Zmluva o poskytnutí služieb podpory a údržby a navýšení a obnovy licencií ochrany koncových zariadení

uzatvorená v súlade s § 269 ods. 2 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov (ďalej len „**Obchodný zákonník**“) a zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

(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:	Seberíniho 1, 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 Mestského súdu Bratislava III, 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 s nízkou hodnotou „**Navýšenie licencií + technická podpora SLA Checkpoint**“ postupom podľa § 117 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**“).

Článok I.
Predmet Zmluvy

1.1 Predmetom tejto Zmluvy je záväzok Dodávateľa poskytnúť Objednávateľovi nasledovné služby týkajúce sa ochrany koncových zariadení v rámci zabezpečenia informačnej a kybernetickej bezpečnosti Objednávateľa:

a) služby podpory a údržby (SLA) pre Checkpoint v rozsahu a za podmienok uvedených v Prílohe č. 1 Zmluvy,
b) predĺženie servisnej podpory na SW a HW produkty uvedené v Prílohe č. 1 Zmluvy,
c) predĺženie softvérových služieb pre produkty uvedených v Prílohe č. 1 Zmluvy,
d) rozšírenie existujúceho riešenia ochrany pre koncové zariadenia, ktoré je pokryté technológiou Check Point - Harmony Endpoint Advanced v rozsahu a za podmienok uvedených v Prílohe č. 1 Zmluvy

(ďalej spolu aj „**predmet plnenia**“) a záväzok Objednávateľa zaplatiť Dodávateľovi dojednanú cenu predmetu plnenia.

1.2 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 SR pre 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 predmetu plnenia s podmienkami vyplývajúcim z uvedených právnych predpisov sa považuje za vadu predmetu plnenia a Dodávateľ bude povinný odstrániť takýto nesúlad bezodplatne bez zbytočného odkladu.

2.3 Dodávateľ sa zároveň zaväzuje poskytovať služby podpory a údržby pre systém ochrany koncových zariadení Checkpoint Objednávateľa za podmienok uvedených v Prílohe č. 1 k tejto Zmluve tak, aby bola zabezpečená administrácia systému vedúca k zabezpečeniu funkčnosti systému, jeho každodennej prevádzky a údržby podľa požiadaviek Objednávateľa v rozsahu podľa Prílohy č. 1 k Zmluve, ako aj realizácia požiadaviek na zmenu konfigurácie a nastavení systému.

2.4 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.

2.5 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.

2.6 Objednávateľ je povinný počas trvania tejto Zmluvy poskytnúť Dodávateľovi nevyhnutnú súčinnosť potrebnú na dodanie 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.

2.7 Dodávateľ zodpovedá za to, že akákoľvek časť predmetu plnenia nebude obsahovať Objednávateľom nevyžiadané alebo neschválené funkcie a vlastnosti, ktoré súčasne nie sú potrebné. Porušenie tejto povinnosti je podstatným porušením Zmluvy.

2.8 Dodávateľ sa zaväzuje minimalizovať pri poskytovaní služieb také systémové prvky, resp. zabezpečovacie prostriedky, ktoré by v budúcnosti mohli viesť k obmedzeniu konkurenčného prostredia.

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

Článok III.
Čas, miesto a spôsob plnenia

3.1 Zmluvné strany sa dohodli, že Dodávateľ je povinný dodať Objednávateľovi jednotlivé položky predmetu plnenia (okrem služieb podpory a údržby) najneskôr do 10 dní odo dňa účinnosti tejto Zmluvy, nie však neskôr ako 31.10.2024.

3.2 Služby podpory a údržby pre systém ochrany koncových zariadení Checkpoint je Dodávateľ povinný plniť odo dňa účinnosti Zmluvy po celú dobu jej trvania (12 mesiacov) priebežne.

3.3 Služby podpory a údržby bude Dodávateľ poskytovať v sídle Objednávateľa, alebo vzdialeným prístupom za podmienok stanovených v Prílohe č. 4 Zmluvy.

3.4 O odovzdaní každej položky predmetu plnenia podľa Prílohy č. 1 spíšu zmluvné strany preberací protokol, ktorý bude podpísaný oboma zmluvnými stranami. Príslušná položka predmetu plnenia sa pokladá za odovzdanú dňom podpísania preberacieho protokolu. Protokol bude vyhotovený v dvoch rovnopisoch, pričom každá zo strán obdrží jeden rovnopis.

3.5 Dodávateľ sa zaväzuje odovzdať Objednávateľovi všetku dokumentáciu, ktorá je potrebná na riadne užívanie predmetu plnenia.

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. 2 k tejto Zmluve.

5.3 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.

5.4 V cene za predmet plnenia sú zahrnuté všetky náklady Objednávateľa pri poskytovaní služieb údržby a podpory (Príloha č. 1 Zmluvy) počas 12 mesiacov.

Článok VI.
Platobné podmienky

6.1 Nárok Dodávateľa na úhradu ceny za jednotlivé položky predmetu plnenia vzniká po riadnom odovzdaní príslušnej položky predmetu plnenia (okrem služieb údržby a podpory) na základe podpísaného preberacieho protokolu.

6.2 Cena za poskytovanie služieb podpory a údržby podľa Prílohy č. 1 je splatná v mesačných splátkach.

6.3 Daňovým dokladom je pre zmluvné strany faktúra. Dodávateľ je po dodaní predmetu plnenia povinný vystaviť faktúru v elektronickej forme vo formáte .pdf a doručiť ju Objednávateľovi na e-mailovú adresu itpodpora@ntssr.sk najneskôr do 5. pracovného dňa mesiaca nasledujúceho po mesiaci, kedy bol predmet plnenia dodaný.

6.4 V prípade služieb podpory a údržby (Príloha č. 1 Zmluvy) je Dodávateľ povinný doručiť Objednávateľovi faktúru v elektronickej forme na e-mailovú adresu uvedenú v predchádzajúcom bode najneskôr do 5. pracovného dňa mesiaca nasledujúceho po poskytnutí služieb.

6.5 Za správnosť obsahu a zhodu elektronickej faktúry s originálom v systéme predávajúceho zodpovedá výhradne Dodávateľ. Objednávateľ nezodpovedá za nedoručenie elektronickej faktúry z technických príčin medzi Dodávateľom a Objednávateľom. Dodávateľ je následne povinný vystaviť faktúru v písomnej forme doručiť ju Objednávateľovi na adresu sídla najneskôr do 10. pracovného dňa po dodaní predmetu plnenia / poskytnutí služieb.

6.6 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 preberací protokol. Za správne vyhotovenie faktúry zodpovedá v plnom rozsahu Dodávateľ.

6.7 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.

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

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

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

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

Článok VII.
Zodpovednosť za vady

7.1 Dodávateľ zodpovedá za vady predmetu plnenia, ktoré má predmet plnenia v čase protokolárneho odovzdania Objednávateľovi, resp. poskytnutia služby podpory a údržby, a to aj v prípade, ak sa takáto vada stane zjavnou až neskôr.

7.2 Za vady predmetu plnenia sa podľa tejto Zmluvy považuje najmä dodanie predmetu plnenia v rozpore s touto Zmluvou a špecifikáciami, nedostatky alebo odchýlky v kvalitatívnych, technologických a technických parametroch, nedostatok iných parametrov požadovaných Objednávateľom, akékoľvek chyby a nesprávne funkcie predmetu plnenia.

7.3 Dodávateľ poskytuje Objednávateľovi zmluvnú záruku na predmet plnenia najmenej v trvaní 12 mesiacov. Záručná doba začína plynúť momentom protokolárneho odovzdania a prevzatia konkrétnej položky predmetu plnenia. Záručná doba neplynie po dobu od nahlásenia vady po jej odstránenie.

7.4 V prípade, ak má predmetu plnenia vady, za ktoré zodpovedá Dodávateľ, Dodávateľ sa zaväzuje tieto vady odstrániť bez zbytočného odkladu.

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

Článok VIII.
Povinnosť mlčanlivosti

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

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

8.7 Zmluvné strany vyhlasujú, že Dodávateľ nebude mať pri plnení tejto Zmluvy prístup k osobným údajom dotknutých osôb, ktoré spracováva Objednávateľ vo svojich informačných systémoch. V prípade, ak pri poskytovaní služieb podpory a údržby alebo v súvislosti s nimi 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.

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

Článok IX.
Sankcie a náhrada škody

9.1 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.

9.2 V prípade omeškania Dodávateľa s dodaním jednotlivých položiek predmetu plnenia v lehote podľa Článku III. bod 3.1 tejto Zmluvy je Objednávateľ oprávnený uplatniť si voči Dodávateľovi nárok na zaplatenie zmluvnej pokuty vo výške 0,05% z ceny za nedodaný predmet plnenia bez DPH za každý aj začatý deň omeškania.

9.3 V prípade nedodržania reakčného času (lehota nástupu na odstránenie chyby) vymedzeného v Tabuľke 1 Prílohy č. 1 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.

9.4 V prípade omeškania Dodávateľa s odstránením kritickej alebo naliehavej vady podľa Tabuľky 1 Prílohy č. 1 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.

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

9.6 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.

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

9.8 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, vrátane škody vyplývajúcej z prípadného prerušenia prevádzky Objednávateľa v dôsledku, že Dodávateľ neplnil svoje povinnosti riadne, odborne a včas.

9.9 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.

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

9.11 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 X.
Doručovanie

10.1 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.

10.2 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.

10.3 V prípade doručovania prostredníctvom spoločnosti oprávnenej poskytovať poštové služby sa písomnosť považuje za doručenú doručením písomnosti doporučenou poštou na adresu zmluvnej strany; za doručenie písomnosti sa považuje aj okamih, keď adresát odmietol prevziať písomnosť, a to okamihom tohto odmietnutia. V prípade, ak sa písomnosť vráti ako nedoručená z dôvodu, že zmluvná strana je neznáma, zmenila adresu, nevyzdvihla si zásielku v odbernej lehote alebo z iného dôvodu, písomnosť sa považuje za doručenú dňom vrátenia nedoručenej písomnosti odosielateľovi, a to i vtedy, ak sa zmluvná strana o tom nedozvie.

10.4 V prípade doručovania prostredníctvom e-mailu sa písomnosť považuje za doručenú okamihom odoslania zrozumiteľnej, určitej a čitateľnej formy informácie v e - mailovej forme. V prípade, ak je odoslanie ukončené mimo pracovných hodín (8,00 hod. – 16,00 hod.), považuje sa písomnosť za doručenú najbližší nasledujúci pracovný deň.

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

10.6 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.

10.7 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 XI.
Subdodávky

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

11.2 Dodávateľ garantuje spôsobilosť subdodávateľov pre plnenie predmetu Zmluvy.

11.3 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.

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

11.5 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. 5 tejto Zmluvy.

11.6 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.

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

Článok XII.
Trvania a skončenie Zmluvy

12.1 Zmluva sa uzatvára na dobu určitú 12 mesiacov odo dňa jej účinnosti.

12.2 Pred uplynutím dojednaného času je možné Zmluvu ukončiť:
a) písomnou dohodou Zmluvných strán,
b) odstúpením v prípadoch uvedených vo všeobecne záväzných právnych predpisoch a v tejto Zmluve.

12.3 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.

12.4 Zmluvné strany sa dohodli, že za podstatné porušenie Zmluvy budú považovať najmä:

12.4.1 na strane Objednávateľa:
a) omeškanie s poskytnutím nevyhnutnej 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,

12.4.2 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. 1 tejto Zmluvy, ktoré nastane najmenej päťkrát v priebehu troch (3) kalendárnych mesiacov nasledujúcich po sebe,
c) porušenie povinnosti mlčanlivosti,
d) Dodávateľ nemal v čase uzavretia Zmluvy v registri partnerov verejného sektora zapísaných konečných užívateľov výhod, alebo ak bolo právoplatne rozhodnuté o vyčiarknutí tohto predávajúceho z registra partnerov verejného sektora, pričom mal podľa zákona povinnosť mať v registri partnerov verejného sektora zapísaných konečných užívateľov výhod, alebo ak mu bol právoplatne uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní;
e) v čase jej uzavretia existoval dôvod na vylúčenie predávajúceho pre nesplnenie podmienky účasti podľa § 32 ods. 1 písm. a) zákona o verejnom obstarávaní;
f) skončenie Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

12.5 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.

12.6 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 alebo mlčanlivosti.

Článok XIII.
Spoločné a záverečné ustanovenia

13.1 Táto Zmluva je platná dňom jej podpisu oboma zmluvnými stranami. Táto Zmluva nadobúda účinnosť 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.

13.2 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.

13.3 Zmluvné strany sa zaväzujú uzatvoriť spoločne s touto Zmluvou aj Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností uvedenú v Prílohe č. 3 k tejto Zmluve.

13.4 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.

13.5 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.

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

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

13.8 Neoddeliteľnou súčasťou tejto Zmluvy sú jej prílohy:
a) Príloha č. 1 – Opis predmetu zákazky
b) Príloha č. 2 – Štruktúrovaný rozpočet
c) Príloha č. 3 – Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
d) Príloha č. 4 – Podmienky vzdialeného prístupu
e) Príloha č. 5 – Zoznam subdodávateľov

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

13.10 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 15. 10. 2024

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

V Bratislave, dňa 9.10.2024

KOLAS s. r. o.
Ing. Anton Gaľa,
Splnomocnený

Opis predmetu zákazky

Verejný obstarávateľ:	Národná transfúzna služba SR
Názov zákazky:	Navýšenie licencií + technická podpora SLA Checkpoint
Druh zákazky:	Služby
Predmet zákazky:	Predmetom zákazky je navýšenie a obnova licencií ochrany koncových zariadení *Harmony Endpoint Advanced* a Firewallov Checkpoint + zabezpečenie technickej podpory SLA pre Checkpoint
Lehota trvania:	12 mesiacov

Položka č. 1

Požiadavky na SLA - Služby v rámci SLA bude Poskytovateľ dodávať počas trvania zmluvy v pracovnej dobe od 9:00 hod. do 17:00 hod. 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 telefonické požiadavky
- Lehoty nástupu na odstránenie chýb (oprava a výmena firewallov, pre ktoré sa obstaráva predĺženie podpory v časti *Položka č. 2* tohto opisu):

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 zásadný vplyv na prevádzku a plnenie úloh objednávateľa.
Kritickým problémom je napríklad, nie však výlučne:

- Úplná nefunkčnosť 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.

Položka č.2

Názov	Popis	Počet (MJ-ks)
Predĺženie servisnej podpory na SW (Support for Software Gateways) Kód produktu: CPCES-CO-STANDARD	Predĺženie podpory na 1 rok na SW: *Check Point - Next Generation Security Management Software for 25 gateways*	1

Položka č.3

Názov	Popis	Počet (MJ-ks)
Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-STANDARD-ADD	Predĺženie podpory na 1 rok na montážne súčiastky do rozvádzača pre modely Check Point 1570 a 1590 (Support for Rack Mount ears for 1570 and 1590 models) Typ podpory – Collaborative Úroveň podpory: STANDARD	1

Položka č.4

Názov	Popis	Počet (MJ-ks)
Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1590-BUN-ADD	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM; 7x24 každý deň, záväzný čas odozvy – 4 hodiny	2

Položka č.5

Názov	Popis	Počet (MJ-ks)
Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1800-ADD	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM; 7x24 každý deň, záväzný čas odozvy – 4 hodiny	2

Položka č.6

Názov	Popis	Počet (MJ-ks)
Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1570-ADD	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM; 7x24 každý deň, záväzný čas odozvy – 4 hodiny	11

Položka č.7

Názov	Popis	Počet (MJ-ks)
Predĺženie softvérovej služby pre ochranu koncového zariadenia Kód produktu: CP-HAR-EP-ADVANCED-REN-1Y	Subskripcia produktu *Harmony Endpoint Advanced* zahŕňa nasledovné: Sandboxing, Web Protection, Attack Investigation, Threat Prevention, Access Control and Threat Intelligence Predĺženie služby na 1 rok	300

Položka č.8

Názov	Popis	Počet (MJ-ks)
Predĺženie softvérovej služby pre Firewall novej generácie, ktorý identifikuje a riadi aplikácie a kontroluje obsah s IPS na odvrátenie zneužitia, umožňuje používateľskú politiku. Kód produktu: CPSB-NGFW-1570-BUN-1Y	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa: Firewall; Identity Awareness; IPsec VPN; Content Awareness; Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	11

Položka č.9

Názov	Popis	Počet (MJ-ks)
Predĺženie softvérovej služby pre Firewall novej generácie, ktorý identifikuje a riadi aplikácie a kontroluje obsah s IPS na odvrátenie zneužitia, umožňuje používateľskú politiku. Kód produktu: CPSB-NGFW-1590-BUN-1Y	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa: Firewall; Identity Awareness; IPsec VPN; Content Awareness; Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	2

Položka č.10

Názov	Popis	Počet (MJ-ks)
Predĺženie softvérovej služby pre Firewall novej generácie zahŕňajúci balík SandBlast, ktorý obsahuje NGTP a pridáva najnovšiu bezpečnosť Zero-Phishing spolu s pokročilým sandboxingom a Content Disarm & Reconstruction (CDR) k ochrane pred neznámymi a zero-day útokmi Kód produktu: CPSB-SNBT-1800-1Y	(Annuity Blades) Firewall; Identity Awareness; IPsec VPN; Content Awareness; Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional; URL-Filtering; Anti-Virus; Anti-Spam; Anti-Bot; DNS Security; SandBlast Threat Emulation; SandBlast Threat Extraction; Zero-Phishing	2

Položka č.11

Názov	Popis	Počet (MJ-ks)
Predĺženie existujúcej softvérovej služby pre dvojfaktorovú autentifikáciu Kód produktu: FAC-VM-Base; FC1-10-0ACVM-248-02-12	Názov: FortiAuthenticator-VM, Base FortiAuthenticator-VM; SW podpora, FortiCare Premium (1 - 500 USERS) do 31.10.2025	1

Položka č.12

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. 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 integrovanú funkciu IPSec VPN pre existujúci firewall. Riešenie musí podporovať tzv. Split Tunnelling, t. j. možnosť prístupu k internetovým stránkam 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 jednorazové 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,	250

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 infiltráciu 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 forenzných 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 šifrovanie 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 používa, Integrácia 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. Jedná sa o rozšírenie existujúceho riešenia, ktoré je pokryté technológiou Check Point – Harmony Endpoint Advanced.	

Sumarizácia položiek:

PČ	Názov	Popis produktu	Množstvo
1.	SLA	Poskytovanie služieb na obdobie 1 roka v zmysle opisu k položke č. 1 (merná jednotka = človekodeň)	48
2.	Predĺženie servisnej podpory na SW (Support for Software Gateways) Kód produktu: CPCES-CO-STANDARD	Predĺženie podpory na 1 rok na SW: *Check Point - Next Generation Security Management Software for 25 gateways*	1
3.	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-STANDARD-ADD	Predĺženie podpory na 1 rok na montážne súčiastky do rozvádzača pre modely Check Point 1570 a 1590 (Support for Rack Mount ears for 1570 and 1590 models) Typ podpory – Collaborative Úroveň podpory: STANDARD	1
4.	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1590-BUN-ADD	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM; 7x24 každý deň, záväzný čas odozvy – 4 hodiny	2
5.	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1800-ADD	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM; 7x24 každý deň, záväzný čas odozvy – 4 hodiny	2
6.	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1570-ADD	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM; 7x24 každý deň, záväzný čas odozvy – 4 hodiny	11
7.	Predĺženie softvérovej služby pre ochranu koncového zariadenia Kód produktu: CP-HAR-EP-ADVANCED-REN-1Y	Subskripcia produktu *Harmony Endpoint Advanced* zahŕňa nasledovné: Sandboxing, Web Protection, Attack Investigation, Threat Prevention, Access Control and Threat Intelligence Predĺženie služby na 1 rok	300
8.	Predĺženie softvérovej služby pre Firewall novej generácie, ktorý identifikuje a riadi aplikácie a kontroluje obsah s IPS na odvrátenie zneužitia, umožňuje používateľskú politiku. Kód produktu: CPSB-NGFW-1570-BUN-1Y	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa: Firewall; Identity Awareness; IPsec VPN; Content Awareness; Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	11
9.	Predĺženie softvérovej služby pre Firewall novej generácie, ktorý identifikuje a riadi aplikácie a kontroluje obsah s IPS na	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa: Firewall; Identity Awareness; IPsec VPN; Content Awareness; Mobile Access; IPS;	2

	odvrátenie zneužitia, umožňuje používateľskú politiku. Kód produktu: CPSB-NGFW-1590-BUN-1Y	Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	
10.	Predĺženie softvérovej služby pre Firewall novej generácie zahŕňajúci balík SandBlast, ktorý obsahuje NGTP a pridáva najnovšiu bezpečnosť Zero-Phishing spolu s pokročilým sandboxingom a Content Disarm & Reconstruction (CDR) k ochrane pred neznámymi a zero-day útokmi Kód produktu: CPSB-SNBT-1800-1Y	(Annuity Blades) Firewall; Identity Awareness; IPsec VPN; Content Awareness; Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional; URL-Filtering; Anti-Virus; Anti-Spam; Anti-Bot; DNS Security; SandBlast Threat Emulation; SandBlast Threat Extraction; Zero-Phishing	2
11.	Predĺženie softvérovej služby pre dvojfaktorovú autentifikáciu Kód produktu: FAC-VM-Base; FC1-10-0ACVM-248-02-12	Názov: FortiAuthenticator-VM, Base FortiAuthenticator-VM; SW podpora, FortiCare Premium (1 - 500 USERS) do 31.10.2025	1
12.	Rozšírenie existujúceho riešenia ochrany koncových zariadení, ktoré je pokryté technológiou Check Point – Harmony Endpoint Advanced.	Rozšírenie existujúceho riešenia Check Point – Harmony Endpoint Advanced o 1 ks	250

Miesta plnenia:

1	Bratislava, Riaditeľstvo + SC	Ďumbierská 3/L, 831 01 Bratislava
2	Bratislava, OC Ružinov	Ružinovská 6, 821 02 Bratislava
3	Bratislava, OC Kramáre	Limbová 3, 833 14 Bratislava
4	OC Nové Zámky	Slovenská 11/A, 940 34 Nové Zámky
5	OC Žilina	Vojtecha Spanyola 43, 010 01 Žilina
6	Banská Bystrica, OC L. Svobodu 1	Námestie L. Svobodu 1, 975 17 Banská Bystrica
7	Banská Bystrica SC Jaseňova 7	Jaseňova 7, 974 09 Banská Bystrica
8	OC Prešov	Jána Hollého 14, 080 01 Prešov
9	OC Košice	Trieda SNP 1, 040 11 Košice
10	OC Trnava	Andreja Žarnova 11, 917 02 Trnava
11	OC Trenčín	Legionárska 28, 911 01 Trenčín
12	OC Nitra	Špitálska 6, 949 01 Nitra
13	OC Poprad	Banícka 803/28, 058 45 Poprad
14	OC Martin	Priehradka 18A, 036 01 Martin

Vzor štruktúrovaného rozpočtu ceny

Verejný obstarávateľ:
Národná transfúzna služba SR, Ďumbierska 3/L, 831 01 Bratislava
Predmet zákazky:
Navýšenie licencií + technická podpora SLA Checkpoint
Postup verejného obstarávania:
Podlimitná zákazka

Uchádzač:
KOLAS a. r. o., Sebranlho 1, 821 03 Bratislava

Štruktúrovaný rozpočet ceny

ROZPOČET

A	B	C	D	E	F	G	H	I	J	K	L	M
POLOŽKA č.	Názov položky	Merná jednotka (MJ)	Opis položky	Obchodný názov	Predpokladané množstvo MJ	Cena za MJ (EUR)				Cena ze predpokladané množstvo MJ (EUR)		
						bez DPH	Sadzba DPH (%)	DPH	s DPH	bez DPH	DPH	s DPH
A	B	C	D	E	F	G	H	G/100 x H	G + I	F x G	K/100 x H	K + L
1	SLA	ks	Poskytovanie služieb na obdobie 1 roka v zmysle opisu k položke č. 1 (merná jednotka = človekoden)	SLA	48	610,00	20	122,00	732,00	29280,00	5856,00	35136,00
2	Predĺženie servisnej podpory na SW (Support for Software Gateways) Kód produktu: CPCES-CO-STANDARD	ks	Predĺženie podpory na 1 rok na SW: Check Point - Next Generation Security Management Software for 25 gateways	Predĺženie podpory na 1 rok na SW: Check Point - Next Generation Security Management Software for 25 gateways Support for Software Gateways; Software Sync Fees Kód produktu CPCES-CO-PREMIUMPRO	1	8838,00	20	1767,20	10603,20	8838,00	1767,20	10603,20
3	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-STANDARD-ADD	ks	Predĺženie podpory na 1 rok na montážne súčiastky do rozvádzača pre modely Check Point 1570 a 1590 (Support for Rack Mount ears for 1570 and 1590 models) Typ podpory – Collaborative Úroveň podpory: STANDARD	Predĺženie podpory na 1 rok na montážne súčiastky do rozvádzača pre modely Check Point 1570 a 1590 (Support for Rack Mount ears for 1570 and 1590 models) Typ podpory – Collaborative Úroveň podpory: STANDARD	1	37,00	20	7,40	44,40	37,00	7,40	44,40
4	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1580-BUN-ADD	ks	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM, 7x24 každý deň, záväzný čas odozvy – 4 hodiny	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM, 7x24 každý deň, záväzný čas odozvy – 4 hodiny Kód produktu: CPCES-CO-PREMIUMPRO-1580-BUN-ADD	2	508,00	20	101,60	609,60	1016,00	203,20	1219,20
5	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1900-ADD	ks	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM, 7x24 každý deň, záväzný čas odozvy – 4 hodiny	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM, 7x24 každý deň, záväzný čas odozvy – 4 hodiny Kód produktu CPCES-CO-PREMIUMPRO-1900-BUN-ADD	2	993,00	20	198,60	1191,60	1986,00	397,20	2383,20
6	Predĺženie servisnej podpory na HW (Support for Appliance Gateways) Kód produktu: CPCES-CO-PREMIUM-1570-ADD	ks	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM, 7x24 každý deň, záväzný čas odozvy – 4 hodiny	Predĺženie podpory na 1 rok Typ podpory – Collaborative Úroveň podpory: PREMIUM, 7x24 každý deň, záväzný čas odozvy – 4 hodiny Kód produktu CPCES-CO-PREMIUMPRO-1570-BUN-ADD	11	250,00	20	50,00	300,00	2750,00	550,00	3300,00
7	Predĺženie softvérovej služby pre ochranu koncového zariadenia Kód produktu: CP-HAR-EP-ADVANCED-REN-1Y	ks	Subskripcia produktu Harmony Endpoint Advanced zahŕňa nasledovné: Sandboxing, Web Protection, Attack Investigation, Threat Prevention, Access Control and Threat Intelligence Predĺženie služby na 1 rok	Subskripcia produktu Harmony Endpoint Advanced zahŕňa nasledovné: Sandboxing, Web Protection, Attack Investigation, Threat Prevention, Access Control and Threat Intelligence Predĺženie služby na 1 rok Kód produktu: CP-HAR-EP-ADVANCED-REN-1Y	300	51,00	20	10,20	61,20	15300,00	3060,00	18360,00
8	Predĺženie softvérovej služby pre Firewall novej generácie, ktorý identifikuje a riadi aplikácie a kontroluje obsah s IPS na odvrátenie zneužitia, umožňuje používateľskú politiku. Kód produktu: CPSB-NGFW-1570-BUN-1Y	ks	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa Firewall; Identity Awareness; IPsec VPN, Content Awareness; Mobile Access; IPS, Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa Firewall, Identity Awareness, IPsec VPN, Content Awareness; Mobile Access, IPS; Application Control; SD-WAN optional, IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	11	414,00	20	82,80	496,80	4554,00	910,80	5464,80
9	Predĺženie softvérovej služby pre Firewall novej generácie, ktorý identifikuje a riadi aplikácie a kontroluje obsah s IPS na odvrátenie zneužitia, umožňuje používateľskú politiku. Kód produktu: CPSB-NGFW-1580-BUN-1Y	ks	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa Firewall; Identity Awareness; IPsec VPN, Content Awareness, Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	(Annuity Blades) Balík bezpečnostného softvéru zahŕňa Firewall, Identity Awareness, IPsec VPN; Content Awareness, Mobile Access, IPS; Application Control, SD-WAN optional; IoT Protect optional; Data Loss Prevention optional Predĺženie služby na 1 rok	2	572,00	20	114,40	686,40	1144,00	228,80	1372,80
10	Predĺženie softvérovej služby pre Firewall novej generácie zahŕňajúci balík SandBlast, ktorý obsahuje NGTP a pridáva najnovšiu bezpečnosť Zero-Phishing spolu s pokročilým sandboxingom a Content Disarm & Reconstruction (CDR) k ochrane pred neznámymi a zero-day útokmi Kód produktu: CPSB-SNBT-1900-1Y	ks	(Annuity Blades) Firewall, Identity Awareness; IPsec VPN, Content Awareness, Mobile Access; IPS, Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional; URL-Filtering; Anti-Virus, Anti-Spam, Anti-Bot, DNS Security; SandBlast Threat Emulation, SandBlast Threat Extraction; Zero-Phishing	(Annuity Blades) Firewall; Identity Awareness, IPsec VPN, Content Awareness, Mobile Access; IPS; Application Control; SD-WAN optional; IoT Protect optional; Data Loss Prevention optional; URL-Filtering; Anti Virus; Anti-Spam, Anti-Bot, DNS Security; SandBlast Threat Emulation, SandBlast Threat Extraction; Zero-Phishing	2	2655,00	20	531,00	3186,00	5310,00	1062,00	6372,00
11	Predĺženie softvérovej služby pre dvojfaktorovú autentifikáciu Kód produktu: FAC-VM-Base; FC1-10-0ACVM-248-02-12	ks	Názov: FortiAuthenticator-VM, Base FortiAuthenticator-VM; SW podpora, FortiCare Premium (1 - 500 USERS) do 31.10.2025	Názov: FortiAuthenticator-VM, Base FortiAuthenticator-VM, SW podpora, FortiCare Premium (1 - 500 USERS) do 31.10.2025	1	421,00	20	84,20	505,20	421,00	84,20	505,20
12	Rozšírenie existujúceho riešenia ochrany koncových zariadení, ktoré je pokryté technológiou Check Point – Harmony Endpoint Advanced.	ks	Rozšírenie existujúceho riešenia Check Point – Harmony Endpoint Advanced o 1 ks	Rozšírenie existujúceho riešenia Check Point – Harmony Endpoint Advanced o 1 ks	250	51,00	20	10,20	61,20	12750,00	2550,00	15300,00
									Celková cena v EUR s DPH			100 060,80 €

Uchádzač vyplní príslušné riadky vpísaním údajov

Údaje vypíni uchádzač

Vstupné hodnoty

Kritérium

Uchádzač: KOLAS a. r. o., Sebranlho 1, 821 03 Bratislava

Národná transfúzna služba SR
NTS

Národná transfúzna služba SR
Ďumbierska 3/L
831 01 BRATISLAVA

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená 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 k□bernetickej bezpečnosti**“)
(ďalej len „**zmluva**“)

medzi zmluvnými stranami:

Prevádzkovateľ:	**Národná transfúzna služba SR**
Sídlo:	Ďumbierska 3/L, 831 01 Bratislava
IČO:	30853915
DIČ :	2021764371
IČ DPH :	SK2021764371
Štatutárny orgán:	Ing. Ivan Oleár, MBA, riaditeľ
Zapísaný:	štátna príspevková organizácia zriadená Zriaďovacou listinou vydanou Ministerstvom zdravotníctva Slovenskej republiky, zo dňa 2.12.2003, č. 03775-4/2003

(ďalej len „**Prevádzkovateľ základnej služb□**')

a

Dodávateľ:	KOLAS s. r. o.
Sídlo/miesto podnikania:	Seberíniho 1, 821 03 Bratislava
IČO:	47060476
IČ DPH:	SK2023758495
DIČ:	2023758495
Štatutárny zástupca:	Mgr. Iveta Gaľová – konateľ
Zapísaná:	Obchodný register Mestského súdu Bratislava III, oddiel: Sro, vložka č. 87961/B

(ďalej len „**Dodávateľ**"')
(Prevádzkovateľ základnej služby a Dodávateľ spolu ďalej len „**zmluvné stran□**“)

Národná transfúzna služba SR
Ďumbierska 3/L
831 01 BRATISLAVA

Článok I.
ÚVODNÉ USTANOVENIA

1. **Národná transfúzna služba** je Prevádzkovateľom základnej služby podľa zákona o kybernetickej bezpečnosti.
2. Identifikovanými základnými službami Prevádzkovateľa základnej služby sú:
   a) správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,
   b) služba, ktorá je prvkom kritickej infraštruktúry alebo informačný systém, ktorý je k nej priamo pripojené.
3. Dodávateľ uzatvára s Prevádzkovateľom základnej služby Zmluvu pod názvom: *Zmluva o poskytnutí služieb podpory a údržby a navýšení a obnovy licencií ochrany koncových zariadení* (ďalej len „**Zmluva**"), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov ako sú definované v zákone o kybernetickej bezpečnosti pre Prevádzkovateľa základnej služby.
4. Prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti.
5. Zmluva stanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa základnej služby, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany prevádzkovateľa základnej služby (ďalej len **„ciele"),** a to aj v spolupráci s Dodávateľom.
6. Plnenie povinností podľa tejto zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania zmluvy.

Článok II.
ZÁKLADNÉ POJMY

Na účely tejto zmluvy sa rozumie:

a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,

Národná transfúzna služba SR
Ďumbierska 3/L
831 01 BRATISLAVA

b) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,
c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
d) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
e) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
g) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,
h) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
i) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
j) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
   - strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
   - vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
   - ohrozenie bezpečnosti informácií,
k) základnou službou služba, ktorá je zaradená v zozname základných služieb a
   - závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona o kybernetickej bezpečnosti,
   - je informačným systémom verejnej správy, alebo
   - je prvkom kritickej infraštruktúry,
l) prevádzkovateľom základnej služby Národná transfúzna služba SR, ktorá prevádzkuje službu, ktorá je prvkom kritickej infraštruktúry,
m) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2 zákona o kybernetickej bezpečnosti,
n) manažér kybernetickej a informačnej bezpečnosti (MKIB) je osoba poverená riadením informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti definované v Politike informačnej bezpečnosti a ďalších smerniciach Prevádzkovateľa základnej služby. Ide najmä o kontrolné činnosti, riešenie bezpečnostných a kybernetických incidentov, riadenie implementácie bezpečnostných

opatrení, konzultačné a metodické činnosti pre oblasť informačnej a kybernetickej bezpečnosti a ďalšie,

o) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

Článok III.
PREDMET ZMLUVY

1. V zmysle § 19 ods. 2 zákona o kybernetickej bezpečnosti a s ohľadom na Zmluvu je predmetom tejto zmluvy stanovenie práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Článok IV.
POVINNOSTI DODÁVATEĽA

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam bezpečnostných opatrení Prevádzkovateľa základnej služby ktoré sú súčasťou jeho bezpečnostných politík a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v prílohe č. 2 tejto zmluvy (ďalej aj ako „**bezpečnostné politik**“). Dodávateľ berie na vedomie, že príloha č. 2 zmluvy bude predmetom ochrany podľa zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov jej obsah nebude podľa § 11 ods. 1 písm. c) zákona č. 185/2015 Z.z. zverejnené. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o obsahu bezpečnostných politík Prevádzkovateľa.
2. Dodávateľ sa zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa.
3. Dodávateľ súhlasí s tým, že bezpečnostné politiky Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa základnej služby a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby. Zmenené bezpečnostné politiky Prevádzkovateľa základnej služby sú pre Dodávateľa záväzné od momentu, kedy nimi Prevádzkovateľ preukázateľne oboznámil Dodávateľa.
4. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto zmluvy.
5. Dodávateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role a

technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto zmluvy.

6. Odplata za plnenie povinností Dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom základnej služby Dodávateľovi podľa Zmluvy a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy od Prevádzkovateľa základnej služby nemá nárok.
7. Dodávateľ sa zaväzuje, že nezapojí ďalšieho dodávateľa (ďalej len „**subdodávateľ**“) úplne alebo čiastočne zabezpečujúceho plnenie tejto zmluvy predtým, než dostane písomný súhlas Prevádzkovateľa základnej služby. Zoznam subdodávateľov v rozsahu podľa ust. § 41 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov tvorí prílohu č. 3 tejto zmluvy. Dodávateľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Dodávateľa uvedené v tejto zmluve. Dodávateľ je plne zodpovedný voči Prevádzkovateľovi základnej služby za plnenie povinností subdodávateľa tak, ako by ich poskytoval sám.
8. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Prevádzkovateľa základnej služby podľa Zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania Zmluvy.

Článok V.
BEZPEČNOSTNÉ OPATRENIA

1. Dodávateľ sa zaväzuje pri plnení Zmluvy dodržiavať bezpečnostné opatrenia implementované Prevádzkovateľom minimálne v rozsahu interných politík a smerníc Prevádzkovateľa, ktoré sú uvedené v prílohe č. 2 tejto zmluvy.
2. Bezpečnostné opatrenia musia zahŕňať najmenej:
   - Detekciu kybernetických bezpečnostných incidentov,
   - Evidenciu kybernetických bezpečnostných incidentov,
   - Postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
   - Určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
3. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu v organizácii.

Článok VI.
PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

Národná transfúzna služba SR
Ďumbierska 3/L
831 01 BRATISLAVA

1. Dodávateľ sa zaväzuje v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby (ďalej len „**incident**"):
   a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa základnej služby,
   b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy a tejto zmluvy alebo budú mať prístup k informáciám Prevádzkovateľa základnej služby,
   c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
   d) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
   e) predchádzať vzniku incidentov,
   f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
   g) prijímať od Prevádzkovateľa základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
   h) zasielať Prevádzkovateľovi základnej služby včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak a
   i) spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby.
2. Dodávateľ sa zaväzuje počas trvania tejto zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto zmluvy.
3. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí sa budú podieľať na plnení Zmluvy a tejto zmluvy a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby, je uvedený v prílohe č. 1. tejto zmluvy. Dodávateľ je povinný písomne oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení a to bezodkladne po tom, ako táto zmena v personálnom obsadení nastane; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení podľa tohto bodu.
4. Dodávateľ sa zaväzuje stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu;

bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi základnej služby na nahliadnutie a zhotovenie kópií.

Článok VII.
POSTUP PRI RIEŠENÍ INCIDENTOV

1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý incident Prevádzkovateľovi základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Dodávateľ sa zaväzuje riešiť incidenty najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len „**reaktívne opatrenie**"). Pri riešení incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a Ministerstvom zdravotníctva Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.
3. Dodávateľ sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby.
4. Dodávateľ sa zaväzuje oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.
6. Po vyriešení incidentu je Dodávateľ na výzvu Prevádzkovateľa základnej služby v určenej lehote povinný predložiť Prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „**ochranné opatrenia**") na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom základnej služby na jeho návrhu.
7. Po schválení ochranného opatrenia Prevádzkovateľom základnej služby, je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní ochranného opatrenia Dodávateľom, je Dodávateľ povinný preveriť jeho účinnosť.

Článok VIII.
ZÁVÄZOK MLČANLIVOSTI

1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením Zmluvy a tejto zmluvy, a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti. Dodávateľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby. Dodávateľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Dodávateľovi.
2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.
4. Dodávateľ sa zaväzuje zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu, obchodného vzťahu alebo iného vzťahu.
5. Po ukončení tejto zmluvy je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. tieto podľa pokynu Prevádzkovateľa základnej služby zničiť.

Článok IX.
KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Dodávateľ sa zaväzuje komunikovať pri plnení povinností podľa tejto zmluvy s Prevádzkovateľom základnej služby spôsobom určeným Prevádzkovateľom základnej služby, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.
3. Dodávateľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.
4. Kontaktné osoby podľa prílohy č. 1 tejto zmluvy môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia tejto zmluvy o doručovaní (článok X., bod 9.,10. a 11.).

Článok X.
SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení,

bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

2. Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
4. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto zmluvy v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
5. Dodávateľ sa zaväzuje dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania incidentov a dokumentovania bezpečnostných školení svojich zamestnancov) a na žiadosť Prevádzkovateľa základnej služby mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
6. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy bezodkladne, pokiaľ to nie je v tejto zmluve alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
7. V prípade, ak Dodávateľ plní zmluvu prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby, Dodávateľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto zmluvy aj u týchto subdodávateľov.
8. V prípade, ak Dodávateľ spôsobí Prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov. Pre odstránenie právnych pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla

Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.

9. V prípade porušenia záväzkov Dodávateľa podľa tejto zmluvy sa zodpovednosť Dodávateľa a náhrada škody spravujú ustanoveniami Zmluvy.
10. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej zmluvnej strane (ďalej len „**písomnosti**") musia byť doručené, ak zmluva neustanovuje inak:
    a) v písomnej forme prostredníctvom pošty doporučene s doručenkou; za deň doručenia sa považuje dátum prevzatia zásielky alebo
    b) osobne do sídla druhej zmluvnej strany.
11. Miestom pre doručovanie písomností sú adresy zmluvných strán uvedené v záhlaví tejto zmluvy. Každá zo zmluvných strán je povinná písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu ohľadne doručovania, a to najneskôr do 5 pracovných dní po tom, čo k takejto zmene dôjde. Pokiaľ sa z dôvodu oneskoreného alebo nevykonaného oznámenia o zmene miesta doručovania nepodarí včas a riadne doručiť písomnosť druhej zmluvnej strane, považuje sa deň neúspešného pokusu o opakované doručenie písomnosti za deň doručenia písomnosti druhej zmluvnej strane so všetkými právnymi dôsledkami pre dotknutú zmluvnú stranu.
12. Dodávateľ sa zaväzuje oznamovať všetky skutočnosti majúce vplyv na zmluvu, ako aj hlásiť ďalšie informácie požadované Prevádzkovateľom základnej služby, písomne na adresu sídla Prevádzkovateľa základnej služby.

Článok XI.
AUDIT KYBERNETICKEJ BEZPEČNOSTI

1. Prevádzkovateľ základnej služby je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto zmluvy.
2. V prípade, ak je Dodávateľ prevádzkovateľom základnej služby alebo sa stane prevádzkovateľom základnej služby počas trvania tejto zmluvy, Dodávateľ je oprávnený nahradiť vykonanie auditu podľa bodu 1. tohto článku zmluvy predložením informácie o výsledkoch vlastného auditu oprávnenou osobou Prevádzkovateľovi spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.
3. Prípadné nedostatky zistené auditom Prevádzkovateľa základnej služby (bod 1. tohto článku zmluvy) alebo treťou osobou (bod 2. tohto článku zmluvy) je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní alebo v lehote, s ktorou Dodávateľ písomne súhlasil v auditnej správe vytvorenej Prevádzkovateľom alebo treťou osobou.

4. Prevádzkovateľ základnej služby môže audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
5. Dodávateľ sa zaväzuje pri audite spolupracovať s Prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
6. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
7. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi základnej služby súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
8. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej 30 (tridsať) pracovných dní vopred svoj zámer realizovať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
10. Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku VIII. ods. 2, 3 a 4 tejto zmluvy sa uplatňujú primerane.
11. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa 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 podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ sa zaväzuje preukázateľne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ 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 platných pre priestory Dodávateľa.

Článok XII.
ZÁVEREČNÉ USTANOVENIA

1. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania Zmluvy alebo iného jej ukončenia.
2. Prevádzkovateľ základnej služby je oprávnený od tejto zmluvy písomne odstúpiť v prípade (i) podstatného porušenia tejto zmluvy zo strany Dodávateľa, alebo (ii) v prípade nepodstatného porušenia, ak Dodávateľ neodstráni takéto porušenie a/alebo jeho následky ani v dodatočnej lehote určenej Dodávateľom. Odstúpenie od tejto zmluvy je platné a účinné dňom preukázateľného doručenia písomného odstúpenia od tejto zmluvy Dodávateľovi.
3. Za podstatné porušenie zmluvy sa považuje:
   a) porušenie povinností Dodávateľom uvedených v čl. IV ods. 1, 8, čl. VI. ods. 3, 4, čl. VII a čl. VIII tejto zmluvy;
   b) ak Dodávateľ vedel v čase uzavretia zmluvy alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola zmluva uzavretá, že Prevádzkovateľ základnej služby nebude mať záujem na plnení povinností pri takom porušení zmluvy;
   c) Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto zmluvy.
4. Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto zmluvy medzi Dodávateľom a Prevádzkovateľom základnej služby je zákonnou povinnosťou Prevádzkovateľa základnej služby. Z uvedeného dôvodu je Prevádzkovateľ základnej služby v prípade skončenia platnosti tejto zmluvy oprávnený bez ďalšieho odstúpiť od Zmluvy.
5. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán.
6. Zrušenie tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy.
7. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.
8. Táto zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
9. Prípadné spory vyplývajúce z tejto zmluvy budú riešené predovšetkým mimosúdne. Podpisom tejto zmluvy zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto zmluvy sú príslušné súdy Slovenskej republiky.
10. Táto zmluva sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo zmluvy nevyplýva niečo iné.

Národná transfúzna služba SR
Ďumbierska 3/L
831 01 BRATISLAVA

11. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto zmluvy na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
12. Ak niektoré ustanovenia tejto zmluvy budú zmluvné strany, súd alebo iné kompetentné orgány považovať za neplatné alebo nevymáhateľné, potom takéto ustanovenie bude neplatné iba v dotknutom a v najužšom možnom rozsahu, pričom jeho zvyšná časť, význam a dopady, ako aj ostatné ustanovenia tejto zmluvy zostávajú v platnosti. Zmluvné strany budú v takom prípade postupovať tak, aby účel ustanovení považovaných za nevymáhateľné alebo neplatné bol v maximálne možnej miere rešpektovaný a pre zmluvné strany právne záväzný vo forme umožňujúcej jeho právnu vymáhateľnosť.
13. Táto zmluva tvorí úplnú dohodu medzi zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto zmluvy zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto zmluvy a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto zmluve neuvedených, ústnych alebo písomných dojednaní a dohôd.
14. Táto zmluva bola vyhotovená v šiestich rovnopisoch, a to v štyroch rovnopisoch pre Prevádzkovateľa základnej služby a vo dvoch rovnopisoch pre Dodávateľa.
15. Táto zmluva nadobúda platnosť a účinnosť dňom podpisu oboma zmluvnými stranami.
16. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
    - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa
17. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah zmluvy dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

V Bratislave dňa 11. 10. 2024

Prevádzkovateľ základnej služby:

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

V Bratislave, dňa 09.10.2024

Dodávateľ:

Ing. Anton Gaľa,
splnomocnený
KOLAS s. r. o.

Príloha č. 4

Podmienky vzdialeného prístupu

- spoločnosti KOLAS s. r. o., Seberíniho 1, 821 03 Bratislava, IČO: 47060476

(ďalej len „Poskytovateľ")

k Zmluve o poskytnutí služieb podpory a údržby a navýšení a obnovy licencií ochrany koncových zariadení

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
Seberíniho 1, 821 03 Bratislava
(ďalej len „Názov")

1 Vzdialený prístup

1.1 Systémom pre účely tejto Prílohy č. 1 sa rozumie „Navýšenie licencií + technická podpora SLA Checkpoint", 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: . 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 oprávnení 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 je plne v kompetencii Objednávateľa a jeho údržba je plne v kompetencii Poskytovateľa alebo jeho subdodávateľa.

2.2 Poskytovateľ požiada o vytvorenie prístupu e-mailom na itpodpora@ntssr.sk. 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.

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. 5 Zmluvy

VYHLÁSENIE UCHÁDZAČA O SUBDODÁVKACH

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

..... KOLAS s. r. o., Seberíniho 1, 821 03 Bratislava, IČO: 47060476 .....

Dolu podpísaný zástupca uchádzača týmto vyhlasujem, že v rámci realizácie predmetu zákazky s názvom **„Navýšenie licencií + technická podpora SLA Checkpoint“** 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 9.10.2024

.....

Ing. Anton Gaľa, splnomocnený
podpis (štatutár alebo splnomocnená osoba)