Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
uzatvorená v zmysle § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len ako „**zmluva**“)
medzi týmito zmluvnými stranami:

názov	**Fakultná nemocnica s poliklinikou Žilina**
Sídlo:	Ul. Vojtecha Spanyola 43, 012 07 Žilina
IČO:	17335825
IČ DPH:	SK2020699923
DIČ:	2020699923
údaj o konajúcej osobe:	Mgr. Eduard Dorčík - riaditeľ
Zriadený:	zriaďovacou listinou Ministerstva zdravotníctva SR č. 3724/1991- A/XIV-1 zo dňa 09.12.1991 v znení jej zmien

(ďalej len „**Prevádzkovateľ**“)

a

obchodné meno:	**STAPRO SLOVENSKO s.r.o.**
sídlo:	Hroncova 3, 040 01 Košice
IČO:	31710459
DIČ:	2020483982
IČ DPH:	SK2020483982
údaj o zápise v OR	Spoločnosť je zapísaná v obchodnom registri MS Košice oddiel Sro, vložka číslo 6435/V
údaj o konajúcej osobe:	Ing. Adrián Petrik, riaditeľ a konateľ

(ďalej len „**Dodávateľ**“)

PREAMBULA

Prevádzkovateľ je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**zákon o kybernetickej bezpečnosti**“).

Základnou službou prevádzkovateľa je poskytovanie zdravotnej starostlivosti, ktorá je v zmysle ustanovenia § 3 písm. l) prvého bodu zákona o kybernetickej bezpečnosti činnosťou v sektore „Zdravotníctvo“, podsektore „Zdravotnícke zariadenia“ závisiace od sietí a informačných systémov a podľa ustanovenia § 17 ods. 2 písm. b) zákona o kybernetickej bezpečnosti sú zaradené do zoznamu základných služieb.

Dodávateľ je zmluvným partnerom Prevádzkovateľa na dodanie diela s názvom „***Rozšírenie NIS FONS Enterprise, oblasť Logistika, Modul Burza tovarov“*** na základe uzatvorenej Zmluvy o dielo č. 017/1/2023/044 zo dňa 8.8.2023, účinná dňa ..18.08.2023... (ďalej len „**základný kontrakt**“).

Dodávateľ vyhlasuje, že je odborne spôsobilý na plnenie predmetu tejto zmluvy. Ak nie je uvedené inak, pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

Článok I.
Predmet zmluvy

1. Predmetom tejto zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti elektronických sietí a informačných systémov Prevádzkovateľa.
2. Táto zmluva upravuje základné princípy spolupráce zmluvných strán pri uskutočňovaní plnenia bezpečnostných opatrení – úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa počas ich životného cyklu, s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby Prevádzkovateľa (ďalej len „**ciele**“).
3. Súčasťou záväzkov Dodávateľa podľa tejto zmluvy je povinnosť Dodávateľa prijímať a dodržiavať bezpečnostné opatrenia v celej IT infraštruktúre a to aj pri vývoji v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Prevádzkovateľ vyhlasuje, že súhlasí so špecifikáciou a rozsahom bezpečnostných opatrení prijímaných Dodávateľom v zmysle tejto zmluvy. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
4. Dodávateľ sa na základe tejto zmluvy zároveň zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa obsiahnuté v ním vydaných smerniciach, a to najmä Prílohu č. 7 Bezpečnostné klauzuly pre dodávateľov a partnerov SM-42 (smernice) Príručka kybernetickej bezpečnosti (ďalej aj ako „SM 42“), ktorej obsah zároveň tvorí aj Prílohu č. 2 tejto zmluvy, ako Bezpečnostné klauzuly pre dodávateľov a partnerov. Prevádzkovateľ sa touto zmluvou zaväzuje, že nie je povinný Dodávateľovi sprístupniť kompletnú SM 42 okrem jej vyššie spomenutej prílohy č. 7 a Dodávateľ predmetné nesprístupnenie SM 42 Prevádzkovateľom akceptuje v plnom rozsahu.
5. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa. Dodávateľ súčasne akceptuje, že bezpečnostné politiky Prevádzkovateľa, ako aj ním prijaté smernice s prílohami v tejto oblasti sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa. Prevádzkovateľ je povinný v prípade aktualizácie a zmien jeho bezpečnostnej politiky, prijaté smernice vrátene ich príloh bezodkladne oboznámiť Dodávateľa formou mailu s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ potvrdí akceptáciu zmien bezpečnostnej politiky.
6. Na základe tejto zmluvy sa tiež Dodávateľ zaväzuje plniť notifikačné povinnosti v celej IT infraštruktúre a to aj pri vývoji v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené jej ciele.
7. Notifikačnými povinnosťami na úseku kybernetickej bezpečnosti v rozsahu tejto zmluvy sú:
   a) povinnosť informovať prevádzkovateľa na poskytovanie elektronických komunikačných služieb alebo sietí, ku ktorému je sieť alebo informačný systém základnej služby pripojená, o zaradení do registra prevádzkovateľov základných služieb,
   b) povinnosť informovať tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente v prípade, ak plnenie zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností bolo nemožné,

c) povinnosť bezodkladne ohlásiť závažný kybernetický bezpečnostný incident,
d) povinnosť oznámiť orgánom činným v trestnom konaní skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin, o ktorom sa dozvedel hodnoverným spôsobom,
e) povinnosť hlásiť zmeny v údajoch, a to do 30 dní odo dňa ich vzniku.

8. 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 celom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa základného kontraktu a za plnenie povinností podľa tejto zmluvy Dodávateľ nemá nárok na žiadne ďalšie peňažné plnenia od Prevádzkovateľa.
9. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania základného kontraktu.

Článok II.
Prevencia kybernetických bezpečnostných incidentov

1. Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť Prevádzkovateľa alebo ktorej následkom je:
   a) strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému Prevádzkovateľa,
   b) obmedzenie alebo odmietnutie dostupnosti základnej služby Prevádzkovateľa,
   c) vysoká pravdepodobnosť kompromitácie činností základnej služby Prevádzkovateľa alebo
   d) ohrozenie bezpečnosti informácií Prevádzkovateľa.
2. Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa (ďalej len „**incidenty**")
   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa,
   b) sledovať výstrahy, varovania, ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov, tieto vyhodnocovať a vykonať protiopatrenia v záujme ochrany oprávnených záujmov Prevádzkovateľa
   c) prijímať od Prevádzkovateľa varovania pred incidentmi,
   d) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa,
   e) vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa alebo kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa,
   f) predchádzať vzniku incidentov,
   g) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
   h) zasielať Prevádzkovateľovi včasné varovania pred incidentmi, o ktorých sa dozvie vlastnou činnosťou podľa tejto zmluvy alebo iným spôsobom,
   i) informovať Prevádzkovateľa o incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
   j) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa

k) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov podieľajúcich sa na plnení základného kontraktu a/alebo tejto zmluvy a/alebo majúcich prístup k informáciám a údajom Prevádzkovateľa.

3. Dodávateľ je povinný mať počas trvania tejto zmluvy také technické, technologické a personálne vybavenie, ktoré je potrebné na riadne a včasné plnenie tejto zmluvy, a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti v rozsahu potrebnom na efektívne napĺňanie cieľov tejto zmluvy.
4. Neoddeliteľnými prílohami tejto zmluvy sú:
   a) konkrétny rozsah činnosti Dodávateľa v zmysle základného kontraktu (Príloha č. 1), konkrétna Bezpečnostné klauzuly pre dodávateľov a partnerov, ktoré prijíma Dodávateľ a s ktorými súhlasí (Príloha č. 2),
   b) zoznam pracovných rolí Dodávateľa, ktoré majú mať prístup k informáciám a údajom Prevádzkovateľa a zoznam zamestnancov Dodávateľa a iných osôb, podieľajúcich sa za Dodávateľa na plnení základného kontraktu a/alebo tejto zmluvy a/alebo majúcich prístup k informáciám a údajom Prevádzkovateľa (Príloha č. 3)
   c) spôsob hlásenia bezpečnostných incidentov (Príloha č. 4)
5. Dodávateľ je povinný emailom bezodkladne oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí Dodávateľa.
6. Dodávateľ je povinný 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 na nahliadnutie a zhotovenie kópií
7. Dodávateľ je povinný prijať a dodržiavať všeobecné a sektorové bezpečnostné opatrenia v dotknutých oblastiach podľa zákona o kybernetickej bezpečnosti a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „**vyhláška**“), najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona o kybernetickej bezpečnosti, a v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa.

Článok III.
Reaktivita pri hlásení incidentov

1. Dodávateľ je povinný Prevádzkovateľovi bezodkladne hlásiť každý incident v príčinnej súvislosti s informačným systémom v jeho správe spôsobom určeným Prevádzkovateľom, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Spôsob hlásenia bezpečnostných incidentov je stanovený v Prílohe č. 4 tejto zmluvy, ktorá tvorí neoddeliteľnú súčasť tejto zmluvy. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, dodávateľ je povinný 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 je povinný riešiť incident 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 incidentu je Dodávateľ povinný na žiadosť Prevádzkovateľa spolupracovať s Prevádzkovateľom, 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 je povinný Prevádzkovateľovi bezodkladne oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok.
4. Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní, a poskytnúť ho Prevádzkovateľovi.
5. Dodávateľ je povinný Prevádzkovateľovi oznámiť skutočnosť, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
6. Po vyriešení incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „**ochranné opatrenia**") na schválenie. Ak dodávateľ nenavrhne ochranné opatrenia v určenej lehote alebo ak sú navrhované ochranné opatrenia zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom na jeho návrhu.
7. Po schválení ochranných opatrení Prevádzkovateľom je Dodávateľ povinný ochranné opatrenia bez zbytočného odkladu vykonať.
8. Po vykonaní ochranných opatrení Dodávateľom je Dodávateľ povinný preveriť ich účinnosť.

Článok IV.
Ochrana informácií a povinnosť zachovávať mlčanlivosť

1. Dodávateľ je povinný chrániť všetky informácie poskytnuté mu Prevádzkovateľom. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa.
2. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením tejto zmluvy a/alebo základného kontraktu 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.
3. Povinnosť zachovávať mlčanlivosť trvá aj po skončení trvania tejto zmluvy a/alebo základného kontraktu.
4. Dodávateľ je povinný zabezpečiť, aby každá osoba zúčastnená na predmete plnenia základného kontraktu a/alebo tejto zmluvy za Dodávateľa neodkladne podpísala vyhlásenie o zachovávaní mlčanlivosti o skutočnostiach, o ktorých sa dozvedela v súvislosti s plnením úloh podľa zákona o kybernetickej bezpečnosti a ktoré nie sú verejne známe. Dodávateľ je v rámci toho povinný zabezpečiť trvalé zachovávanie mlčanlivosti o všetkých takýchto skutočnostiach každou z týchto osôb, a to aj po skončení plnenia predmetu zmluvy.

Článok V.
Spôsob a forma hlásenia ďalších informácií požadovaných Prevádzkovateľom na plnenie jeho povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti a ich vymedzenie, kontaktné osoby na úseku kybernetickej bezpečnosti

1. Dodávateľ je povinný hlásiť Prevádzkovateľovi za účelom plnenia povinností Prevádzkovateľa vyplývajúcich zo zákona o kybernetickej bezpečnosti všetky ďalšie Prevádzkovateľom požadované informácie, najmä informácie potrebné pre:
   a) riešenie kybernetického bezpečnostného incidentu,
   b) hlásenie závažného kybernetického incidentu,
   c) poskytnutie súčinnosti a spolupráce s Národným bezpečnostným úradom,
   d) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,

e) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka.

2. Dodávateľ je povinný realizovať hlásenia podľa predchádzajúceho ustanovenia bodu 1. tohto článku zmluvy a komunikovať s Prevádzkovateľom pri plnení povinností podľa tejto zmluvy spôsobom a formou určeným Prevádzkovateľom, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií. Zmluvné strany berú na vedomie, že hlásenia podľa bodu 1. tohto článku zmluvy ako aj poskytovanie ďalších informácií pri plnení povinností podľa tejto zmluvy si budú realizovať telefonicky, e-mailom a/alebo písomne, pričom konkrétny spôsob a formu takého oznámenia budú voliť podľa hľadiska účelnosti a naliehavosti nahlasovaných informácií.
3. Prevádzkovateľ určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti a vyšetrovania incidentov, ktoré sú uvedené v prílohe č. 2 tejto zmluvy.
4. Zmenu kontaktných osôb na úseku kybernetickej bezpečnosti môže každá zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok VI.
Podmienky a možnosti zapojenia ďalšieho Dodávateľa

1. Dodávateľ môže za účelom plnenia svojho záväzku podľa základného kontraktu ustanoviť ďalšieho Dodávateľa (ďalej len „**Subdodávateľ**“), ktorý bude čiastočne zabezpečovať plnenie pre Prevádzkovateľa namiesto Dodávateľa, avšak za splnenia nasledovných podmienok:
   a) Dodávateľ môže ustanoviť Subdodávateľa iba na základe predchádzajúceho písomného súhlasu Prevádzkovateľa; Dodávateľ v žiadosti o udelenie súhlasu písomne oznámi Prevádzkovateľovi obchodné meno a ostatné identifikačné údaje Subdodávateľa,
   b) Dodávateľ je povinný zmluvne zaviazať Subdodávateľa k plneniu povinností podľa základného kontraktu a tejto zmluvy, a uložiť mu rovnaké povinnosti týkajúce sa plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa, ako sú ustanovené v tejto zmluve,
   c) zodpovednosť voči Prevádzkovateľovi nesie Dodávateľ, ak Subdodávateľ nesplní svoje povinnosti týkajúce základného kontraktu a tejto zmluvy; tým nie je dotknutý nárok Dodávateľa na náhradu škody voči Subdodávateľovi.

Článok VII.
Spoločné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti, a inými zákonnými úpravami, 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 je ďalej povinný plniť povinnosti podľa tejto zmluvy v súlade so sektorovými bezpečnostnými opatreniami (§ 32 ods. 2 zákona o kybernetickej bezpečnosti), ktoré vydáva Ministerstvo zdravotníctva Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.
3. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
4. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (evidovanie logov a incidentov a dokumentovanie školení svojich zamestnancov – prezenčné listiny) a na žiadosť Prevádzkovateľa mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
5. Dodávateľ je oprávnený plniť predmet zmluvy pre Prevádzkovateľa prostredníctvom svojich Subdodávateľov čiastočne v nevyhnutnom rozsahu v prípade, že toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa, pričom je povinný zabezpečiť riadne plnenie povinností na úseku kybernetickej bezpečnosti v rozsahu zákona o kybernetickej bezpečnosti. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať kontrolné činnosti a audit v súlade s ustanoveniami čl. IX. tejto zmluvy aj u takýchto Subdodávateľov, zabezpečujúcich úplne alebo čiastočne plnenie základného kontraktu pre Prevádzkovateľa namiesto Dodávateľa.
6. Ak by na účely plnenia tejto Zmluvy boli spracovávané akékoľvek osobné údaje získané od Prevádzkovateľa základnej služby, Dodávateľ tak učiní v zmysle Pravidiel spracúvania osobných údajov dostupných na webovom sídle Dodávateľa (https://www.fnspza.sk/), ktoré sú vytvorené 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 („Nariadenie GDPR“), ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov, v znení neskorších predpisov. Dodávateľ vykoná všetky primerané technické a organizačné opatrenia na ochranu proti neoprávnenému alebo protiprávnemu spracúvaniu osobných údajov a proti náhodnej strate, zničeniu alebo poškodeniu osobných údajov.

Článok VIII.
Trvanie a zánik zmluvy, sankčný mechanizmus

1. Táto zmluva sa uzatvára na dobu určitú, odo dňa jej uzatvorenia do konca trvania základného kontraktu definovaného podľa preambuly v ods. 3 tejto zmluvy.
2. Zmluvný vzťah na základe tejto zmluvy zanikne súčasne so zánikom základného kontraktu.
3. Túto zmluvu je možné ukončiť vždy dohodou zmluvných strán o skončení trvania zmluvy, a to ku dňu uvedenému v takej dohode.
4. Prevádzkovateľ je oprávnený od tejto zmluvy písomne odstúpiť v prípadoch, ak Dodávateľ porušuje svoje povinnosti vyplývajúce z tejto zmluvy. Možnosť ktorejkoľvek zmluvnej strany odstúpiť od tejto zmluvy zo zákonom ustanovených dôvodov týmto nie je dotknutá.
5. Zánik 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, ku ktorému dôjde do jej zániku.
6. V prípade každého jednotlivého porušenia ktorejkoľvek povinnosti Dodávateľa, vyplývajúcej z tejto zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 5.000,-EUR (slovami: päťtisíc Euro).

7. V prípade opakovaného porušenia identickej povinnosti Dodávateľa, vyplývajúcej z tejto zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 30.000,-EUR (slovami: tridsaťtisíc Euro).
8. Zmluvná pokuta je splatná na základe výzvy Prevádzkovateľa na zaplatenie zmluvnej pokuty v lehote 14 dní odo dňa jej doručenia Dodávateľovi.
9. Nárok Prevádzkovateľa na náhradu škody voči Dodávateľovi, aj vo výške presahujúcej zmluvnú pokutu, nie je ustanoveniami o dojednaní zmluvnej pokuty, uplatnením zmluvnej pokuty voči Dodávateľovi ani jej zaplatením Dodávateľom dotknutý.
10. Ak vznikne Prevádzkovateľovi vznikne ujma z dôvodu pochybenia Dodávateľa, ktorý poruší svoje povinnosti v oblasti kybernetickej bezpečnosti dojednané touto zmluvou alebo uložené mu právnymi predpismi, a to tak, že Prevádzkovateľ bude na základe alebo v súvislosti s takou skutočnosťou zodpovedný za správny delikt v oblasti kybernetickej bezpečnosti alebo ochrany osobných údajov, vzniká Prevádzkovateľovi nárok na náhradu takejto ujmy voči Dodávateľovi v plnom rozsahu, vrátane prípadných ďalších vynaložených nákladov, vrátane nákladov za právne zastúpenie.

Článok IX.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu kybernetickej bezpečnosti u Dodávateľa Prevádzkovateľom

1. Prevádzkovateľ 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, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto zmluvy.
2. Prevádzkovateľ je oprávnený realizovať audit u Dodávateľa sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu uskutočňuje taká Prevádzkovateľom poverená tretia osoba.
3. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
4. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky osobám, ktoré sa za Dodávateľa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
5. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad plnenia povinností Dodávateľom s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne bezpečnostné povedomie svojich zamestnancov a iných osôb zúčastnených na predmete plnenia základného kontraktu a/alebo tejto zmluvy za Dodávateľa, ich záväzok a poučenie o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
6. Prevádzkovateľ je povinný oznámiť Dodávateľovi svoj zámer realizovať u Dodávateľa audit najmenej 7 pracovných dní vopred.
7. Výsledok auditu Prevádzkovateľ zaznamená do zápisnice. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 30 kalendárnych dní.
11. Ak Dodávateľ bezdôvodne neumožní Prevádzkovateľovi /resp. Prevádzkovateľom poverenej tretej osobe/ vykonanie auditu ani po opakovanej písomnej výzve, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy. Prevádzkovateľ je na základe nesplnenia si povinnosti Dodávateľom v zmysle predchádzajúcej vety

oprávnený tak odstúpiť od základného kontraktu s Dodávateľom a uplatniť si tak voči Dodávateľovi pokutu vo výške 10. 000,-EUR (slovami: desaťtisíc Euro).

8. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy.
9. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu u Dodávateľa a ktoré nie sú verejne známe. Prevádzkovateľ je povinný zabezpečiť zachovávanie mlčanlivosti v tomto zmysle každou osobou zúčastnenou na audite u Dodávateľa. Povinnosť zachovávať mlčanlivosť trvá aj po skončení trvania tejto zmluvy a/alebo základného kontraktu.
10. Prevádzkovateľ a ním poverené osoby 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 musia byť Dodávateľom oboznámení v zmysle nasledujúcich ustanovení tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. 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 je povinný preukázateľne informovať Prevádzkovateľa a ním poverené osoby 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 X.
Záverečné ustanovenia

1. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto zmluvy Prevádzkovateľovi udelí, poskytne, prevedie alebo na Prevádzkovateľa postúpi všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu s Prevádzkovateľom založeného touto zmluvou po dobu dohodnutú v trvaní päť rokov po ukončení zmluvného vzťahu.
2. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto zmluvy Prevádzkovateľovi vráti, prevedie a podľa pokynov Prevádzkovateľa prípadne aj zničí všetky informácie, ku ktorým mal Dodávateľ počas trvania zmluvného vzťahu prístup k Prevádzkovateľovi.
3. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto zmluvy a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na plnenie predmetu tejto zmluvy.
4. Akékoľvek sankcie a pokuty uplatnené podľa tejto zmluvy, ktoré si uplatní jedna zo zmluvných strán, je druhá zmluvná strana povinná uhradiť najneskôr do 30 dní odo dňa doručenia výzvy/faktúry na úhradu pokuty bezhotovostne na číslo účtu, uvedený vo výzve/faktúre doručenej na tento účel.
5. Dodávateľ bez predchádzajúceho písomného súhlasu Prevádzkovateľa nemá právo previesť práva a povinnosti vyplývajúce z tejto zmluvy na tretiu osobu.
6. Táto zmluva predstavuje úplnú dohodu zmluvných strán týkajúcu sa predmetu tejto zmluvy a nahrádza v celom rozsahu akékoľvek predchádzajúce dohody či návrhy uvádzané

v korešpondencii či na rokovaniach, či už ústne alebo písomné, ku ktorým došlo pred uzatvorením tejto zmluvy a ktoré jej uzatvorením zanikajú.

7. Táto zmluva sa riadi právom Slovenskej republiky. Právne vzťahy neupravené touto zmluvou sa spravujú príslušnými ustanoveniami Obchodného zákonníka a ostatnými všeobecne záväznými právnymi predpismi. Na riešenie sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.
8. Zmluva je vyhotovená v štyroch vyhotoveniach, ktoré majú povahu originálu, po dvoch vyhotoveniach pre každú zmluvnú stranu.
9. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy v zmysle ustanovenia čl. II, bodu 3. tejto zmluvy.
10. Akúkoľvek zmenu alebo doplnenie tejto zmluvy je možné vykonať výlučne formou písomných dodatkov podpísaných oboma zmluvnými stranami.
11. Táto zmluva je uzatvorená, vzniká a zaväzuje zmluvné strany okamihom, keď je podpísaná oboma zmluvnými stranami. V prípade, ak je niektorá so zmluvných strán povinná takúto zmluvu zverejniť v Centrálnom registri zmlúv, vykoná tak po jej podpísaní oboma zmluvnými stranami.
12. Osoby konajúce za zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, prejav ich vôle je slobodný a vážny, určitý a zrozumiteľný a je plne v súlade s obsahom tejto zmluvy, zmluvná voľnosť zmluvných strán nie je obmedzená, zmluvu si pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom ju vlastnoručne podpísali.

V Žiline, dňa 17.08. 2023	V Košiciach, dňa 8.8.2023
za Prevádzkovateľa	za Dodávateľa
_____	_____
Mgr. Eduard Dorčík, riaditeľ	Ing. Adrián Petrik, riaditeľ

Príloha č. 1 – Rozsah činností Dodávateľa v zmysle základného kontraktu
Príloha č. 2 – Bezpečnostné klauzuly pre dodávateľov a partnerov
Príloha č. 3 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa v zmysle základného kontraktu
Príloha č. 4 - Spôsob hlásenia bezpečnostných incidentov

PRÍLOHA 1

Rozsah činností Dodávateľa v zmysle základného kontraktu

Realizácia základného kontraktu pozostáva z nasledovných odborných činností:

- Analýza a projektová dokumentácia – Zhotoviteľ predloží obstarávateľovi Realizačný plán projektu, ktorý bude obsahovať vecný a časový harmonogram projektu.
- Konfigurácia systémového prostredia.
- Inštalácia, implementácia a systémová integrácia systému.
- Projektové riadenie.
- Zaškolenie používateľov.
- Podpora pri nábehu do ostrej prevádzky.
- Záručný servis.

PRÍLOHA 2

Bezpečnostné klauzuly pre dodávateľov a partnerov

1. Dodávateľ má právo pristupovať iba na zariadenia Fakultnej nemocnice s poliklinikou ďalej aj „FNsP" Žilina, ktoré sú vyslovene pod jeho správou. Prístup na iné zariadenie bez súhlasu Manažéra kybernetickej bezpečnosti ďalej aj „MKB" a odboru informatiky a správy systémov, je vážnym porušením pravidiel FNsP Žilina?.
2. V prípade, že by dodávateľ/partner využíval na služby, ktoré prevádzkuje pre FNsP Žilina subdodávateľa, je tento dodávateľ/partner povinný o tejto skutočnosti informovať a požiadať o súhlas MKB.
3. Vzdialený prístup do infraštruktúry FNsP Žilina je povolený len prostredníctvom schváleného VPN prístupu. Akýkoľvek iný prístup je zakázaný.
4. Všetky informácie pochádzajúce z prostredia FNsP Žilina sú dôverné po neobmedzenú dobu. V prípade, že sa dodávateľ k takýmto informáciám dostal omylom, je povinný to nahlásiť MKB a počkať na jeho pokyny a ďalší postup.
5. FNsP Žilina má právo na prístup k všetkým informáciám a to uloženým, alebo spracovávaným dodávateľom
6. FNsP Žilina má právo na bezpečnostný audit u dodávateľa/partnera, alebo má právo na takýto audit poveriť tretie spoločnosti. Takýto audit musí byť ohlásený minimálne 14 dní dopredu a jeho odmietnutie bude považované za hrubé porušenie pravidiel bezpečnosti FNsP Žilina.
7. FNsP Žilina má právo na monitorovanie všetkých činností dodávateľa/partnera v sieti Fakultnej nemocnice s poliklinikou a to bez ďalšieho schválenia dodávateľom/partnerom.
8. Po ukončení spolupráce s FNsP Žilina je dodávateľ/partner povinný bezodkladne zlikvidovať všetky dôverné informácie týkajúce sa FNsP Žilina, ktoré nadobudol počas spolupráce, ale aj tie, ktoré priamo nesúvisia so spoluprácou medzi dodávateľom/partnerom a FNsP Žilina.
9. Všetky osobné počítače pripájané priamo, alebo pomocou VPN musia spĺňať nasledovné kritériá:
    a. Osobný počítač má nainštalované všetky výrobcom predpísané aktualizácie
    b. Osobný počítač má nainštalovaný a aktuálny osobný antivírový systém
    c. Osobný počítač musí mať zapnutý osobný firewall
    d. Výnimky z týchto pravidiel schvaľuje MKB a odbor informatiky a správy systémov
10. Všetky sieťové zariadenia pripájané priamo, alebo pomocou VPN musia spĺňať nasledovné kritériá:
    a. Zariadenie musí bežať na poslednom stabilnom a výrobcom odporúčanom firmvéry
    b. Zariadenie musí mať aplikované všetky výrobcom stanovené bezpečnostné aktualizácie
    c. Výnimky z týchto pravidiel schvaľuje MKB a odboru informatiky a správy systémov

d. Pri fyzickom pripájaní akéhokoľvek zariadenia do siete fakultnej nemocnice s poliklinikou musí byť prítomný technik z odboru informatiky a správy systémov

11. Pri zistení neoprávneného prístupu do siete dodávateľa/partnera má tento povinnosť automaticky o tejto skutočnosti informovať FNsP Žilina a to konkrétne MKB a odbor informatiky a správy systémov. Informácia musí obsahovať okrem oznamu, aj konkrétne informácie o incidente, ako vyšetrenie incidentu, nápravné opatrenia a pod.
12. Každá osoba poverená dodávateľom/partnerom, ktorá pristupuje do siete FNsP Žilina sa musí do VPN prihlasovať vlastným prihlasovacím menom a heslom tak, aby bola zabezpečená jej jednoznačná identifikácia. Prihlasovanie zdieľanými kontami osoby alebo osôb dodávateľa/partnera nie je povolené a považuje sa za hrubé porušenie bezpečnostnej politiky FNsP Žilina.
13. Každá zmena konfigurácie zariadenia pripojeného do siete FNsP Žilina musí byť odkonzultovaná s MKB a odborom informatiky a správy systémov.
14. Dodávateľ/partner je povinný, okamžite odobrať všetky prístupy do infraštruktúry FNsP Žilina osobe, poverenej týmto dodávateľom/partnerom, ktorá s ním ukončila pracovný alebo obdobný pracovný vzťah alebo zmluvný vzťah ukončila spoluprácu s dodávateľom/partnerom a bezodkladne o tejto skutočnosti informovať FNsP Žilina.
15. Dodávateľ sa zaväzuje prijať a dodržiavať minimálne bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. d), f), g), k), m) Zákona o kybernetickej bezpečnosti v rozsahu podľa § 12, 10, 9, 15, 14 Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
16. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
17. Dodávateľ prehlasuje, že má zavedené a implementované bezpečnostné opatrenia podľa §20, ods. 3 Zákona o kybernetickej bezpečnosti pre oblasť:
    (i) riadenia prístupov,
    (ii) bezpečnosti pri prevádzke informačných systémov a sietí,
    (iii) hodnotenia zraniteľností a bezpečnostných aktualizácií,
    (iv) zaznamenávania udalostí a monitorovania,
    (v) riešenia kybernetických bezpečnostných incidentov.
18. Dodávateľ sa zaväzuje, že má vypracovanú bezpečnostnú dokumentáciu, ktorá obsahuje:

(i) Schválená bezpečnostná stratégia kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,
    (ii) Klasifikácia informácií a kategorizácia sietí a informačných systémov,
    (iii) Zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
    (iv) Vykonaná analýza rizík kybernetickej bezpečnosti.
19. Dodávateľ sa zaväzuje prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN EN ISO/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy,

Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

20. Dodávateľ sa zaväzuje vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na realizácií Projektu alebo budú mať prístup k informáciám Prevádzkovateľa základnej služby

PRÍLOHA 3
Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa v zmysle základného kontraktu

Prevádzkovateľ základnej služby:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou základnej služby**	**Telefónny kontakt**	**Email**
Jan Taliga	MKB	Bezpečnostný správca	041/515810	MKB@fnspza.sk
Vladimir Hirner	Security Specialista	Zmena konfiguracii Vysetrovanie incidentov	041 5110 650	it@fnspza.sk
Marian Kormaňák	Bezpečnostný správca	Incident manažment	041/515810	kormanak@fnspza.sk

Dodávateľ základnej služby:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou základnej služby**	**Telefónny kontakt**	**Email**
RNDr. Jana Šutá, MBA	Projektový manažér	Riadenie projektu	0905 382 550	suta@stapro.sk
Ing. Tomáš Červeňák	Hlavný analytik	Analýza, inštalácia, konfigurácia, školenie, konzultácie, podpora	0908 724 153	cervenak@stapro.sk
Ing. Marián Hrtánek	Konzultant	Analýza, inštalácia, konfigurácia školenie, konzultácie, podpora	0915 751 156	hrtanek@stapro.sk
Ing. Ľuboš Pavlinský	Konzultant	Analýza, inštalácia, konfigurácia školenie, konzultácie, podpora	0905 988 612	pavlinsky@stapro.sk

PRÍLOHA 4
Spôsob hlásenia bezpečnostných incidentov

Forma hlásenia: emailom na: kyberincident@fnspza.sk

Obsah hlásenia:

Fáza zistenia:

Identifikátor hlásenia
Dátum a čas zistenia incidentu
Kto zistil incident
Popis incidentu
Kto hlásil

Fáza riešenia:

Identifikátor hlásenia
Kto riešil incident
Dátum a čas doriešenia
Popis riešenia
Popis vzniknutých škôd
Opis prijatých opatrení
Návrh na prijatie nových opatrení
Kto hlásil