre min. 16TB musí byť súčasťou ponuky	áno
25	Priradenie povolenej či zakázanej aplikácie musí byť natívnou súčasťou vytvárania štandardného bezpečnostného pravidla bez nutnosti vytvárať profil	áno
26	Možnosť upgrade/update software firewallu, bezpečnostných update (IPS signatury, geolokačná databáza, apod.), knfigurácii atď. z grafického rozhrania managementu	áno
27	Možnosť posielať preddefinované reporty emailom. (podpora tiež autentizovaného SMTP pre komunikáciu s mail relay)	áno
30	Riešenie poskytuje dynamické objekty so zoznamom IP adries reprezentujúce externé služby typu Office365, Cloudové služby (AWS, Azure apod.), DropBox, ZOOM a ďalšie, a rôzne geografické lokality až na úrovni jednotlivých zemí.	áno
31	Možnosť použiť tieto dynamické objekty vo FW pravidlách, NAT pravidlách a definícii HTTPS inšpekcie	áno
32	Dynamické objekty sa musia automaticky aktualizovať bez nutnosti zásahu administrátora	áno

Endpoint- Ochrana pre koncové zariadenia

Popis	Počet
Pokročilá ochrana pred hrozbami pre koncové zariadenia. Ochrana koncových zariadení zahŕňa webovú ochranu, forenznú ochranu prístupu, emuláciu a extrakciu sandboxu. Navrhované riešenie by malo byť postavené na modulárnej architektúre, ktorá umožní zapnutie jednotlivých komponentov ochrany, aby mohlo byť kombinované s existujúcou bezpečnosťou na koncových bodoch, ktorá je už vlastnená. Navrhované riešenie musí umožňovať správcovi vytvorenie logickej skupiny naprieč niekoľkými funkčnými (AD) skupinami. Správca musí byť schopný riadiť politiku na úrovni užívateľa a skupiny. Schopnosť integrácie so službou Active Directory. Navrhované riešenie by malo vyžadovať inštaláciu programov alebo nástrojov s administratívnymi funkciami na pracovných koncových staniciach užívateľov. Koncoví užívatelia nesmú ovládať alebo meniť nastavenie, alebo meniť zásady zabezpečenia. Software alebo agenti nainštalovaný na užívateľských staniciach nesmú vyžadovať lokálne administrátorské práva k spusteniu. Koncoví užívatelia nesmú byť schopný obísť bezpečnostné zásady, aj keď majú práva miestnych správcov.	300

Navrhované riešenie musí mať zabudované kontroly, ktoré zabránia koncovím užívateľom vykonávať nasledujúce operácie na svojich pracovných staniciach. Politiky a citlivé informácie prenášané medzi serverom a pracovnou stanicou (agent) musia byť behom prenosu šifrované. Navrhovaný klient koncového bodu musí mať integraovanú funkciu IPSec VPN pre existujúci firewall. Riešenie mnusí podporovať tzv. Split Tunnelling, t.j. možnosť prístupu k internetovým stránkám mimo VPN, zatiaľ čo intranetová komunikácia je smerovaná do VPN tunela. Podporované overovanie musí obsahovať užívateľské meno / heslo alebo klientský certifikát. Musí byť možné používať jednorázové heslo (OTP) v spojení so štandardným užívateľským heslom (druhý faktor) vo forme SMS kódu. Musí byť prípadná podpora multifaktorovej autentizácie. Riešenie musí podporovať pripojenie VPN v prostredí za NAT zariadením a bránami firewall, ktoré neumožňujú IPSec spojenie (možnosť tunelovať VPN cez HTTPS). Navrhované riešenie musí byť schopné detekovať a odstrániť víry, spyware a ďalší malware na základe kombinácie signatúr, blokátorov chovania a heuristické. Navrhované riešenie by malo byť schopné detekovať a identifikovať prítomnosť vírusov v pamäti systému, bootovacích sektoroch, tabuľkách oddielov a na všetkých formách dát uložených na pevnom disku systému a iných vymeniteľných médiách. "Užívateľ by mal mať možnosť vykonať kontrolu vírusov na určitých jednotkách, adresároch alebo súboroch. Kontrola vírusov by mala byť vykonávaná v reálnom čase a mala by byť aktivovaná na vyžiadanie. Skenovanie vírusov by malo mať minimálny vplyv na výkon pracovnej stanice / notebooku." Navrhované riešenie musí detekovať a zablokovať akýkoľvek pokus o infekciu známym malwarom. Po zistení malwaru musí navrhované riešenie informovať používateľa o pokuse o infekciu vírusom. Navrhované riešenie by tiež malo byť schopné vykonať nápravné opatrenia na odstránenie vírusového kódu z infikovaných súborov, zavádzacích sektorov alebo tabuliek oddielov. Navrhované riešenie musí byť schopné presunúť neopravený súbor infikovaný vírusom do bezpečného priestoru na miestnom pevnom disku pre ďalšiu kontrolu alebo akciu. Navrhované riešenie musí byť schopné skenovať najpopulárnejšie kompresné formáty a prílohy, ako sú všetky typy dokumentov Microsoft Office, komprimované súbory a štandardné grafické súbory, ako sú JPG a GIF. "Navrhované riešenie musí overiť integritu súboru updatu vírusových signatúr pred jeho akceptáciou. Navrhované riešenie musí umožňovať inkrementálne updaty vírusových signatúr." Navrhované riešenie musí byť schopné získať v prípade potreby aktualizáciu signatúr vírusov z centralizovaného servera alebo z Internetu. Navrhované riešenie musí byť schopné získať v prípade potreby aktualizáciu signatúr vírusov z centralizovaného servera alebo z Internetu. "Navrhované riešenie musí detekovať, identifikovať, blokovať a odstrániť tieto škodlivé aplikácie v reálnom čase: (a) Spyware; (b) Adware; (c) Trójske kone; (d) Root kity; (e) Diallery; (h) Ransomware; (i) Iné potenciálne škodlivé a nežiaduce aplikácie"."Navrhované riešenie by malo byť schopné zabrániť inštalácii vyššie uvedených nežiaducich aplikácií.Musí byť schopné automaticky identifikovať vstupný bod malwaru a vplyv na firemné prostredie.Musí byť schopné automaticky vygenerovať forenznú správu o vykonaní útoku. Musí byť schopné rozpoznať post infekčnú komunikáciu s riadiacim centrom malware. Malo by byť schopné ukladať dáta do hostiteľského zariadenia bez prídavného alebo externého zariadenia. Musí byť odolné proti „evasion“ technikám moderného malwaru. Aktívne zabraňuje tomu, aby sa škodlivý obsah dostal k používateľom tým, že rýchlo poskytne bezpečné rekonštruované kópie, zatiaľ čo pôvodné súbory sú kontrolované na možné hrozby (sanitizácia dokumentov, content disarming and reconstruction technológie). Sanitizované súbory musia byť možné uložiť v pôvodnom formáte alebo ako pdf súbor. Mal by byť schopný sa integrovať s AV riešeniami tretích strán. Blokuje útoky bez ohľadu na to, či sú to webové, e-mailové alebo vymeniteľné médiá. Detekuje a blokuje príkazy a riadiace komunikácie, aby zastavili exfiltráciu dát aj pri vzdialenej práci a karantény infikovaných systémov na obmedzenie šírenia malware. Riešenie by malo mať automatizovanú funkciu analýzy udalostí, ktorá poskytuje komplexný pohľad na tok útoku, príčinu, dopad na organizáciu a vstupný bod útoku, umožňujúci zrýchlenú sanáciu. Riešenie by malo podporovať detekciu útokov nultého dňa, detekciou a odoslaním podozrivých súborov do prostredia sanboxu pre emuláciu (buď v Cloud prostredí, alebo ""on-premise)). Statická analýza pred emuláciou. Riešenie musí obsahovať aj EDR komponenty pre pokročilú detekciu hrozieb. Riešenie musí podporovať možnosť exportu kompletných forenských dát do lokálneho SIEMu aj bez nutnosti cloud EDR manažmentu. Možnosť emulovať súbory väčšie ako 10 MB všetkých podporovaných súborových typov. Riešenie musí podporovať emuláciu spustiteľných súborov, archívov, dokumentov, JAVA a flash súborov.Riešenie by malo podporovať forenznú analýzu a trajektóriu súborov. Detekuje a zabraňuje útokom Ransomware. Automaticky obnovuje súbory v prípadoch, keď boli súbory vďaka Ransomware zašifrované. Záloha je uložená a chránená - nemôže byť zašifrovaná ransomwarom. Riešenie umožňuje aj manuálnu obnovu súborov. Riešenie nesmie využívať na ochranu proti ransomware Microsoft volume shadow copy technológiu. Používa detekciu správania a technológie strojového učenia na detekciu nových variantov malwaru.Dashboard poskytuje možnosť zobrazenia všetkých súvisiacich udalostí. Možnosť generovať agregovaný report, ktorá obsahuje dáta o koncových bodoch a sieťové dáta. Schopnosť automaticky generovať podrobný forenzný report. Poskytuje plné forenzné údaje nazhromaždené v čase. Automaticky identifikuje vstupný bod." "Automatický report rozsahu vniknutia škodlivého softvéru. Identifikuje škodlivú / podozrivú aktivitu podľa kategórií / priradenie rizík. Poskytuje úplný stromový prehľad udalostí a útokov. Podľa zvoleného IOC (Indicator of Compromise) (malware proces, URL) môže administrátor vyhľadať ďalšie infikované stanice. Umožňuje vyhľadávať jednotlivé IOC cez všetky koncové stanice. Možnosť spustenia automatickej analýzy z detekcie incidentu sieťového bezpečnostného prvku. Spúšťanie automatickej analýzy od incidentov produktov tretích strán. Dokáže zobraziť reputáciu súboru vo forenznej správe. Schopnosť karantény alebo izolovanie celého počítača. Schopnosť vykonať karanténu súborov / procesov. Schopnosť blokovať a zadržať súbor pred rozšírením na všetky koncové body. Podporuje doplnok do webových prehliadačov, ktorý poskytuje ochranu pred útokmi nultého dňa a extrakciu dát pre sťahované súbory v bezpečnom móde. Riešenie by malo byť schopné pozdržať download cez webový prehliadač. Prehliadače Google Chrome, Internet Explorer a FireFox sú podporované pre rozšírenie prehliadača APT. Povinnou súčasťou riešenia musí byť aj ochrana proti krádeži korporátnych hesiel. Forenzné údaje zhromaždené riešením sú uložené lokálne na samotnom koncovom bode. Uložené údaje sú chránené pred neoprávneným prístupom alebo narušením štruktúry. Riešenie zhromažďuje prebiehajúce informácie o činnosti operačného systému. Zhromaždené informácie zahŕňajú procesnú činnosť, sieťovú komunikáciu, zmeny v registri, prístup k súborovým systémom a mnoho ďalších indikátorov, ktoré sú snímané senzormi agenta. Podpora šifrovania diskov a médií. Riešenie musí podporovať ako vlastné šifrovanie tak aj prevzatie správy Microsoft bitlocker šifrčovanie pevných diskov. Navrhované riešenie musí poskytnúť jednoduchý, ale bezpečný spôsob prístupu k pracovnej stanici v prípade, že užívateľ zabudne heslo alebo opustí spoločnosť bez predchádzajúceho upozornenia	

(mechanizmus Challenge response pre obnovu hesla). Možnosť blokovania použitia firemných credentials na iných verejných službách. Navrhované riešenie by malo podporovať Windows 8.1 Update 1 (32-bit a 64-bit), Windows 10 (32-bit a 64-bit), Windows 11, Windows 2008 R2 (64-bit), Windows 2012, Windows 2012R2 , Windows 2016, Windows 2019, MAC OS, Linux Ubuntu, RHEL. Reporty musia obsahovať integrovanú Mitre Attacks maticu s vyznačenými technikami, ktoré malware používalntegrácia so SIEM - qRadar, ArcSight, Splunk. Reporty obsahuje zoznam zasiahnutých súborov/dát v prípade útoku. Ponúkané riešenie musí rovnakou licenciou pokryť ako cloud správu politík, tak aj on-premis manažment a správu politík.	

a) Zoznam s počtom lokalít a požadované množstvo prác

Popis	Riaditeľstvo (počet)	Pobočky (Počet)
Inštalácia HW	3	14
Inštalácia SW	3	14
Práce	3	14

V Bratislave, dňa

podpis (štatutár alebo splnomocnená osoba)
Mgr. Iveta Gaľová – konateľ

Príloha č.4 Zmluvy

Podmienky poskytovania služieb podpory a údržby (SLA)

1. Služby v rámci SLA bude Poskytovateľ dodávať počas trvania zmluvy v pracovnej dobe (od 9:00 do 17:00 v pracovných dňoch).

- Správa, zabezpečenie prevádzky zariadení, čím sa rozumie zabezpečenie administrácie systému vedúcej k zabezpečeniu funkčnosti Systému, jeho každodennej prevádzky a údržby podľa požiadaviek Objednávateľa v rozsahu min 4 človekodni mesačne. Súčasťou služby je i realizácia požiadaviek na zmenu konfigurácie a nastavení systému. Úkony a kroky v rámci poskytovania služby sa vykonávajú zo sídla Poskytovateľa, príp. priamo v sídle Objednávateľa.
- Inštalácia Software, updates a upgrades, (v prípade zakúpenia Objednávateľom)
- Vzdialená diagnostika
- Nápravné opatrenia na nápravu chyby v SW alebo HW a výkon obmedzujúce faktory
- riešenie vzniknutých prevádzkových problémov
- Vzdialená podpora a údržba systému
- Reakcia na email-ové a telefonnické požiadavky

Lehoty nástupu na odstránenie chýb (oprava a výmena HW uvedeného v Prílohe)

Tabuľka 1

Kategória závažnosti zo strany Objednávateľa	Lehoty nástupu na odstránenie chyby	Potrebná súčinnosť zo strany Objednávateľa	Doba neutralizácie problému
Kritická	Do 4 hodín od oznámenia	Objednávateľ zabezpečí prístup k zariadeniam a poskytne potrebnú súčinnosť	Nasledujúci pracovný deň
Naliehavá	Do 8 hodín od oznámenia	Objednávateľ zabezpečí prístup k zariadeniam a poskytne potrebnú súčinnosť	Do 3 pracovných dní
Obyčajná	Do 2 dní od oznámenia		4 týždne

Definície pojmov:

Kritický problém je systémová alebo aplikačná chyba spôsobujúca zlyhanie alebo obmedzenie funkčnosti systému alebo jeho časti. Takto vzniknutá situácia má významný vplyv na funkčnosť zariadenia alebo systému a má zasdný vplyv na prevádzku a plnenie úloh objednávateľa.
Kritickým problémom je napríklad, nie však výlučne:
- Úplná nefunkčnost zariadenia
- obmedzenie kapacít alebo schopnosti zvládnuť prevádzku do takej miery, že predpokladanú záťaž nemožno zvládnuť,
- Objednávateľ stratil kompletne základný proces pri plnení svojich úloh vyplývajúcich zo všeobecne záväzných právnych predpisov.

Naliehavý problém sú hardvérové a softvérové okolnosti vedúce k podmienkam, ktoré závažným spôsobom ovplyvnia prevádzku, údržbu a správu systému a vyžadujú si okamžitú pozornosť. Urgentnosť je menšia ako pri kritickom probléme kvôli menšiemu dopadu na plnenie úloh Objednávateľa vyplývajúcich zo všeobecne záväzných právnych predpisov. Naliehavým problémom je napríklad, nie však výlučne:
- zníženie kapacity alebo funkcie merania prevádzky,
- strata dohľadu na funkčnosť a/alebo schopnosti diagnostikovať,
- krátkodobé výpadky
- nemožný prístup pre rutinné administratívne činnosti,
- znížená možnosť prístupu pre údržbu alebo obnovy,
- znížená schopnosť systému poskytovať oznamy o kritických alebo naliehavých problémoch,
- každé podstatné zvýšenie počtu chybových hlásení súvisiacich s produktom.

Obyčajný problém sú hardvérové a softvérové okolnosti, ktoré nezhoršia podstatne funkciu systému. Ide o problémy, ktoré nemajú podstatný vplyv na plnenie úloh Objednávateľa vyplývajúcich zo všeobecne záväzných právnych predpisov. Obyčajným problémom je napríklad, nie však výlučne:
- zhoršenie služieb, ale práca môže pokračovať v zhoršenom stave,
- ak poskytovanie služieb a plnenie úloh Objednávateľa funguje s menšími prekážkami.

Neutralizácia je akcia alebo séria akcií, ktoré sa vykonajú s cieľom obnoviť obvyklú prevádzku alebo zníženie závažnosti problému. Neutralizácia nemusí byť finálne riešenie.

Systém je súbor zariadení dodaných Poskytovateľom, zapojených tak, aby umožňovali Objednávateľovi prenášať dáta v požadovanom objeme.

V Bratislave, dňa

.....

Mgr. Iveta Gaľová – konateľ

Špecifikácia predmetu plnenia vo vzťahu k dvojfaktorovej autentifikácii

Implementácia firewallow a dvojfaktorovej autentifikácie do siete NTSSR

Tento návrh sa zaoberá nasadením firewallow vo všetkých lokalitách za účelom celkového zvýšenia bezpečnosti siete a zabezpečením súladu so ZoKB a odporúčaniami auditu. Prostredníctvom firewallow sa vykoná segmentácia sietí na všetkých lokalitách a riadenie prístupov medzi jednotlivými segmentami s centrálnou správou. Ich dôslednou konfiguráciou budú naplnené nasledovné odporúčania auditu:

O-0008 - § 4 -	Dôsledná segmentácia siete, kategorizácia a určenie bezpečnostných zón na firewalle.
O-0028 - § 10 -	Implementácia segmentácie prostredníctvom VLAN v každej lokalite, oddelenie jednotlivých typov zariadení (server, klientska stanica, tlačiareň...) do samostatných sieťových segmentov, nastavenie riadených prestupov prostredníctvom firewallu a granulárne nastavených pravidiel.
O-0029 - § 10 -	Dôsledná segmentácia siete a umiestňovanie serverov so službami priamo prístupnými z externých sietí do dedikovaných DMZ segmentov.
O-0030 - § 10 -	Implementácia segmentácie siete a umiestňovanie serverov do segmentov v závislosti od bezpečnostných požiadaviek a účelov.
O-0031 – § 10 -	Implementácia segmentácie siete vo všetkých lokalitách a zabezpečenie prepojenia jednotlivých segmentov prostredníctvom firewallu.
O-0032 – § 10 -	Segmentácia siete a povoľovanie spojní na základe princípu zásady najnižších privilégií
O-0033 - § 10 -	Implementácia segmentácie a povoľovanie len špecifikovaných služieb na firewalle

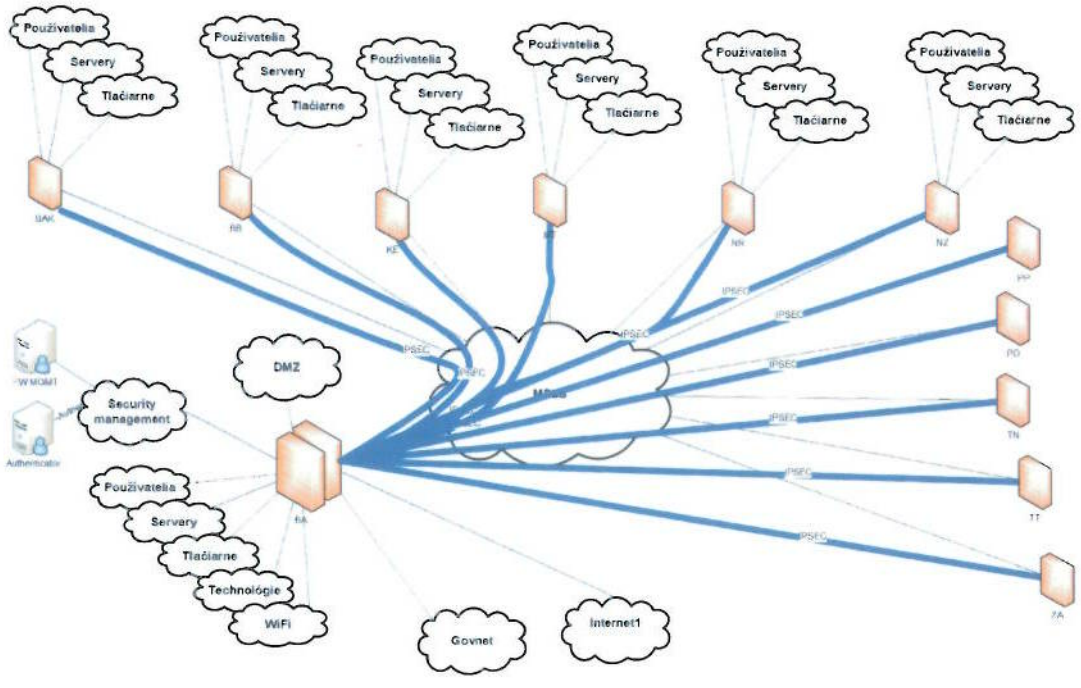
Čiastočne pokryté bude aj opatrenie č 44, nakoľko všetky sieťové spojenia budú zaznamenávané firewallmi a záznamy budú centrálne ukladané na logserveri.
O-0044 - § 11 - Implementácia centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systém

Do siete bude implementovaný systém pre silnú dvojfaktorovú autentifikáciu a tento bude integrovaný so vzdialeným prístupom. Nasadením 2FA a následnou rekonfiguráciou prístupov budú naplnené nasledovné odporúčania auditu:

O-0035 - § 10 - Implementácia dvojfaktorovej autentizácie pri vzdialenom prístupe do internej siete.
O-0036 - § 10 - Identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti
O-0050 - § 12 - Riadenie vzdialeného prístupu formou zriadenia VPN prístupov pre dodávateľov.

Návrh riešenia

Navrhované riešenie počíta s využitím a rozšírením existujúceho riešenia. Súčasne používané firewally na riaditeľstve budú nahradené výkonnejšími modelmi. Existujúce zariadenia sa použijú na lokalitách. Ostatné lokality budú osadené tiež rovnakými modelmi. Riaditeľstvo bude mať firewally vo vysokodostupnom zapojení, na lokalitách budú bez vysokej dostupnosti, dostupnosť bude zabezpečená dodávateľskou SLA. High level dizajn navrhovanej topológie je na nasledujúcom obrázku. Presný zoznam segmentov vrátane IP plánu bude predmetom detailného dizajnu.



Požiadavky na HW zariadenie a manažment:

Počet zariadení: 2

Požiadavka č.	Parameter	Hodnota (áno/nie)
1	Požadované funkcionality: Firewall, IPS, Aplikačná kontrola+URL filtering, Malware a Botnet ochrana, HTTPs inšpekcia, DLP a ochrana proti Zero-day malware	áno
2	Okamžite použitelné preddefinované IPS politiky	áno
3	Možnosť definície IPS výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
4	Možnosť nastavenia monitorovacieho alebo blokovacieho režimu IPS globálne, na úrovni politiky, alebo na úrovni jednotlivej ochrany / signatúry	áno
5	Možnosť konfigurácie a ladenia IPS engine priamo z log výstupov firewallu	áno
6	Nové signatúry IPS musia byť viditelne označené a musia byť aktivované iba v detekčnom režime	áno
7	Detekcia/blokovanie šírenia škodlivého kódu (malware)	áno
8	Minimálne podporované typy súborov pre dynamickú sandbox emuláciu:powerpoint, word, excel, pdf, exe, archivy (zip, tar, 7z, rar)	áno
9	Podporovaná veľkosť emulovaných súborov v sandbox, min. 80MB	áno
10	Možnosť definície Antivirus výnimiek podľa kombinácie: src IP + dst IP + service + útok / signatúra	áno
11	Riadenie politky na základe užívateľských skupín z Active Directory	áno
12	Ochrana proti SNI spoofing v rámci HTTPs inspekce	áno
13	Podpora plnohodnotné HTTPS inspekce pre HTTPS, IMAPS,POP3S	áno
14	Možnosť granulárneho riadenie HTTPs (inšpekcia spojenia alebo bypass) - podľa kombinácie: aplikácia / URL / URL kategória	áno
15	Možnosť vypnutie HTTPS inspekcie pre Wifi	áno
16	Zariadenie musí byť schopné vyčítať identity priamo z doménového kontroleru bez nutnosti inštalovať akúkoľvek externú komponentu	áno
17	Podpora IPSec VPN tunelov	áno
18	VPN IPSec musí podporovať nasledujúce šifrovacie protokoly: AES-128, AES-256, CAST, DES	áno
19	VPN IPSec musí podporovať dátovú integritu pre MD5, SHA1, SHA-256, AES-XCBC	áno
20	Riešenie musí podporovať IP compression pre S2S VPN	áno
21	Podpora Remote Access VPN pre 500 používateľov - vrátane licencie	áno
22	Priepustnost Firewallu, minimálne 17000 Mbps (RFC 3511, 2544, 2647, 1242)	áno
23	Priepustnost Threat prevention, minimálne 2 Gbps (FW, IPS, Threat ochrana, APPC)	áno
24	Počet nových spojení za sekundu (CPS) minimálne 65.000	áno
25	Počet súčasných spojení, min. 2.400.000	áno
26	Fanless - bez aktivných chladiacich komponent.	áno
27	Maximálna hodnota BTU 320 za hodinu	áno
28	Počet fyzických sieťových rozhraní, min. 16x 10/100/1000	áno
29	min. 2x 2.5GbE optický port	áno
	duálne WAN porty - 2x1Gbps	áno
30	podpora alespon 1x 10Gbps SFP+	áno
31	Dedikovaný management port RJ45 1x1Gbps	áno
32	Duálne zdroje napájenia	áno
33	Storage min 250GB SSD	áno
34	2x USB port 3.0	áno
35	1x USB-C vrátane RJ-45 console port	áno
36	Podpora slotu pre formát microSD memory karet do velkosti 64 GB	áno

37	Maximálna spotreba energie 36W	áno
38	Riešenie musí byt uvedené v Gartner Enterprise Firewall Magic Quandrant, každý rok za posledné 3 roky (2019,2020,2021) v kvadrante Leader	áno
39	Podpora vysokej dostupnosti Active-Standby	áno
40	Failover cluster time maximálne 1s	áno
41	Podpora debuggovania problémových scenárov na úrovni L2 - L7	áno
42	Podpora linux nástrojov (min. SCP, BASH, VI, TOP), spúšťania linuxových BASH skriptov a nástrojov tretích stran	áno
43	Riešenie musí podporovať možnosť obnovenia predchádzajúceho OS image (revert) a z lokálneho úložiska	áno
44	Inštalácia dvoch zariadení do standardného 19" kabinetu 1U (velikosť boxu maximálně desktop standard size - 210 x 170 x 45mm)	áno
45	Zero touch deployment (nastavenie prvotnej konfigurácie z USB flash)	áno
46	Dodávaná firewall platforma musia byt vo forme samostatnej fyzickej hardware appliance	áno
47	Podpora lokálného aj centrálného managementu jednotného pre oba typy zariadení	áno
48	Podpora mobilné aplikácie pro remote management	áno
49	Podpora DynDNS a reach my device.	áno
50	Cloud management v cene zariadení	áno
51	Remote Access licencie musí byť súčasťou licencie zariadení.	áno

V Bratislave, dňa

.....

podpis (štatutár alebo splnomocnená osoba)
Mgr. Iveta Gaľová – konateľ

Kalkulácia ceny/ Štruktúra ceny za predmet plnenia

Cenová ponuka na predmet zákazky „Rozvoj governance a úrovne KB v NTS SR“

Obchodné meno, sídlo a IČO uchádzača: KOLAS s. r. o., Tomášikova 10/G, 821 03 Bratislava, IČO: 47060476

Zdaniteľná osoba registrovaná pre účely DPH v Slovenskej republike podľa § 4 zákona:

Zdaniteľná osoba registrovaná pre účely DPH v inej členskej krajine EÚ:

Cena za implementáciu, služby a podporu počas prvého roku realizácie projektu

„Rozvoj governance a úrovne KB v NTS SR“											
P.č.	Názov položky	Obchodný názov	Výrobca	Merná jednotka	Množstvo MJ	Cena za MJ v EUR		Cena celkom za požadované množstvo MJ v EUR			
						bez DPH	s DPH	bez DPH	výška DPH v EUR	Sadzba DPH v %	s DPH
1.	Analýza a dizajn riešenia	Analýza a dizajn riešenia	-	človekodeň	30	606,25 €	727,50 €	18 187,50 €	3 637,50 €	20	21 825,00 €
2.	Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governance (podľa požiadaviek bodu a) v prílohe č. 3. Opis predmetu zákazky)	Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governance	-	človekodeň	60	606,25 €	727,50 €	36 375,00 €	7 275,00 €	20	43 650,00 €
3.	Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – inštalácia (podľa požiadaviek v prílohe (podľa požiadaviek bodu b) a c) v prílohe č. 3. Opis predmetu zákazky)	Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – inštalácia	-	človekodeň	60	606,25 €	727,50 €	36 375,00 €	7 275,00 €	20	43 650,00 €
4.	Dodávka SW vybavenia (podľa požiadaviek v prílohe (podľa požiadaviek bodu b) a c) v prílohe č. 3. Opis predmetu zákazky) s podporou a servisom prvý rok	Collaborative Enterprise Support - Premium: Next Generation Security Management Software for 25 gateways (SmartEvent & Compliance 1 year)	Check Point	balík	1	13 790,50 €	16 548,60 €	13 790,50 €	2 758,10 €	20	16 548,60 €
5.	Dvojfaktorová autentifikácia - inštalácia (podľa požiadaviek bodu e) v prílohe č. 3. Opis predmetu zákazky) s podporou a servisom prvý rok	Dvojfaktorová autentifikácia - FortiAuthenticator	Fortinet	balík	1	9 450,00 €	11 340,00 €	9 450,00 €	1 890,00 €	20	11 340,00 €
6.	Dodávka HW vybavenia (podľa požiadaviek bodu b) a c) v prílohe č. 3. Opis predmetu zákazky) s podporou a servisom prvý rok	1800 and 1570 Base Appliance with SandBlast subscription package for 1 year	Check Point	balík	1	23 094,47 €	27 713,36 €	23 094,47 €	4 618,89 €	20	27 713,36 €
7.	Nasadenie a podpora kybernetickej bezpečnosti, systémov a IT technológií – (podľa požiadaviek bodu e) v prílohe č. 3. Opis predmetu zákazky) s podporou a servisom prvý rok	Nasadenie a podpora kybernetickej bezpečnosti, systémov a IT technológií	-	človekodeň	48	606,25 €	727,50 €	29 100,00 €	5 820,00 €	20	34 920,00 €
Cena celkom za predmet zákazky v EUR bez DPH:											166 372,47 €
Výška DPH v EUR:											33 274,49 €
Cena celkom za predmet zákazky v EUR s DPH:											199 646,96 €

Vyhlasujem, že cenová ponuka spĺňa požiadavky verejného obstarávateľa uvedené vo výzve na predloženie cenovej ponuky a jej prílohách a obsahuje všetky náklady súvisiace s dodaním predmetu zákazky.

V Bratislave, dňa

.....

podpis (štatutár alebo splnomocnená osoba)

Mgr. Iveta Gallová – konateľ

Harmonogram realizácie zákazky - míľniky

Verejný obstarávateľ: Národná transfúzna služba SR, Ďumbierska 3/L, 831 01 Bratislava
Názov zákazky: Rozvoj governance a úrovne KB v NTS SR
Dodávateľ: KOLAS s. r. o., Tomášikova 10/G, 821 03 Bratislava, IČO: 47060476

Popis položky	Odhadovaný termín dodania (od DD.MM.RRRR do DD.MM.RRRR)	Predpokladaná dodacia doba od zadania objednávky (v dňoch)
Míľnik č. 1: Analýza a dizajn riešenia	od 11.04.2023 do 18.04.2023	30 dní
Míľnik č. 2: Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governence - Vypracovanie bezpečnostnej dokumentácie, aktualizácia existujúcej dokumentácie riadenia kybernetickej bezpečnosti	od 17.04.2023 do 28.04.2023	60 dní
Míľnik č. 3: Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governence - Klasifikácia informácií a kategorizácia IS a sietí	od 11.7.2023 do 18.7.2023	90 dní
Míľnik č. 4: Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governence - Analýza rizík, BCM	od 11.9.2023 do 18.9.2023	150 dní
Míľnik č. 5: Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governence - Riadenie vzťahov s tretími stranami	od 29.9.2023 do 6.10.2023	170 dní
Míľnik č. 6: Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – governence - BCM, kontinuita riadenia KB	od 23.10.2023 do 31.10.2023	190 dní
Míľnik č. 7 : Implementácia bezpečnostných opatrení nariadených auditom kybernetickej bezpečnosti – inštalácia	od 8.5.2023 do 15.5.2023	90 dní po dodávke HW
Míľnik č. 8: Dodávka SW vybavenia	od 11.04.2023 do 18.04.2023	30 dní
Míľnik č. 9: Dvojfaktorová autentifikácia - inštalácia	od 8.5.2023 do 15.5.2023	90 dní po dodávke HW
Míľnik č. 10: Dodávka HW vybavenia	od 11.04.2023 do 18.04.2023	30 dní
Míľnik č. 11: Nasadenie a podpora kybernetickej bezpečnosti, systémov a IT technológií	priebežne počas plnenia zmluvy	priebežne počas plnenia zmluvy

V Bratislave, dátum:

.....
Mgr. Iveta Gaľová
konateľ

VYHLÁSENIE UCHÁDZAČA O SUBDODÁVKACH

Uchádzač
(obchodné meno, sídlo/ miesto podnikania uchádzača, IČO
alebo obchodné mená,sídla/miesta podnikania, IČO)

KOLAS s. r. o., Tomášikova 10/G, 821 03 Bratislava, IČO: 47060476

Dolu podpísaný zástupca uchádzača týmto vyhlasujem, že v rámci realizácie predmetu zákazky s názvom **„Rozvoj governance a úrovne KB v NTS SR"** vyhlásenej verejným obstarávateľom Národná transfúzna služba SR

a. nebudem využívať subdodávky a celé plnenie zabezpečím sám.*
~~b. budem využívať subdodávky a na tento účel uvádzam:*~~
**(nehodiace sa prečiarknite)*

	Subdodávateľ (obch. meno, sídlo alebo miesto podnikania, IČO)	Kontaktná osoba (meno a priezvisko, tel. č., e-mail)	Popis dodávok vykonávaných subdodávateľom	Podiel plnenia zmluvy v % z celkového objemu	Podiel plnenia zmluvy vo finančnom vyjadrení v EUR bez DPH
1.					
2.					
3.					
4.					
5.					
6.					

Čestne vyhlasujem, že každý subdodávateľ spĺňa alebo najneskôr v čase plnenia bude spĺňať podmienky podľa § 32 ods. 1 prípadne podľa § 11 ods. 1 zákona o verejnom obstarávaní; tým nie je dotknutá zodpovednosť úspešného uchádzača alebo uchádzačovza plnenie predmetu zmluvy.

Akceptujem pravidlá zmeny subdodávateľov počas plnenia zmluvy, ktoré sú uvedené v návrhu rámcovej kúpnej zmluvy.

V Bratislave, dňa

.....
podpis (štatutár alebo splnomocnená osoba)
Mgr. Iveta Gaľová – konateľ

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená podľa ust. § 269 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti medzi zmluvnými stranami:

Objednávateľ

Názov:	**Národná transfúzna služba SR**
Sídlo:	Ďumbierska 3/L, 831 01 Bratislava
Zriadená:	Štátna príspevková organizácia zriadená Zriaďovacou listinou MZ SR č. 003775-4/2003 zo dňa 02.12.2003
IČO:	30 853 915
DIČ:	2021764371
IČ pre DPH:	SK2021764371
Bankové spojenie:	Štátna pokladnica
Číslo účtu (IBAN):	SK18 8180 0000 0070 0028 8579
Štatutárny zástupca:	Ing. Ivan Oleár, MBA, riaditeľ
Osoba oprávnená na rokovanie:	
vo veciach zmluvy	Ing. Ivan Oleár, MBA
vo veciach odborných	Ing. Jozef Macko
E-mail:	jozef.macko@ntssr.sk
Internetová adresa:	www.ntssr.sk

(ďalej len „**Objednávateľ**")

a

Poskytovateľ

Obchodné meno:	KOLAS s. r. o.
Sídlo:	Tomášikova 10/G, 821 03 Bratislava
Zapísaná:	v obchodnom registri Okresného súdu Bratislava I, oddiel: Sro, vložka č. 87961/B
IČO:	47060476
DIČ:	2023758495
IČ pre DPH:	SK2023758495
Bankové spojenie:	VÚB, a. s.
Číslo účtu:	SK3902000000003653927456
V mene ktorej koná:	Mgr. Iveta Gaľová – konateľ
Osoba oprávnená na rokovanie	
vo veciach zmluvy:	Mgr. Michal Holomek
vo veciach odborných:	Ing. Viliam Martinkovič
Tel.:	tel. č.: +421 2 32 144 211
E-mail:	obchod@kolas.sk
Internetová adresa:	www.kolas.sk

(ďalej len „**Poskytovateľ**")

Článok 1
Úvodné ustanovenia

1.1 Objednávateľ a Poskytovateľ uzavreli dňa _____ Zmluvu o dielo a poskytovaní služieb (ďalej len „**Zmluva o dielo**"), predmetom ktorej je záväzok Poskytovateľa vykonať pre Objednávateľa dielo spočívajúce v rozvoji governance a úrovne informačnej a kybernetickej bezpečnosti v NTS SR a poskytnúť Objednávateľovi služby podpory a údržby v rozsahu a za podmienok stanovených v Zmluve o dielo.

1.2 Objednávateľ je prevádzkovateľom základnej služby v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o kybernetickej bezpečnosti**") a je povinný plniť povinnosti v zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „**Vyhláška NBÚ**").

1.3 Poskytovateľ je v zmysle Zmluvy o dielo dodávateľom služieb (činností), ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Objednávateľa ako prevádzkovateľa základnej služby.

1.4 Na základe vyššie uvedených skutočností a v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti Objednávateľ a Poskytovateľ týmto uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**Zmluva**").

Článok 2
Predmet Zmluvy

2.1 Predmetom tejto Zmluvy je záväzok Poskytovateľa:

a) poskytnúť Objednávateľovi súčinnosť pri výkone činností uvedených v § 19 ods. 6 zákona o kybernetickej bezpečnosti,
b) prijať opatrenia minimálne v rozsahu Vyhlášky NBÚ a § 20 zákona o kybernetickej bezpečnosti,
c) plniť povinnosti týkajúce sa kybernetickej bezpečnosti Objednávateľa podľa tejto Zmluvy,
d) zdokumentovať prijaté bezpečnostné opatrenia najmenej v rozsahu stanovenom § 20 zákona o kybernetickej bezpečnosti.

2.2 Miestom plnenia tejto Zmluvy sú najmä pracoviská alebo sídlo Objednávateľa, pracovisko alebo sídlo Poskytovateľa, alebo pracoviská a sídla subdodávateľov.

2.3 Bezpečnostné opatrenia a notifikačné povinnosti sa Poskytovateľ zaväzuje plniť od okamihu nadobudnutia účinnosti tejto Zmluvy až do skončenia poskytovania Služieb, pokiaľ z aplikovateľných právnych predpisov nevyplývajú určité povinnosti pre Poskytovateľa aj po skončení Zmluvy o dielo.

Článok 3
Práva a povinnosti Poskytovateľa

3.1 Poskytovateľ je povinný vykonávať činnosti v tejto Zmluve v súlade s platnými právnymi predpismi. V prípade, že Poskytovateľ v rámci servisných zásahov bude využívať vzdialený prístup do počítačovej siete Objednávateľa, musí postupovať podľa ustanovení uvedených v **Prílohe č. 1 „Vzdialený prístup"**, ktorá tvorí neoddeliteľnú súčasť tejto Zmluvy.

3.2 Poskytovateľ sa zaväzuje pri plnení Zmluvy dodržiavať bezpečnostné politiky Objednávateľa (ďalej ako „**bezpečnostná politika**"). Poskytovateľ podpisom tejto Zmluvy vyhlasuje, že sa pred podpisom tejto Zmluvy oboznámil s bezpečnostnou politikou Objednávateľa, ktorá je uvedená v nasledovných dokumentoch:

- Smernica Národnej transfúznej služby SR o informačnej bezpečnosti č. 02/2020
- Smernica Národnej transfúznej služby SR o kybernetickej bezpečnosti č. 03/2020

3.3 Poskytovateľ súhlasí s tým, že bezpečnostná politika sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Objednávateľa a aktuálnym hrozbám dotýkajúcim sa Poskytovateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa. Objednávateľ je povinný bezodkladne oboznámiť Poskytovateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Poskytovateľ následne písomne potvrdí oboznámenie sa so zmenenou bezpečnostnou politikou. Takéto potvrdenie je oprávnená podpísať kontaktná osoba Poskytovateľa podľa v Článku 8 bod 8.3 tejto Zmluvy.

3.4 Poskytovateľ sa zaväzuje chrániť všetky informácie poskytnuté Objednávateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

3.5 Poskytovateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Objednávateľom pri plnení povinností Objednávateľa podľa zákona o kybernetickej bezpečnosti alebo Vyhlášky NBÚ, a to zaslaním e-mailu na kontaktnú osobu Objednávateľa uvedenú v Článku 8 bod 8.3 tejto Zmluvy.

3.6 Poskytovateľ sa zaväzuje hlásiť všetky informácie, ktoré majú vplyv na túto Zmluvy zaslaním e-mailu na kontaktnú osobu Objednávateľa uvedenú v Článku 8 bod 8.3 tejto Zmluvy.

3.7 V oblasti technických zraniteľností systémov a zariadení realizuje Poskytovateľ opatrenia podľa § 9 Vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Objednávateľovi a ktoré toto poskytovanie služieb Objednávateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

3.7.1 Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou služieb poskytovaných podľa Zmluvy o dielo.

3.7.2 Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, ak sú súčasťou služieb poskytovaných podľa Zmluvy o dielo.

3.7.3 Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

3.8 Poskytovateľ je ďalej povinný :

3.8.1 zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Poskytovateľa nebolo možné zasiahnuť siete a informačné systémy Objednávateľa,

3.8.2 sledovať hrozby dotýkajúce sa Poskytovateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa (ďalej len „**incidenty**"),

3.8.3 zasielať Objednávateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak,

3.8.4 spolupracovať s Objednávateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa,

3.8.5 po skončení Zmluvy o dielo vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má Poskytovateľ počas plnenia Zmluvy o dielo prístup, okrem prípadov, ak z osobitných právnych predpisov vyplýva opak,

3.8.6 prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, 10, 12, 14 a 15 Vyhlášky NBÚ, a v rozsahu špecifikovanom v bezpečnostnej politike Objednávateľa.

3.9 Poskytovateľ môže zapojiť do plnenia Zmluvy o dielo tretiu osobu (subdodávateľa) len s predchádzajúcim písomným súhlasom Objednávateľa.

3.10 Ak Poskytovateľ zapojí do plnenia Zmluvy o dielo subdodávateľa, Poskytovateľ je povinný uložiť mu rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení a notifikačných povinností, ako sú ustanovené v tejto Zmluve. V prípade, ak Poskytovateľ použije na plnenie Zmluvy o dielo subdodávateľa, zodpovedá Objednávateľovi za porušenie povinností vyplývajúcich z tejto Zmluvy tak, akoby plnil sám.

3.11 Poskytovateľ vykonáva len činnosti, ktoré vyplývajú zo Zmluvy o dielo, tejto Zmluvy, z právnych predpisov alebo ich vykonáva na základe písomnej požiadavky Objednávateľa. Na výkon týchto činností môže poveriť Poskytovateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v Prílohe č. 1 tejto Zmluvy.

3.12 Akákoľvek zmena v personálnom obsadení pracovných rolí musí byť Objednávateľovi oznámená vopred. Oznámenie zašle Poskytovateľ e-mailom kontaktnej osobe Objednávateľa. Na zmenu v personálnom obsadení pracovných rolí nie je potrebný súhlas Objednávateľa. Poskytovateľ týmto poveruje kontaktnú osobu Poskytovateľ podľa Článku 8 bod 8.3 tejto Zmluvy na oznámenie zmeny v personálnom obsadení pracovných rolí Objednávateľovi.

3.13 Za plnenie povinností podľa tejto Zmluvy nemá Poskytovateľ nárok na žiadnu odplatu ani náhradu nákladov s výnimkou dohodnutej odplaty podľa Zmluvy o dielo.

Článok 4
Reaktivita pri riešení incidentov

4.1 Poskytovateľ je povinný neodkladne hlásiť Objednávateľovi kybernetický bezpečnostný incident definovaný čl. 3 písm. j) zákona o kybernetickej bezpečnosti. Zamestnanci Poskytovateľa, prípadne subdodávateľa sú oboznámení so spôsobom oznamovania kybernetických bezpečnostných incidentov v súvislosti s prevádzkou sietí a informačných systémov

Objednávateľa pri plnení Zmluvy o dielo a oznamujú akékoľvek podozrenie, o ktorom vedia alebo by so zreteľom na všetky okolnosti mali vedieť, že by mohlo mať negatívny dopad na bezpečnosť siete alebo informačného systému Objednávateľa na e-mailovej adrese Objednávateľa **informatika@ntssr.sk.**

4.2 Ak v čase hlásenia incidentu stále trvajú prejavy incidentu, Poskytovateľ odošle Objednávateľovi neúplné hlásenie aj s odkazom, že ide o neúplné hlásenie. Poskytovateľ neúplné hlásenie bez zbytočného odkladu doplní po obnove riadnej a úplnej prevádzky siete a všetkých informačných systémov Objednávateľa.

4.3 Najčastejšími spôsobmi riešenia incidentov, ktoré Poskytovateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou incidentov (ďalej len „**Reakčné opatrenia**"), a to ako na výzvu Objednávateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie.

4.4 Poskytovateľ pri reakciách na incidenty spolupracuje s Objednávateľom, Národným bezpečnostným úradom SR a inými príslušnými orgánmi a za týmto účelom poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami a ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.

4.5 Poskytovateľ bez zbytočného odkladu oznámi Objednávateľovi implementáciu Reakčných opatrení.

4.6 Ak o to Objednávateľ požiada, po úspešnej implementácii Reakčného opatrenia Poskytovateľ predloží návrh bezpečnostných opatrení a postupov, ktoré zabezpečia, že nedôjde k opakovaniu, pokračovaniu či šíreniu incidentu. Ak ochranné opatrenie neprinesie požadovaný efekt, Poskytovateľ vypracuje a predloží iné ochranné opatrenie. S povolením Objednávateľa Poskytovateľ implementuje ochranné opatrenie a spíše záznam o efektívnosti jeho implementácie.

Článok 5
Zodpovednosť

5.1 Zmluvné strany berú na vedomie, že ani pri vynaložení maximálneho úsilia nie je možné úplne eliminovať vznik incidentov.

5.2 Poskytovateľ je však povinný prijať a vykonávať všetky opatrenia, tak na svojej strane, ako aj u Objednávateľa, o ktorých predpokladá, alebo o ktorých možno pri vynaložení odbornej starostlivosti predpokladať, že incidentom zabránia alebo zmiernia ich škodlivé následky.

5.3 Poskytovateľ berie na vedomie, že neplnenie jeho povinností podľa tejto Zmluvy riadne a/alebo včas môže spôsobiť vznik škody Objednávateľovi alebo tretím osobám, pričom v prípade škôd ako dôsledkov incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Poskytovateľa podľa tejto Zmluvy neprejavili, alebo by sa prejavili v menšej intenzite, zodpovedá Poskytovateľ v plnom rozsahu.

5.4 Poskytovateľ zodpovedá Objednávateľovi okrem prípadu podľa bodu 5.3 vyššie aj za akúkoľvek inú škodu, ktorá vznikla v dôsledku toho, že Poskytovateľ neplnil povinnosti podľa tejto Zmluvy riadne a/alebo včas. Škodou sa pre účely tejto Zmluvy rozumie aj akákoľvek sankcia uložená príslušnými orgánmi verejnej moci Objednávateľovi v dôsledku toho, že Poskytovateľ neplnil svoje povinnosti vyplývajúce z tejto Zmluvy riadne a/alebo včas.

Článok 6
Audit kybernetickej bezpečnosti

6.1 Poskytovateľ umožní zástupcovi Objednávateľa zodpovednému za kybernetickú bezpečnosť a ním určeným osobám riadny výkon auditu (kontroly) výkonu činností Poskytovateľa podľa tejto Zmluvy.

6.2 Audit môže byť vykonaný v pracovných dňoch v bežných pracovných hodinách po predchádzajúcom oznámení Objednávateľa, ktoré uskutoční najmenej 3 pracovné dní vopred.

6.3 Audit sa uskutoční najmenej v rozsahu: nahliadania do dokumentov, nahliadanie do informačných systémov, auditu procesov, pracovných postupov v sídle alebo na pracovisku Poskytovateľa.

6.4 Audit je možné vykonať len pri dodržaní všeobecne záväzných právnych predpisov týkajúcich sa najmä ochrany osobných údajov. Za dodržanie týchto predpisov pri výkone auditu Objednávateľom zodpovedá Poskytovateľ, ktorý je povinný prijať všetky opatrenia nevyhnutné na ochranu osobných údajov, ktoré spracováva, prípadne iných údajov, ktoré podľa všeobecne záväzných právnych predpisov alebo zmlúv s tretími osobami nemôžu byť celkom alebo sčasti sprístupnené Objednávateľovi.

6.5 Akékoľvek nedostatky alebo pochybenia zistené auditom je Poskytovateľ povinný odstrániť bezodkladne, avšak najneskôr do 30 kalendárnych dní.

6.6 Poskytovateľ je povinný pri audite spolupracovať s Objednávateľom a poskytnúť mu potrebnú súčinnosť spočívajúcu najmä v prístupe k do svojich priestorov, k dokumentácii a technickému a technologickému vybaveniu, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.

6.7 Objednávateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe, vrátane informácií o Poskytovateľovi, jeho činnosti, systéme vnútorného riadenia, pracovno-právnych vzťahoch a pod. Objednávateľ a jeho zamestnanci pri návšteve priestorov Poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny Poskytovateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „**BOZP**") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „**PO**"), s ktorými boli oboznámení. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov Objednávateľa o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Poskytovateľ na zaistenie BOZP a PO, o opatreniach a postupe v

prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO.

Článok 7
Ochrana informácií

7.1 Poskytovateľ je povinný zachovávať dôvernosť všetkých informácií týkajúcich sa Objednávateľa a jeho činnosti, ktoré mu Objednávateľ sprístupnil, alebo ktoré sa mu stali inak známe v súvislosti s plnením Zmluvy o dielo. Poskytovateľ sa najmä zaväzuje, že tieto informácie neprístupní tretej osobe, ani ich nepoužite vo svoj prospech alebo v prospech tretej osoby za iným účelom ako je plnenie Zmluvy o dielo.

7.2 Každá osoba zúčastnená za Poskytovateľa na predmete plnenie je povinná zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti, čo je povinný zabezpečiť Poskytovateľ.

Článok 8
Kontaktné osoby a doručovanie

8.1 Poskytovateľ je povinný komunikovať pri plnení povinností podľa tejto Zmluvy s Objednávateľom e-mailom na kontaktné údaje Objednávateľa uvedené v tomto článku Zmluvy, alebo iným vhodným spôsobom, pričom vo všetkých prípadoch musí byť prenos informácií uskutočnený za podmienok umožňujúcich chránený prenos informácií.

8.2 Objednávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Poskytovateľom na úseku kybernetickej bezpečnosti: Ing. Jozef Macko, jozef.macko@ntssr.sk

8.3 Poskytovateľ určuje nasledovnú kontaktnú osobu na úseku kybernetickej bezpečnosti pre komunikáciu s Objednávateľom: Viliam Martinkovič, viliam.martinkovic@kolas.sk

8.4 Kontaktná osoba Poskytovateľa plní úlohy pri zabezpečovaní reaktivity podľa Článku 4 tejto Zmluvy. Kontaktná osoba plní notifikačné povinnosti podľa Zmluvy.

8.5 Kontaktné osoby podľa bodov 8.2 a 8.3 tohto článku Zmluvy a pracovné role podľa Prílohy č. 1 Zmluvy môže príslušná zmluvná strana zmeniť bez vyhotovenia dodatku k tejto Zmluve, ak oznámi novú kontaktnú osobu a /alebo pracovnú rolu druhej zmluvnej strane v písomnej forme. Pre oznamovanie zmien pracovných rolí platí Článok 3 bod 3.12 Zmluvy. V prípade, že kontaktné osoby a pracovné role Poskytovateľa majú prístup k informáciám a údajom Objednávateľa, sú povinné zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

8.6 Zmluvné strany sa dohodli, že písomnosti podľa tejto Zmluvy sa doručujú osobne, poštou, kuriérskou službou alebo e-mailom. Každá zo zmluvných strán je povinná písomne informovať druhú zmluvnú stranu o akejkoľvek zmene adresy, e-mailu, alebo kontaktných údajov.

8.7 Písomnosti doručované osobne sa považujú za doručené okamihom ich prevzatia, alebo dňom, kedy adresát preukázateľne odmietol prevziať zásielku. Písomnosti doručované poštou alebo

kuriérskou službou sa považujú za doručené v deň prevzatia zásielky adresátom, alebo v deň, kedy sa zásielka vrátila späť adresátovi ako nedoručená z dôvodov, ktoré nespočívajú na strane odosielateľa, a to aj v prípade, ak sa o nej adresát nedozvedel. Písomnosti doručované prostredníctvom e-mailu na e-mailové adresy uvedené v tejto Zmluve sa považujú za doručené nasledujúci pracovný deň po ich odoslaní.

Článok 9
Trvanie Zmluvy a spôsoby jej skončenia

9.1 Táto Zmluva sa uzatvára na dobu trvania Zmluvy o dielo a služieb poskytovaných na jej základe Poskytovateľom Objednávateľovi, okrem tých ustanovení, ktoré majú podľa Zmluvy alebo zákona trvať aj po skončení Zmluvy, najmä záväzkov na náhradu škody.

9.2 Objednávateľ je oprávnený od tejto Zmluvy odstúpiť v prípadoch, ak Poskytovateľ poruší niektorú z povinností vyplývajúcich z tejto Zmluvy. V prípade porušenia Zmluvy podstatným spôsobom je Objednávateľ oprávnený odstúpiť od Zmluvy bezodkladne po tom, ako sa o porušení dozvie.

9.3 V prípade, ak porušenie Zmluvy Poskytovateľom nemá charakter podstatného porušenia, Objednávateľ je oprávnený odstúpiť od Zmluvy v prípade, ak Poskytovateľ neodstráni porušenie povinností alebo jeho následky ani v dodatočnej primeranej lehote, ktorú mu Objednávateľ určí.

9.4 Odstúpenie od tejto Zmluvy musí byť písomné. Odstúpenie je účinné dňom jeho doručenia druhej zmluvnej strane.

9.5 S ohľadom na § 8 ods. 2 písm. p) Vyhlášky NBÚ, po ukončení tejto Zmluvy je Poskytovateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Objednávateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Objednávateľom ako prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto Zmluvy.

9.6 Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto Zmluvy medzi Objednávateľom a Poskytovateľom je zákonnou povinnosťou Objednávateľa. Z uvedeného dôvodu je Objednávateľ v prípade skončenia platnosti tejto Zmluvy oprávnený bez ďalšieho odstúpiť od Zmluvy o dielo.

Článok 10
Záverečné ustanovenia

10.1 Táto Zmluva nadobúda platnosť jej podpisu zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej podpisu oboma zmluvnými stranami.

10.2 Práva a povinnosti zmluvných strán neupravené v tejto Zmluve sa riadia Zmluvou o dielo a platnými právnymi predpismi, najmä zákonom o kybernetickej bezpečnosti a Vyhláškou NBÚ. Ustanovenia Zmluvy o dielo uzatvorenej medzi Poskytovateľom a Objednávateľom ostávajú

podpisom tejto Zmluvy nedotknuté, okrem povinností Poskytovateľa, ktoré sú v tejto Zmluve upravené prísnejšie.

10.3 Nič v tejto Zmluve nemožno vykladať tak, že zbavuje ktorúkoľvek zmluvnú stranu zodpovednosti za plnenie jej povinností, ktoré jej vyplývajú zo zákona o kybernetickej bezpečnosti, Vyhlášky NBÚ, prípadne iných právnych predpisov v oblasti ochrany údajov.

10.4 Táto Zmluva sa môže meniť alebo ukončiť iba dohodou zmluvných strán v písomnej forme.

10.5 Prílohou č. 2 tejto Zmluvy je Zoznam pracovných rolí.

10.6 Zmluvné strany vyhlasujú, že si túto Zmluvu prečítali, jej obsahu porozumeli a súhlasia s ním, a že Zmluvu uzatvárajú slobodne, vážne a bez nátlaku, na znak čoho túto Zmluvu podpisujú.

V Bratislave, dňa _	V Bratislave, dňa
Za Objednávateľa:	Za Poskytovateľa:
Národná transfúzna služba SR Ing. Ivan Oleár, MBA, riaditeľ	**KOLAS s. r. o.** Mgr. Iveta Gaľová – konateľ

Príloha č. 1 Vzdialený prístup

- spoločnosti KOLAS s. r. o., Tomášikova 10/G, 821 03 Bratislava, IČO: 47060476

(ďalej len „Poskytovateľ")

k Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

medzi

Objednávateľ: **Národná transfúzna služba SR,** IČO: 30 853 915
Ďumbierska 3/L, 831 01 Bratislava
(ďalej len „NTS SR")

Poskytovateľ: **KOLAS s. r. o.**
IČO: 47060476
Tomášikova 10/G, 821 03 Bratislava
(ďalej len „Názov")

1 Vzdialený prístup

1.1 Systémom pre účely tejto Prílohy č. 1 sa rozumie „Rozvoj governance a úrovne KB v NTS SR", inštalovaný na pracoviskách NTS SR, ktorý je udržiavaný a podporovaný Poskytovateľom alebo jeho subdodávateľmi (ďalej len „Systém"). Vzdialený prístup do Systému NTS SR sa vykoná v nasledovných prípadoch:

- zásahy objednané NTS SR,
- zákroky súvisiace s analýzou či odstránením poruchy alebo havárie Systému hlásené NTS SR,
- zásahy vopred prerokované s NTS SR,
- plánované zákroky prerokované s NTS SR .

1.2 Vzdialený prístup do Systému môže Poskytovateľ alebo jeho subdodávateľ vykonávať najmä v pracovných dňoch v čase od 07:00 do 16:30, vo výnimočných prípadoch po dohode s NTS SR aj mimo vyššie uvedeného času.

1.3 Osoby, ktoré sú oprávnené v mene Poskytovateľa a jeho subdodávateľa vzdialene pristupovať k Systému sú: Viliam Martinkovič, Jozef Palgut a Martin Barňak. Poskytovateľ sa zaväzuje zabezpečiť, že žiadne iné osoby nebudú mať možnosť vzdialene pristupovať k systému.

1.4 Oprávnené osoby NTS SR, ktoré budú komunikovať s Poskytovateľom alebo jeho subdodávateľom vo veciach vzdialeného prístupu, najmä objednávať servisné zásahy a zákroky, prerokovávať plánované zásahy a zákroky a pod. sú: pracovníci odboru IT NTS SR, alebo ním poverený pracovník.

1.5 NTS SR aj Poskytovateľ sú oprávnený jednostranne zmeniť zoznam oprávnených osôb za svoju stranu, a to písomným oznámením podpísaným osobami oprávnenými konať v mene príslušnej zmluvnej strany, doručeným druhej zmluvnej strane. Zmena zoznamu oprávnených osôb je voči druhej zmluvnej strane účinná na 3. deň po doručení takéhoto oznámenia.

1.6 Poskytovateľ je povinný všetky osoby oprávnené vzdialene pristupovať k Systému písomne poučiť o ich povinnosti mlčanlivosti ohľadne akýchkoľvek informácií týkajúcich sa NTS SR alebo tretích osôb, ktoré im budú sprístupnené, alebo ktoré sa inak dostanú do ich dispozície pri realizácii vzdialeného prístupu k Systému.

2 Vytvorenie prístupu

2.1 Vytvorenie vzdialeného prístupu k Systému a jeho údržba je plne v kompetencii Poskytovateľa alebo jeho subdodávateľa.

2.2 Poskytovateľ alebo jeho subdodávateľ je oprávnený vytvoriť vzdialený prístup len so súhlasom NTS SR. Schvaľovanie vzdialeného prístupu prebieha podľa interných predpisov NTS SR.

2.3 NTS SR je oprávnená dočasne prerušiť poskytovanie vzdialeného prístupu v prípade podozrenia na jeho zneužitie alebo aj bez udania dôvodu.

3 Súčinnosť zmluvných strán a servisné podmienky

3.1 Zmluvné strany si sú vedomé významu a dôležitosti bezporuchového nepretržitého chodu a funkčnosti Systému. Z tohto dôvodu obidve zmluvné strany sa zaväzujú vytvárať optimálne podmienky pre činnosť oprávnených osôb zabezpečujúcich plnenie povinností podľa Zmluvy.

3.2 NTS SR sa zaväzuje zabezpečiť prístup pre oprávnených pracovníkov Poskytovateľa alebo jeho subdodávateľa k Systému prostredníctvom vzdialeného pripojenia pre realizáciu správy a monitorovania Systému a odstraňovania vád. NTS SR nezodpovedá za splnenie licenčných podmienok používaného softvéru Poskytovateľa alebo jeho subdodávateľom.

3.3 Všetky zmeny konfigurácie Systému zo strany Poskytovateľa alebo subdodávateľa budú vykonávané výhradne so súhlasom NTS SR a budú riadne zdokumentované. Príslušná dokumentácia musí byť na požiadanie dostupná pracovníkom NTS SR. Akákoľvek zmena konfigurácie Systému alebo modifikácie programového kódu, ktorý je súčasťou Systému, zo strany NTS SR alebo tretej strany bez súhlasu Poskytovateľa je považovaná za podstatné porušenie Výpožičnej zmluvy.

3.4 V prípade, že lokalizáciu poruchy a jej odstraňovanie bude vykonávať pracovník subdodávateľa, Poskytovateľ zodpovedá za prípadné škody, riziká či problémy súvisiace s poskytovanou službou vykonávanou pracovníkmi subdodávateľa.

Príloha č. 10 zmluvy

MIESTA REALIZÁCIE

Rozvoj governance a úrovne KB v NTS SR

Pracovisko NTS SR	Adresa pracoviska
Bratislava, Riaditeľstvo Ďumbierska 3/L	Ďumbierska 3/L, 83101,Bratislava
Bratislava, SC Ďumbierska 3/L	Ďumbierska 3/L, 83101,Bratislava
Banská Bystrica, SC Jaseňová 7	Jaseňová 7, Banská Bystrica
Bratislava, OC Ružinov	Ružinovská 6, 821 02 Bratislava
Bratislava, OC Kramáre	Limbová 3, 833 14 Bratislava
OC Nové Zámky	Slovenská 11/A, 940 34 Nové Zámky
OC Žilina	Vojtecha Spanyola 43, 010 01 Žilina
Banská Bystrica, OC L. Svobodu 1	Námestie L. Svobodu 1, 975 17 Banská Bystrica
OC Prešov	Jána Hollého 14, 080 01 Prešov
SC + OC Košice	Trieda SNP 1, 040 11 Košice
OC Trnava	Andreja Žarnova 11, 917 02 Trnava
OC Trenčín	Legionárska 28, 911 01 Trenčín
OC Nitra	Špitálska 6, 949 01 Nitra
OC Poprad	Banícka 803/28, 058 45 Poprad
OC Martin	Priehradka 18A, 036 01 Martin

V Bratislave, dňa

.....

podpis (štatutár alebo splnomocnená osoba)
Mgr. Iveta Galová – konateľ