52/23

ZMLUVA O ODBORNÝCH SLUŽBÁCH
Číslo zmluvy ZML/0017/2023

Článok č. 1. Zmluvné strany

Klient: **Národný ústav detskej tuberkulózy a respiračných chorôb, n. o. Dolný Smokovec**
058 81 Dolný Smokovec – Vysoké Tatry

Konajúci prostredníctvom:	Ing. Miroslava Mištunová, PhD., MPH
IČO:	37886479
DIČ:	2021819327
IČ pre DPH:	SK 2021819327
Bankové spojenie:	VÚB Poprad
IBAN:	SK73 0200 0000 0000 2883 2562
SWIFT:	SUBASKBX

Nezisková organizácia je zapísaná v registri NO Okresným úradom v Prešove pod č.OVVS-80/2004 dňa 1. apríla 2004

(ďalej len „**Klient**", „**Prevádzkovateľ základnej služby**" alebo „**PZS**")

Dodávateľ: **Kompetenčné a certifikačné centrum kybernetickej bezpečnosti**
Na družstvo 125
916 25 Brunovce

Konajúci prostredníctvom:	Ing. Ivan Makatura
IČO:	52839052
DIČ:	2121156345
IČ pre DPH:	-
Bankové spojenie:	Štátna pokladnica
IBAN:	SK9181800000007000639084
SWIFT:	SPSRSKBAXXX

(ďalej len „**dodávateľ**")

Klient a dodávateľ sa ďalej označujú jednotlivo ako „**zmluvná strana**" a spoločne ako „**zmluvné strany**". Táto Zmluva o odborných službách sa ďalej označuje spoločne s jej prílohami ako „zmluva". Zmluvné strany s úmyslom byť viazané podmienkami uvedenými nižšie uzatvárajú túto zmluvu o odborných službách podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v platnom znení (ďalej len „**Obchodný zákonník**").

Článok č. 2. Predmet zmluvy

2.1. Dodávateľ sa zaväzuje poskytnúť klientovi služby vymedzené v Článok č. 3. tejto zmluvy v súlade s podmienkami dohodnutými v tejto zmluve (ďalej len „**služby**" a klient sa zaväzuje uhradiť za poskytnuté služby dodávateľovi odmenu dohodnutú v Článok č. 5. Článok č. 4. tejto zmluvy.

Článok č. 3. Rozsah služieb – Audit kybernetickej bezpečnosti

3.1. Predmetom zmluvy je záväzok dodávateľa vykonať audit kybernetickej bezpečnosti klienta tak, ako je bližšie špecifikované v bode 3.5 nižšie, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení (ďalej len „**zákon**"), príslušnej Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z. (ďalej len „**Vyhláška o bezpečnostných opatreniach**") ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a Vyhlášky Národného bezpečnostného úradu č. 493/2022 Z.z. (ďalej len „**Vyhláška o audite**") o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

3.2. Dodávateľ sa v rámci auditu kybernetickej bezpečnosti zaväzuje zabezpečiť výkon auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti(ďalej len „**Audítor kybernetickej bezpečnosti**") podľa Vyhlášky o audite, ktorý spĺňa všetky požiadavky na výkon auditu.

3.3. Dodávateľ je oprávnený použiť na splnenie predmetu tejto zmluvy subdodávateľov, za predpokladu, že s nimi uzatvoril písomnú zmluvu a o zapojení subdodávateľa vopred informoval klienta. Tým nie je dotknutá zodpovednosť za splnenie predmetu tejto zmluvy.

3.4. Zmluvné strany sa dohodli, že predmet zmluvy sa považuje za splnený riadne a včas dňom predloženia záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti podľa bodu 3.7 tejto zmluvy.

3.5. Audítor kybernetickej bezpečnosti sa v rámci auditu kybernetickej bezpečnosti zaväzuje poskytnúť nasledovné služby:

a) v súlade so Štandardom na výkon auditu kybernetickej bezpečnosti vydanom Kompetenčným centrom kybernetickej bezpečnosti (ďalej len „**Metodika auditu**", uvedenom na URL: https://www.nbu.gov.sk/wp-content/uploads/2022/05/Metodika-auditu-kybernetickej-bezpecnosti.pdf) a v súlade s požiadavkami Zákona a Vyhlášky o bezpečnostných opatreniach výkon auditu kybernetickej bezpečnosti, a teda auditu sietí a informačných systémov klienta ako prevádzkovateľa základnej služby, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek Zákona a Vyhlášky o bezpečnostných opatreniach, ktoré definujú príslušné požiadavky na prevádzkovateľa základnej služby. Audit kybernetickej bezpečnosti zahŕňa tieto požiadavky:

I. Posúdenie prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine v oblastiach:
   a. Organizácia informačnej bezpečnosti,
   b. Riadenie aktív, hrozieb a rizík,
   c. Personálna bezpečnosť,
   d. Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
   e. Technických zraniteľností systémov a zariadení,
   f. Riadenie bezpečnosti sietí a informačných systémov,
   g. Riadenie prevádzky,
   h. Riadenie prístupov,
   i. Kryptografických opatrení,
   j. Riešenia kybernetických bezpečnostných incidentov,
   k. Monitorovania, testovania bezpečnosti a bezpečnostných auditov,
   l. Fyzickej bezpečnosti a bezpečnosti prostredia,
   m. Riadenia kontinuity procesov.

3.6. Klient je povinný poskytnúť dodávateľovi všetky informácie a súčinnosť potrebnú pre splnenie predmetu tejto zmluvy.

3.7. Výstupom auditu kybernetickej bezpečnosti je Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti v slovenskom jazyku (ďalej aj ako „**správa**") vypracovaná v súlade s požiadavkami Vyhlášky o audite. V prípade požiadavky klienta na vyhotovenie správy aj v anglickom jazyku sa uvedená požiadavka považuje za požiadavku o dodatočnú službu spoplatnenú podľa bodu 3.11 tejto zmluvy.

Správa bude mať nasledovnú štruktúru, pokiaľ z Vyhlášky o audite nevyplýva iná štruktúra a rozsah:
(a) Meno, priezvisko a číslo platného certifikátu audítora, dátum vyhotovenia a podpis audítora,
(b) Vymedzenie rozsahu vykonaného auditu kybernetickej bezpečnosti,
(c) Cieľ auditu kybernetickej bezpečnosti,
(d) Použité postupy a metodiky vykonaného auditu kybernetickej bezpečnosti,
(e) Zhrnutie zistení výsledkov auditu kybernetickej bezpečnosti a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,
(f) Odporúčané nápravné opatrenia audítora pri zistení nedostatkov,
(g) Dokumenty, ktorými sú najmä
   1. Kópiu certifikátu audítora,
   2. Kópiu žiadosti o výkon auditu podľa prílohy č. 1 Vyhlášky o audite,
   3. Výpočet rozsahu trvania auditu a zdôvodnenie skrátenia alebo predĺženia,
   4. Kontrolný záznam auditovaných bezpečnostných opatrení s vyjadrením prevádzkovateľa základnej služby so zisteniami auditu,
   5. Harmonogram auditu,
   6. Zoznam posúdenej dokumentácie,
   7. Uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,

8. Zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sieti a informačných systémov, a konkrétne uvedenie nedostatkov.

Správa bude podľa požiadavky klienta buď predložená v jednom elektronickom vyhotovení štatutárnemu orgánu klienta zabezpečeným kanálom a podpísaná kvalifikovaným elektronickým podpisom audítora kybernetickej bezpečnosti **ALEBO** správa bude predložená v tlačenom vyhotovení v dvoch vyhotoveniach štatutárnemu orgánu klienta spôsobom podľa bodu 6.3 tejto zmluvy.

Správa bude pripravená výlučne pre informovanie štatutárneho orgánu klienta a relevantných zainteresovaných strán klienta na účel špecifikovaný vyššie. Štatutárny orgán klienta je oprávnený správu v podobe predloženej audítorom kybernetickej bezpečnosti predložiť Národnému bezpečnostnému úradu (ďalej len „**NBÚ**"), v súlade s účelom popísaným vyššie v tejto zmluve a ďalej sprístupniť nasledujúcemu audítorovi kybernetickej bezpečnosti vykonávajúcemu audit kybernetickej bezpečnosti u klienta pre informačné účely. Správa ani žiadna jej časť nesmie byť distribuovaná žiadnej tretej strane (s výnimkou výslovného predchádzajúceho písomného súhlasu dodávateľa udeleného vopred), ani použitá klientom na žiaden iný účel. Žiadna tretia strana nie je oprávnená použiť správu alebo akékoľvek informácie v nich uvedené ani sa na ne spoliehať, pokiaľ osobitný právny predpis nestanovuje inak.

3.8. Audit kybernetickej bezpečnosti vykonáva Audítor kybernetickej bezpečnosti k stavu ku dňu výkonu auditu kybernetickej bezpečnosti, pričom Audítor kybernetickej bezpečnosti nie je povinný monitorovať a zohľadňovať siete a informačné systémy klienta ani udalosti, ktoré nastali po dátume vydania správy a ani nie je povinný správu aktualizovať.

3.9. Žiadne informácie, ktoré Audítor kybernetickej bezpečnosti predloží klientovi mimo správy, nepredstavujú jeho konečné názory ani závery. Konečné názory alebo závery sa uvedú výlučne v správe.

3.10. Pre vylúčenie akýchkoľvek pochybností platí, že akýkoľvek nesúhlas klienta so závermi Audítora kybernetickej bezpečnosti uvedenými v správe sa nepovažuje za porušenie povinností dodávateľa ani audítora kybernetickej bezpečnosti vyplývajúcich zo zmluvy a nezakladá právo klienta na odstúpenie od zmluvy alebo iné s porušením povinnosti podľa tejto zmluvy inak súvisiace nároky.

3.11. Dodávateľ poskytne dodatočné služby podľa požiadaviek klienta, na ktorých sa obe zmluvné strany dohodnú vo forme dodatku k tejto zmluve alebo na základe dodávateľom potvrdenej objednávky klienta. Základom pre stanovenie platby za dodatočné služby je cenník uvedený v čl.5.6 tejto zmluvy. Dodatočné služby sa považujú za poskytnuté riadne a včas najneskôr dňom podľa bodu 3.4 zmluvy.

Článok č. 4. Miesto plnenia a harmonogram poskytovania služieb

4.1. Zmluvné strany sa dohodli, že preferovanou formou poskytovania služieb je vzdialené poskytovanie služieb On-Line, pokiaľ si charakter služby alebo okolnosti nevyžadujú poskytnutie služby na mieste - On-Site, a to v priestoroch klienta, resp. dodávateľa.

4.2. Predpokladaný harmonogram poskytovania služieb je nasledovný:

Fáza auditu	***Termín***
Nastavenie auditného programu	**7 dní od účinnosti zmluvy**
Výkon auditu kybernetickej bezpečnosti	**60 dní od nastavenia auditného programu**
Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti (Správa)	**15 dní od ukončenia výkonu auditu**

Tieto predbežné termíny sa môžu v odôvodnených prípadoch a v nevyhnutnom rozsahu zmeniť vzhľadom na personálne potreby klienta a Audítora kybernetickej bezpečnosti a vzhľadom na iné okolnosti, ktoré sa môžu pri poskytovaní služby podľa tejto zmluvy vyskytnúť. Príslušná lehota vyššie sa v prípade „Nastavenie auditného programu" začína počítať odo dňa účinnosti zmluvy a ostatné lehoty ukončením predchádzajúcej fázy auditu, ak nie je lehota daná konkrétnym dátumom.

Výsledkom akéhokoľvek oneskorenia zo strany klienta pri poskytnutí uvedených informácií, dokumentácie a všetkých údajov potrebných pre poskytnutie služieb podľa tejto zmluvy alebo akejkoľvek inej súčinnosti, ktorú je klient podľa tejto zmluvy povinný poskytnúť, bude oneskorenie uvedeného harmonogramu poskytovania Služieb zo strany Audítora kybernetickej bezpečnosti. Akékoľvek dodatočné informácie a/alebo úpravy vykonané klientom po tom, čo boli nevyhnutné informácie a dokumentácia predložená audítorovi kybernetickej bezpečnosti, môžu mať za následok oneskorenie a/alebo dodatočné poplatky podľa 3.11. Audítor kybernetickej bezpečnosti sa zaväzuje informovať klienta o akýchkoľvek skutočnostiach vedúcich k oneskoreniu v dodržaní termínov alebo o iných okolnostiach, ktoré by mohli mať nepriaznivý vplyv na poskytovanie služieb podľa tejto zmluvy bezodkladne po tom, čo sa o nich audítor kybernetickej bezpečnosti dozvie. V takomto prípade audítor informačných systémov oznámi klientovi primerane upravený harmonogram poskytovania služieb, pričom takto oznámený upravený harmonogram (aj opakovane) sa považuje za platný harmonogram auditu kybernetickej bezpečnosti.

4.3. Audítor kybernetickej bezpečnosti predloží návrh správy klientovi na vyjadrenie pred vydaním finálnej verzie správy. Klient je oprávnený predložiť svoje pripomienky k návrhu správy najneskôr do 7 pracovných dní od predloženia príslušného návrhu správy audítora. Audítor kybernetickej bezpečnosti následne, najneskôr do 7 dní od ukončenia výkonu auditu a po získaní pripomienok od klienta, vydá finálnu verziu správy. V prípade, že sa klient nevyjadrí vo vyššie stanovenej lehote, považuje sa návrh správy za akceptovaný zo strany klienta a Audítor kybernetickej bezpečnosti vydá finálnu verziu správy.

4.4. Klient zabezpečí pravdivé, správne a úplné informácie a dokumenty potrebné na riadne a včasné splnenie predmetu zmluvy. Klient vyhlasuje, že pred dodávateľom alebo Audítorom kybernetickej bezpečnosti nebudú zamlčané žiadne informácie, ktoré dodávateľ alebo Audítor kybernetickej bezpečnosti potrebuje na účely plnenia predmetu zmluvy, bez ohľadu na to, či dodávateľ alebo audítor kybernetickej bezpečnosti takého informácie špecificky požadoval.

4.5. Klient je povinný určiť aspoň jedného pracovníka (ďalej „**poverený pracovník**"), ktorý bude zodpovedný za plnenie administratívnych a iných požiadaviek na účely realizácie predmetu tejto zmluvy. Klient oznámi meno a kontaktné údaje (email, mobilné telefónne číslo) určeného pracovníka Audítorovi kybernetickej bezpečnosti pred začatím poskytovania služieb.

4.6. Audítor kybernetickej bezpečnosti predloží poverenému pracovníkovi detailnú požiadavku na informácie a dokumentáciu aspoň v rozsahu definovanom vo Vyhláške o audite. Tieto informácie a dokumentáciu klient doručí Audítorovi kybernetickej bezpečnosti najneskôr 5 dní pred začatím poskytovania služieb, ak Audítor kybernetickej bezpečnosti neurčil neskoršiu lehotu. Audítor kybernetickej bezpečnosti nezačne poskytovať služby, kým od klienta neobdrží požadované úplné informácie a dokumentáciu. Ak informácie predložené Audítorovi kybernetickej bezpečnosti zo strany klienta nie sú doručené včas alebo nebudú dostatočné alebo primerané, za podmienok uvedených v zmluve si Audítor kybernetickej bezpečnosti vyhradzuje právo zmeniť harmonogram poskytovania služieb primerane podľa dostupnosti požadovaných informácií a jeho možností alebo odporučiť odklad výkonu auditu. V prípade, ak v dôsledku nedostatku súčinnosti na strane klienta bude dodávateľ alebo audítor kybernetickej bezpečnosti povinný požadovať doplnenie informácií alebo dokumentov alebo si tieto budú vyžadovať akúkoľvek úpravu, dodávateľ je oprávnený účtovať klientovi práce naviac v súlade s bodom 3.11.

Článok č. 5. Odmena a platobné podmienky

5.1. Cena za služby uvedené v bode 3.1 vyššie bola dohodou zmluvných strán stanovená na **4 200 EUR** (slovom: Štyritisícdvesto eur) (ďalej len „**cena**"). Dodávateľ nie je platca DPH.

5.2. Cena sa bude fakturovať po ukončení poskytovania služby, ktorou sa rozumie predloženie finálnej Správy klientovi spôsobom podľa bodu 3.7 zmluvy. Faktúra bude vystavená do 5 dní odo dňa predloženia finálnej správy klientovi. Faktúra je splatná do 30 dní po dni jej doručenia klientovi.

5.3. Ceny boli stanovené dohodou zmluvných strán na základe platnej slovenskej legislatívy a na základe predpokladu poskytnutia úplných a pravdivých informácií a riadnej súčinnosti zo strany klienta. Klient berie na vedomie a súhlasí, že akákoľvek zmena týchto atribútov, parametrov alebo nedostatok súčinnosti na strane klienta môže mať za následok zmenu ceny, na čo dodávateľ vopred klienta upozorní, spolu s vyčíslením zmeny ceny a jej odôvodnením.

5.4. Zmluvné strany sa dohodli, že faktúry budú vyhotovené v elektronickej podobe (tzv. elektronická faktúra) vo formáte PDF/A a Klientovi budú doručované emailom na emailovú adresu uvedenú v záhlaví tejto zmluvy alebo v bode 6.1 tejto zmluvy, pričom faktúry sa považujú za doručené

Klientovi dňom ich doručenia. Dodávateľ zodpovedá za správnosť a úplnosť faktúry, ktorá musí obsahovať náležitosti daňového dokladu v zmysle právnych platných prepisov.

5.5. Všetky peňažné plnenia podľa zmluvy sú splatné v EUR na bankový účet dodávateľa uvedený na faktúre.

5.6. Dodávateľ si vyhradzuje právo fakturovať dodatočné poplatky z titulu práce navyše, ako aj z titulu nedostatku na strane klienta, najmä nedostatku v podobe neposkytnutia riadnej a včasnej súčinnosti, nepredloženia informácií potrebných pre poskytnutie služieb podľa tejto zmluvy, poskytnutia neúplných alebo nesprávnych informácií, ktoré boli poskytnuté audítorovi kybernetickej bezpečnosti alebo v dôsledku zmien, ktoré klient vykonal po začiatku Auditu kybernetickej bezpečnosti; na takúto úpravu ceny dodávateľ vopred klienta upozorní, spolu s vyčíslením zmeny ceny a jej odôvodnením. Tieto činnosti dodávateľa sa považujú za dodatočné služby v rámci tejto zmluvy. Pokiaľ nie je dohodnuté inak, výška takýchto poplatkov bude určená na základe dodatočného času, ktorý audítor kybernetickej bezpečnosti vynaloží z dôvodov podľa tohto bodu zmluvy a štandardných hodinových sadzieb bez DPH, ktoré sú uvedené v nasledujúcej tabuľke (tzv. osobodní, resp. *manday,* pričom jeden osobodeň predstavuje 8 pracovných hodín):

Audítor kybernetickej bezpečnosti	[540]
Asistent audítora	[540]
IT bezpečnostný špecialista	[540]

5.7. V prípade omeškania klienta s úhradou akéhokoľvek peňažného plnenia alebo jeho časti podľa tejto zmluvy je dodávateľ oprávnený uplatniť si voči klientovi úroky z omeškania vo výške 0,5 % z dlžnej sumy za každý aj začatý deň omeškania. Klient sa zaväzuje úrok z omeškania podľa predchádzajúcej vety dodávateľovi uhradiť na základe faktúry dodávateľa.

5.8. Klient si vyhradzuje, že veriteľ nemôže postúpiť pohľadávky voči dlžníkovi tretej osobe, podľa §524 a nasl. zák. č.40/1964Zb. Občianskeho zákonníka v znení neskorších predpisov, bez predchádzajúceho písomného súhlasu dlžníka. Právny úkon, ktorým veriteľ postúpi pohľadávky voči dlžníkovi tretej osobe bez predchádzajúceho súhlasu dlžníka, je podľa §39 Občianskeho zákonníka neplatný. Písomný súhlas dlžníka je oprávnený vydať len jeho štatutárny orgán. Veriteľ berie na vedomie, že súhlas dlžníka, ktorý je zdravotníckym zariadením je platný len za podmienky, že bol na takýto úkon udelený predchádzajúci písomný súhlas MZ SR.

Článok č. 6. Komunikácia

6.1. Adresy, telefónne čísla a e-mailové adresy zmluvných strán na účely ich oznámení týkajúcich sa tejto zmluvy sú:

Za dodávateľa:
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Do pozornosti: Alexandra Húsková, Obchodné oddelenie
adresa uvedená v úvode zmluvy
Tel: +421 903761801
E-mail: alexandra.huskova@cybercompetence.sk

Klient:
Národný ústav detskej tuberkulózy a respiračných chorôb, n. o. Dolný Smokovec
Do pozornosti: Ing. Daniel Slezák, Oddelenie informačných technológií
adresa uvedená v úvode zmluvy
Tel: +421 524412150, +421 911 614 081
E-mail: daniel.slezak@nudtarch.sk

6.2. O zmene kontaktných údajov alebo kontaktných osôb je dotknutá zmluvná strana povinná druhú zmluvnú stranu informovať bez zbytočného odkladu.

6.3. S výnimkou otázok týkajúcich sa zániku tejto zmluvy, nárokov na náhradu škody alebo iné peňažné plnenie podľa tejto zmluvy, ktorú musia byť uplatnené písomne, sú zmluvné strany oprávnené komunikovať aj formou emailu a táto emailová komunikácia bude považovaná za riadne oznámenie podľa tejto zmluvy. Písomnosť sa považuje za doručenú za nasledovných podmienok:

(a) v prípade osobného doručovania odovzdaním písomnosti oprávnenej osobe alebo inej osobe oprávnenej prijímať písomnosti za túto zmluvnú stranu a podpisom takej osoby na doručenke a/alebo kópii doručovanej písomnosti, alebo odmietnutím prevzatia písomnosti takou osobou,

(b) v prípade poštového doručovania doručením na adresu zmluvnej strany a v prípade doporučenej zásielky odovzdaním písomnosti osobe oprávnenej prijímať písomnosti za túto zmluvnú stranu a podpisom takej osoby na doručenke, najneskôr však uplynutím siedmych dní odo dňa uvedeného na podacom lístku, a to bez ohľadu na úspešnosť doručenia,

(c) v prípade doručovania prostredníctvom elektronickej pošty dňom nasledujúcim po odoslaní elektronickej pošty, ak prijímajúca zmluvná strana nepotvrdí prijatie elektronickej správy skôr, a to i v prípade, ak sa druhá zmluvná strana o doručení elektronickej pošty nedozvedela alebo ak sa z dôvodov na prijímajúcej zmluvnej strane s obsahom neoboznámila,

6.4. Klient si je vedomý, že v prípade emailovej komunikácie nemožno zaručiť úplnú bezpečnosť a bezchybnosť a že takéto informácie môžu byť zachytené, poškodené, môžu sa stratiť, zničiť, môžu byť doručené neskoro alebo neúplné, alebo môžu byť inak negatívne ovplyvnené.

Článok č. 7. Obmedzenie zodpovednosti

7.1. Dodávateľ zodpovedá len za skutočnú škodu spôsobenú porušením tejto zmluvy, najviac však do výšky ceny.

7.2. Dodávateľ v súvislosti s plnením predmetu zmluvy nezodpovedá za žiadne nároky tretích strán voči klientovi. Zodpovedá však za prípadné nároky subdodávateľa, ktorého použil na splnenie predmetu tejto zmluvy podľa bodu 3.3 tejto zmluvy v prípade, že tieto ostanú aj napriek splneniu si všetkých povinností PZS podľa tejto zmluvy z dôvodov na strane dodávateľa neuspokojené.

7.3. Klient má zmluvný vzťah výlučne s dodávateľom. Klient nebude mať žiadne nároky voči iným osobám použitým pri plnení tejto zmluvy s výnimkou dodávateľa.

Článok č. 8. Autorské práva a duševné vlastníctvo

8.1. Dodávateľ je nositeľom všetkých práv duševného vlastníctva na všetko, čo vytvoril audítor kybernetickej bezpečnosti pred alebo počas poskytovania služieb, vrátane správ, písomného poradenstva, listov, odporúčaní alebo iných výstupov poskytovania služieb klientovi (ďalej ako „**výstupy**"). Výstupy zostávajú vo vlastníctve dodávateľa. Momentom úhrady ceny a ďalších zmluvou predpokladaných peňažných plnení udeľuje dodávateľ klientovi nevýhradnú licenciu na použitie týchto Výstupov na dosiahnutie účelu tejto zmluvy a v súlade s ostatnými ustanoveniami zmluvy. Licencia sa udeľuje na obdobie trvania majetkových práv k výstupom. Spôsoby používania výstupov ako aj vecný a územný rozsah licencie sú obmedzené účelom, na ktorý boli výstupy vypracované.

8.2. Dodávateľ sa zaväzuje neposkytnúť alebo nesprístupniť výstupy vrátane záverečnej správy tretím stranám, s výnimkou prípadov, ak tak ustanovuje všeobecne záväzný právny predpis alebo to je vyžadované orgánom verejnej moci pri výkone svojej pôsobnosti, súdom alebo iným oprávneným subjektom.

Článok č. 9. Mlčanlivosť

9.1. Audítor kybernetickej bezpečnosti je povinný vo vzťahu ku všetkým mu poskytnutým informáciám a údajom zachovávať mlčanlivosť podľa § 12 Zákona.

Článok č. 10. Ochrana osobných údajov

10.1. V súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „Nariadenie") a zákonom č. 18/2018 Z. z. o ochrane osobných údajov, v znení neskorších predpisov (ďalej len „Zákon OOÚ") klient a dodávateľ sú v postavení samostatných prevádzkovateľov.

10.2. Klient aj dodávateľ sú povinní dôsledne chrániť všetky spracúvané osobné údaje, s ktorými prídu do styku pri plnení predmetu tejto zmluvy. Klient aj dodávateľ sú povinní prijať primerané technické a organizačné opatrenia tak, aby spracúvanie osobných údajov spĺňalo požiadavky Nariadenia resp. Zákona OOÚ a aby bola zabezpečená ochrana práv dotknutých osôb podľa Nariadenia a Zákona OOÚ. Zároveň sú povinní plniť ďalšie povinnosti uložené príslušnými právnymi predpismi v oblasti ochrany osobných údajov a ochrany informácií.

10.3. Klient potvrdzuje, že všetky osobné údaje poskytnuté dodávateľovi boli získané zákonným spôsobom, pri zachovaní všetkých základných zásad spracúvania osobných údajov.

Článok č. 11. Trvanie a ukončenie zmluvy

11.1. Platnosť zmluvy sa skončí podľa toho, ktorý prípad nastane skôr:
(a) riadnym splnením predmetu zmluvy; alebo
(b) zmluvné strany uzatvoria písomnú dohodu o ukončení platnosti zmluvy; alebo

(c) odstúpením od zmluvy po tom, ako jedna zmluvná strana prevezme písomné oznámenie druhej zmluvnej strany o odstúpení od zmluvy, v ktorom sa uvádza, že druhá zmluvná strana porušila povinnosti jej vyplývajúce zo zmluvy (ďalej len „porušujúca zmluvná strana") za predpokladu, že porušujúca zmluvná strana bola na porušovanie povinností vopred písomne upozornená a napriek tomu nevykonala nápravu v primeranej lehote (ktorá nesmie byť kratšia ako 15 dní) od doručenia písomného upozornenia.

11.2. Dodávateľ je oprávnený od zmluvy odstúpiť na základe písomného oznámenia doručeného klientovi, ak zistí, že sa objavila závažná prekážka vo výkone auditu pred dňom alebo počas výkonu Auditu kybernetickej bezpečnosti (okrem iného vrátane zmeny v príslušnej legislatíve alebo v dôsledku rozhodnutia štátneho orgánu alebo inej príslušnej profesijnej organizácie alebo zmeny vo vlastníckej štruktúre klienta alebo jeho pridružených osôb, alebo náležitostiach žiadosti o Audit kybernetickej bezpečnosti), na základe ktorých by plnenie ktorejkoľvek časti zmluvy zo strany dodávateľa bolo zmenené, sťažené, protiprávne alebo inak nezákonné alebo v rozpore s pravidlami nezávislosti alebo pravidlami profesijnej etiky.

11.3. Ukončenie zmluvy nemá vplyv na povinnosť klienta uhradiť dodávateľovi cenu za služby, ktoré podľa zmluvy poskytol do dňa účinnosti ukončenia platnosti zmluvy. Zmluvné strany sa dohodli, že cena podľa prechádzajúcej vety sa vypočíta ako súčin hodinových sadzieb podľa bodu 5.6 zmluvy a počtu dní, ktoré dodávateľ vynaložil na poskytovanie služieb do ukončenia zmluvy. V prípade ukončenia zmluvy z dôvodov na strane klienta vzniká dodávateľovi popri cene podľa tohto bodu zmluvy nárok na zmluvnú pokutu vo výške 10% z ceny.

Článok č. 12. Záverečné ustanovenia

12.1. Objednávateľ je povinnou osobou v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám, v znení neskorších predpisov. Zmluva zároveň spĺňa podmienku jej zverejnenia podľa tohto zákona. Na základe uvedeného sa prevádzkovateľ zaväzuje túto zmluvu po podpise zmluvnými stranami bezodkladne zverejniť zákonným spôsobom. Zmluva nadobúda platnosť dňom jej podpisu obidvoma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia. Zmluvné strany berú na vedomie, že porušením alebo ohrozením obchodného tajomstva podľa tejto zmluvy nie je jej zverejnenie.

12.2. Zmluvné strany vyhlasujú, že získali všetky potrebné povolenia a oprávnenia na uzavretie tejto zmluvy a na jej plnenie.

12.3. Táto zmluva sa vyhotovuje v dvoch vyhotoveniach v slovenskom jazyku. Každá zmluvná strana dostane po jednom vyhotovení v slovenskom jazyku.

12.4. Akékoľvek zmeny a/alebo doplnenia zmluvy sa môžu vykonať iba na základe dohody obidvoch zmluvných strán, a to vo forme písomných a očíslovaných dodatkov k zmluve podpísaných oprávnenými zástupcami oboch zmluvných strán.

12.5. Klient súhlasí s tým, aby bol uvedený v referenčných listinách dodávateľa v súvislosti s poskytovaním služieb podľa zmluvy.

12.6. V prípade, že akékoľvek ustanovenie zmluvy je alebo sa stane neplatným, neúčinným alebo vykonateľným, nie je tým dotknutá platnosť, účinnosť, alebo vykonateľnosť ostatných ustanovení zmluvy, pokiaľ to nevylučuje v zmysle všeobecne záväzných právnych predpisov samotná povaha takého ustanovenia. Zmluvné strany sa zaväzujú bez zbytočného odkladu po tom, ako zistia, že niektoré z ustanovení zmluvy je neplatné, neúčinné alebo nevykonateľné, nahradiť dotknuté ustanovenie ustanovením novým, ktorého obsah bude v čo najväčšej miere zodpovedať vôli zmluvných strán v čase uzatvorenia zmluvy.

12.7. Zmluvné strany vyhlasujú, že túto zmluvu uzatvorili slobodne, vážne a bez omylu, nebola uzatvorená v tiesni ani za nápadne nevýhodných podmienok, že si zmluvu prečítali a jej obsahu porozumeli, a na znak súhlasu s jej obsahom ju podpisujú.

12.8. Zoznam príloh – neoddeliteľnou súčasťou tejto zmluvy sú:

a) Príloha č. 1 – Kópia dotazníka k výkonu auditu.

V Bratislave dňa 24. 4. 2023

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Ing. Ivan Makatura
Generálny riaditeľ

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
IČO: 52839052 DIČ: 2121156345
www.cybercompetence.sk

V DS dňa 26.4.2023

Národný ústav detskej tuberkulózy a respiračných chorôb, n. o. Dolný Smokovec
Ing. Miroslava Mištunová, PhD., MPH
Riaditeľka

Národný ústav detskej tuberkulózy a respiračných chorôb, n.o.
059 81 DOLNÝ SMOKOVEC - VYSOKÉ TATRY

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Dotazník za účelom odhadu rozsahu prác

Spoločnosť	Národný ústav detskej tuberkulózy a respiračných chorôb n. o., Dolný Smokovec
Zodpovedný zamestnanec (meno, email, tel. číslo)	Ing. Daniel Slezák, daniel.slezak@nudtarch.sk, 052/4412150

Č.	Otázka	Odpoveď
1	Ste prevádzkovateľom prvku kritickej infraštruktúry[1]?	áno
2	Ste prevádzkovateľom základnej služby („PZS")?	áno
2.1	Ak áno, aké základné služby prevádzkujete?	laboratórium
3	Počet užívateľov Siete a Informačného Systému[2]s väzbou na základné služby? (ďalej len IS) *Príklad:* *1500 interných* *3000 externých*	136 interných
4	Počet IS pre jednotlivé základné služby?	1
5	Počet zamestnancov zúčastňujúcich na prevádzke IS s väzbou na základnú službu?	14
6	Štruktúra správy IS s väzbou na základnú službu *Centralizovaná verzus distribuovaná*	centralizovaná
7	Počet externých pracovísk, kde je prevádzkovaný samostatný IS s väzbou na základnú službu, iný ako na ostatných pracoviskách?	0
8	Máte s tretími stranami uzavreté akékoľvek zmluvy na výkon činností, ktoré priamo súvisia s prevádzkou IS s väzbou na základné služby (*ak áno, počet a typ služieb*)? *Príklad:* *1 x dodávateľ podpory užívateľských staníc* *1 x dodávateľ IS zariadení* *1 x dodávateľ laboratórnych zariadení*	1 x podpora uživ. staníc 1 x dodávateľ IS
9	Počet zamestnancov tretích strán zúčastňujúcich na prevádzke IS s väzbou na základnú službu?	0
10	Máte vypracovanú bezpečnostnú dokumentáciu týkajúcu sa Vašich IS (*ak áno, akú a z ktorého roku*)?	áno
11	Máte určenú rolu manažéra kybernetickej bezpečnosti? (*CISO*)	Andrej Mišura
12	Máte zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení?	áno
13	Máte schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti?	áno
14	Máte zadefinovanú klasifikáciu informácií?	ámo
15	Vykonali ste kategorizáciu IS podľa požiadaviek Zákona?	áno
15.1	Ak áno, sú IS zaradené do:	
15.2	I. kategórie	-
15.3	II. kategórie	NIS, VEMA, UAFALAN
15.4	III. kategórie	-

1 § 2 písm. a) zákona č. 45/2011 Z.z. o kritickej infraštruktúre
2§ 3 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

16	Máte záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti podľa § 29 zákona.	Áno
17	Máte vypracované postupy a procesy pre riadenie aktív, hrozieb a rizík?	Áno
18	Máte identifikované a evidované aktíva využívané pre základnú službu?	Áno
19	Máte vypracované a zavedené riadenie personálnej bezpečnosti?	Áno
20	Máte vypracované a zavedené riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov?	Čiastočne
21	Máte zavedený systém a procesy na identifikáciu technických zraniteľností v IS s väzbou na základnú službu?	Áno
22	Máte zavedené prvky riadenia bezpečnosti sietí a informačných systémov?	Áno
23	Máte zavedené praktiky riadenia prevádzky?	Áno
24	Máte zavedené riadenie prístupov osôb alebo systémov do IS s väzbou na základnú službu?	Áno
25	Máte vypracované a zavedené kryptografické opatrenia?	Čiastočne
26	Máte vypracovaný a zavedený postup riešenia kybernetických incidentov?	Áno
27	Vyskytol sa závažný kybernetický bezpečnostný incident za posledné 2 roky?	Nie
28	Porušili ste povinnosti ZoKB, prípadne bola udelená pokuta? *(ak áno, aké)*	Nie
29	Máte zavedený centralizovaný bezpečnostný dohľad nad IS s väzbou na základnú službu?	Nie
30	Máte zavedenú fyzickú bezpečnosť a bezpečnosť prostredia v súvislosti s IS s väzbou na základnú službu?	Áno
31	Máte vypracované a zavedene pravidlá a postupy riadenia kontinuity procesov v súvislosti s IS s väzbou na základnú službu?	Áno
32	Máte vypracované a pravidelné testované krízové plány v súvislosti s IS s väzbou na základnú službu?	Nie
33	Máte vypracované, zavedené a pravidelne testované postupy zálohovania a obnovy siete a informačného systému?	Áno
34	Ste držiteľom certifikátu podľa technickej normy (napr. ISO 27001) a certifikovaná oblasť zahŕňa IS s väzbou na základnú službu? *(uveďte aj podľa akej normy)*	nemáme
35	Máte potvrdenie o priemyselnej bezpečnosti? *(ak áno, uveďte číslo)*	Nemáme
36	Ďalšie informácie	