Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 017/5/2024/185

uzatvorená v zmysle § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 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:	Vojtecha Spanyola 43, 012 07 Žilina
IČO:	17 335 825
IČ DPH:	SK2020699923
DIČ:	2020699923
Zastúpený:	MUDr. Juraj Kacian, MPH - 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, Košice 1 040 01
IČO:	31 710 549
DIČ:	2020483982
IČ DPH:	SK2020483982
Štatutárny orgán:	Ing. Adrián Petrik, konateľ
Zapísaný:	v Obchodnom registri Mestského súdu Košice, odd. Sro, vložka č. 6435/V

(ďalej len „**Dodávateľ**“)

PREAMBULA

1. 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**“).
2. 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“ závisiacou od sietí a informačných systémov a podľa ustanovenia § 17 ods. 2 písm. b) zákona o kybernetickej bezpečnosti je zaradená do zoznamu základných služieb.
3. Prevádzkovateľ vyhlasuje, že si je vedomý svojich zmluvných a zákonných povinností, prijal všetky potrebné bezpečnostné opatrenia, ktoré bude počas platnosti tejto zmluvy udržiavať, má zodpovedajúce materiálne, technické a personálne vybavenie a zaväzuje sa poskytnúť Dodávateľovi potrebnú súčinnosť a informácie, aby mohol efektívne napĺňať účel a predmet tejto zmluvy.
4. Dodávateľ je zmluvným partnerom Prevádzkovateľa na poskytovanie služieb pre zabezpečenie a podporu prevádzky informačných systémov objednávateľa, resp. pre

zabezpečenie a podporu prevádzky vybraných informačných technológií na základe týchto uzavretých zmlúv:

- **Zmluva o dielo č. 017/1/2023/044** na dodanie diela s názvom „Rozšírenie NIS FONS Enterprise, oblasť Logistika, Modul Burza tovarov“ zo dňa 08.08.2023, účinná od 18.08.2023,
- **Zmluva o dielo č. 017/1/2023/045** na dodanie diela s názvom „Rozšírenie NIS FONS Enterprise, oblasť Logistika, Modul Vykrývanie objednávok“ zo dňa 08.08.2023, účinná od 18.08.2023,
- **Supervízna zmluva č. 017/1/2023/047, č. ST202302** na dodávanie služieb na zabezpečenie a podporu prevádzky laboratórneho informačného systému FONS Openlims inštalovaného v sídle Prevádzkovateľa v laboratórnych pracoviskách Oddelenia hematológie a krvnej banky zo dňa 08.08.2023, účinná od 18.08.2023,
- **Zmluva o dielo č. 017/1/2023/046** na dodanie diela s názvom „Rozšírenie NIS FONS Enterprise, oblasť Klinika, Modul eID“ zo dňa 23.02.2024, účinná od 12.03.2024,
- **Supervízna zmluva č. ST202415, č. objednávateľa 017/1/2024/145, podpora prevádzky IS** zo dňa 16.10.2024, účinná od 19.10.2024

(ďalej spoločne aj ako „**základný kontrakt**“)

5. Dodávateľ vyhlasuje, že je odborne spôsobilý na plnenie predmetu tejto zmluvy. Ďalej prehlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tejto zmluvy.
6. Dodávateľ sa zaväzuje vykonávať všetky činnosti definované v tejto Zmluve v súlade s všeobecne záväznými právnymi predpismi.
7. Zmluvné strany zhodne prehlasujú, že nič v tejto zmluve nezbavuje zmluvné strany zodpovednosti za plnenie vlastných povinností, ktoré im vyplývajú z právnych predpisov vydaných v súlade so zákonom o kybernetickej bezpečnosti a zo zákona o kybernetickej bezpečnosti.
8. Pojmy uvedené v tejto zmluve sa zhodujú s pojmami definovanými zákonom o kybernetickej bezpečnosti a v prípade ich slovnej nezhody sa použijú ustanovenia zákona o kybernetickej bezpečnosti, ktoré sú im významom najbližšie.
9. Ak sa v zmluve uvádza „dodanie produktu“ v rôznych gramatických tvaroch, zmluvné strany tým majú na mysli činnosť Dodávateľa na základe základného kontraktu bližšie identifikovanú v bode 4 tejto Preambuly bez ohľadu na to, či ide o dodanie tovaru alebo poskytnutie služby.

Článok I.
Predmet zmluvy

1. Predmetom tejto zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností Dodávateľa pri dodaní produktu na základe základného kontraktu, t. z. činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa počas celej doby výkonu činnosti Dodávateľa.
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 IT infraštruktúre Prevádzkovateľa pri dodaní produktu na základe základného kontraktu, a to aj pri jeho vývoji, ak je jeho súčasťou, v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy a bola zabezpečená kompatibilita s existujúcimi sieťami a informačnými systémami Prevádzkovateľa a zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej politike, ktorú Prevádzkovateľ definoval v prílohe č. 2 tejto zmluvy. Dodávateľ vyhlasuje, že súhlasí so špecifikáciou a rozsahom bezpečnostných opatrení požadovaných Prevádzkovateľom v zmysle tejto zmluvy. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom v zmysle tejto zmluvy.

4. Dodávateľ sa na základe tejto zmluvy zároveň zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa definované **v Prílohe č. 2 tejto zmluvy Bezpečnostné klauzuly pre dodávateľov a partnerov.**

5. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa uvedenými v Prílohe č. 2 tejto zmluvy. Dodávateľ súčasne akceptuje, že bezpečnostné politiky Prevádzkovateľa, ako aj ním prijaté smernice 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, oznámiť tieto zmeny bezodkladne Dodávateľovi formou mailu s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ mailom potvrdí akceptáciu zmien bezpečnostnej politiky.

6. Na základe tejto zmluvy sa tiež Dodávateľ zaväzuje plniť notifikačné povinnosti vo vzťahu k produktu dodanému na základe základného kontraktu tak, ako je definované v článku II, III a V tejto zmluvy, a to aj pri vývoji v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené jej ciele.

7. 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.

8. 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 alebo ktorej následkom je:

a) strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,

b) obmedzenie alebo odmietnutie dostupnosti základnej služby,

c) vysoká pravdepodobnosť kompromitácie činností základnej služby alebo

d) ohrozenie bezpečnosti informácií

(ďalej aj „**incidenty**“).

2. Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na prevádzku sietí a informačných systémov Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa

a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby sa minimalizovalo riziko prieniku kybernetického incidentu Dodávateľa do IT infraštruktúry 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 prevádzku sietí a informačných systémov Prevádzkovateľa,

e) vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na prevádzku sietí a informačných systémov 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, a to výlučne v súvislosti s produktami dodávanými na základe základného kontraktu,

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),

b) konkrétne Bezpečnostné klauzuly pre dodávateľov a partnerov, ktoré prijíma Dodávateľ a s ktorými súhlasí (Príloha č. 2),

c) zoznam pracovných rolí Prevádzkovateľa a 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**),

d) spôsob hlásenia bezpečnostných incidentov (Príloha č. 4).

5. Dodávateľ je povinný emailom na adresu: MKB@fnspza.sk, it@fnspza.sk bezodkladne oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí Dodávateľa.

6. Dodávateľ, ktorý je súčasne zaradený do registra prevádzkovateľov základných služieb, 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.

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. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti, a v rozsahu špecifikovanom v Prílohe č. 2 tejto zmluvy. Vykonanie bezpečnostných opatrení a povinností pre oblasť podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti podľa predchádzajúcej vety sa vzťahuje výlučne na zabezpečenie bezpečnostných opatrení vo vzťahu ku dodanému produktu Dodávateľa na základe základného kontraktu a vo vzťahu k jeho prepojeniu do sietí a informačných systémov Prevádzkovateľa tak, aby bola zabezpečená kybernetická bezpečnosť sietí a informačných systémov Prevádzkovateľa.

Článok III.
Reaktivita pri hlásení incidentov

1. Dodávateľ je povinný Prevádzkovateľovi bezodkladne, najneskôr do 24 hodín, hlásiť každý incident v príčinnej súvislosti s produktom dodaným na základe základného kontraktu 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 alebo iným ekvivalentným elektronickým spôsobom, ktorý permanentne zaznamenáva bezpečnostné incidenty a notifikuje Prevádzkovateľa. 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 primeranej lehote, nie dlhšej ako 5 pracovných dní, 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, v rozsahu, v akom za ne Dodávateľ zodpovedá, 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, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa. 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. 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 tejto zmluvy alebo základného kontraktu, 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. V prípade vzniku incidentu súvisiacom s plnením zo strany Dodávateľa alebo jeho Subdodávateľov je Dodávateľ povinný na žiadosť Prevádzkovateľa predložiť vyhlásenie o zachovávaní mlčanlivosti podľa prvej vety tohto bodu tejto 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 v súvislosti s dodaným produktom, 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 alebo iným ekvivalentným elektronickým spôsobom, ktorý permanentne zaznamenáva bezpečnostné incidenty a notifikuje Prevádzkovateľa, 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. 3 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 a v spojitosti s touto zmluvou ustanoviť ďalšieho Dodávateľa (ďalej len „**Subdodávateľ**“), ktorého činnosť môže mať vplyv na zabezpečenie bezpečnosti sietí a informačných systémov Prevádzkovateľa alebo ktorý bude mať prístup k údajom a informáciám Prevádzkovateľa, a 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) Za plnenie povinností svojich Subdodávateľov podľa tejto zmluvy zodpovedá priamo Dodávateľ tak, ako by ich poskytoval sám. 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 v prípade porušenia bezpečnostných opatrení alebo akýchkoľvek iných povinností dohodnutých v tejto zmluve Subdodávateľom, rovnako v prípade porušenia povinnosti Dodávateľa predložiť Subdodávateľa definovaného v tejto zmluve, nesie Dodávateľ; 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, ak sú Ministerstvom zdravotníctva Slovenskej republiky v postavení ústredného orgánu pre sektor zdravotníctvo vydané.
3. Dodávateľ je povinný v súvislosti s dodávanými produktami nakladať s informáciami, 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 v primeranej miere (v rozsahu evidovania logov a incidentov a dokumentovanie školení svojich zamestnancov – prezenčné listiny) a v prípade kybernetického incidentu spôsobeného porušením povinností na strane Dodávateľa v súvislosti s plnením tejto zmluvy alebo auditu vykonávanom u Dodávateľa v zmysle čl. IX tejto zmluvy predložiť Prevádzkovateľovi na jeho žiadosť uvedenú dokumentáciu/evidenciu na nahliadnutie.
5. Dodávateľ je oprávnený plniť svoj záväzok podľa základného kontraktu a v spojitosti s touto zmluvou aj prostredníctvom svojich Subdodávateľov za podmienok bližšie uvedených v čl. VI. tejto zmluvy, pričom je povinný zabezpečiť u Subdodávateľov riadne plnenie povinností na úseku kybernetickej bezpečnosti v rozsahu zákona o kybernetickej bezpečnosti. Dodávateľ je povinný zabezpečiť audit Subdodávateľov treťou stranou – renomovanou spoločnosťou, pričom o výsledku auditu je na požiadanie povinný oboznámiť Prevádzkovateľa.

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 Prevádzkovateľa (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, ak zmluvné strany neuzatvorili osobitnú zmluvu o spracúvaní osobných údajov, ktorej ustanovenia majú prednosť. 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.
7. Dodávateľ ako poučená osoba potvrdzuje svojím podpisom, že bol informovaný o zásadách ochrany osobných údajov v zmysle článku 13 a 14 príslušných recitálov Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, dostupné na webových stránkach prevádzkovateľa v sekcii „Ochrana osobných údajov, GDPR“.

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 bližšie definovaného v preambule v bod 4 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 poruší svoje povinnosti vyplývajúce z tejto zmluvy, a zároveň toto porušenie možno posúdiť ako závažné porušenie zmluvy. Možnosť ktorejkoľvek zmluvnej strany odstúpiť od tejto zmluvy zo zákonom ustanovených dôvodov týmto nie je dotknutá. Odstúpenie je účinné dňom doručenia písomného oznámenia o odstúpení od zmluvy druhej zmluvnej strane. V prípade pochybností sa má za to, že oznámenie o odstúpení bolo doručené na tretí deň odo dňa jeho zaslania poštou doporučene na adresu sídla druhej zmluvnej strany, pričom deň odoslania sa do tejto lehoty nepočíta. Odstúpením od zmluvy nie je dotknuté právo na náhradu škody a na úhradu zmluvnej pokuty, na ktorú vznikol nárok odstupujúcej strane pred odstúpením od zmluvy.
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 (slovom: päťtisíc eur).
7. Zmluvná pokuta je splatná na základe výzvy Prevádzkovateľa na zaplatenie zmluvnej pokuty v lehote 60 dní odo dňa jej doručenia Dodávateľovi.

8. Dodávateľ zodpovedá za škodu spôsobenú Prevádzkovateľovi porušením svojich povinností. Nárok Prevádzkovateľa na náhradu celkovej spôsobenej 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. Škoda sa nahrádza prednostne v peniazoch. Ak Prevádzkovateľovi vznikne škoda 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 škody v plnej výške voči Dodávateľovi.
9. Zmluvné strany sa dohodli, že prerušenie poskytovania služby vzdialeného prístupu Prevádzkovateľom Dodávateľovi alebo jeho Subdodávateľom v zmysle Prílohy č. 2 bod 3 tejto zmluvy, nemôže byť chápané ako porušenie vzájomných zmluvných vzťahov alebo neposkytnutie súčinnosti zo strany Prevádzkovateľa a Dodávateľ si z tohto titulu nemôže nárokovať akúkoľvek náhradu škody, náhrady alebo úľavy v ostatných zmluvných vzťahoch medzi Prevádzkovateľom a Dodávateľom.

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 certifikovanej tretej osoby, s ustanovením ktorej za audítora súhlasí aj Dodávateľ; v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu uskutočňuje taká Prevádzkovateľom poverená tretia osoba. V prípade, ak Dodávateľ neudelí Prevádzkovateľovi súhlas k dvom rôznym tretím osobám navrhnutým Prevádzkovateľom na vykonanie auditu u Dodávateľa, Prevádzkovateľ je oprávnený vykonať audit prostredníctvom inej tretej osoby podľa vlastného výberu, aj bez súhlasu Dodávateľa.
3. S výnimkou prípadu, ak dôjde na strane Dodávateľa ku kybernetickému incidentu, je audit možné vykonávať najviac 1 (jeden) krát ročne, a to spôsobom, aby takéto kontroly nezasahovali nad nevyhnutne nutnú mieru do činnosti Dodávateľa. V prípade vzniku kybernetického incidentu na strane Dodávateľa je Prevádzkovateľ oprávnený vykonať audit u Dodávateľa operatívne. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré bezprostredne súvisia s dodaným produktom na základe základného kontraktu a 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 14 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.
8. V prípade, ak Dodávateľ, jeho Subdodávateľ alebo výrobca produktu, v súvislosti s ktorým sú poskytované služby na základe základného kontraktu už bol v priebehu 1 predchádzajúceho roka auditovaný nezávislou externou akreditovanou autoritou a auditom kybernetickej bezpečnosti sa preukázalo splnenie požiadaviek na kybernetickú bezpečnosť, je Dodávateľ oprávnený preukázať splnenie povinností Dodávateľa certifikátom alebo iným výsledkom o vykonaní auditu, čím sa má za to, že audit Prevádzkovateľa bol riadne vykonaný, a teda Prevádzkovateľ nie je oprávnený vykonať ďalší audit v priebehu predmetného roka. V prípade, ak Dodávateľ alebo výrobca produktu, v súvislosti s ktorým sú poskytované služby na základe základného kontraktu nebol v priebehu jedného (1) predchádzajúceho roka auditovaný nezávislou externou akreditovanou autoritou, má Dodávateľ oprávnenie zabezpečiť vykonanie auditu podľa predchádzajúcej vety v primeranej lehote prostredníctvom nezávislej akreditovanej spoločnosti, výsledky ktorého je povinný bezodkladne po vykonaní auditu poskytnúť Prevádzkovateľovi (napríklad prostredníctvom poskytnutia certifikátu).
9. Ak Dodávateľ bezdôvodne neumožní Prevádzkovateľovi, resp. Prevádzkovateľom poverenej tretej osobe v zmysle bodu 2 tohto článku zmluvy, vykonanie auditu ani po opakovanej písomnej výzve, ani do 10 kalendárnych dní nepredloží na písomnú výzvu certifikát alebo iný výsledok o vykonaní auditu podľa predchádzajúceho bodu tejto zmluvy, 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 zmluvnú pokutu vo výške 5. 000,-EUR (slovom: päťtisíc eur).
10. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy.
11. 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.
12. 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. Uvedené povinnosti platia primerane aj pre Dodávateľa a jeho zamestnancov/resp. Subdodávateľa a jeho zamestnancov pri návšteve priestorov Prevádzkovateľa pri plnení predmetu základného kontraktu a plnení predmetu tejto zmluvy.

Článok X.
Záverečné ustanovenia

1. Táto zmluva ruší a nahrádza predchádzajúce zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností uzavreté medzi Prevádzkovateľom a Dodávateľom, a to konkrétne:
   - Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností zo dňa 17.08.2023, účinná dňa 18.08.2023, uzavretú k zmluve na dodanie diela s názvom „Rozšírenie NIS FONS Enterprise, oblasť Logistika, Modul Burza tovarov“ na základe uzavretej Zmluvy o dielo č. 017/1/2023/044 zo dňa 08.08.2023, účinná dňa 18.08.2023,
   - Zmluvu a o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností zo dňa 17.08.2023, účinná dňa 18.08.2023, uzavretú k zmluve na dodanie diela s názvom „Rozšírenie NIS FONS Enterprise, oblasť Logistika, Modul Vykrývanie objednávok“ na základe uzavretej Zmluvy o dielo č. 017/1/2023/045 zo dňa 08.08.2023, účinná dňa 18.08.2023,
   - Zmluvu a o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností zo dňa 17.08.2023, účinná dňa 18.08.2023, uzavretú k zmluve na dodávanie služieb na zabezpečenie a podporu prevádzky laboratórneho informačného systému FONS Openlims inštalovaného v sídle Prevádzkovateľa v laboratórnych pracoviskách Oddelenia hematológie a krvnej banky na základe uzavretej Supervíznej zmluvy č. 017/1/2023/047, č. ST202302 zo dňa 8.8.2023, účinná dňa 18.08.2023,
   - Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností zo dňa 23.02.2024, účinná dňa 23.02.2024, uzavretú k zmluve na dodanie diela s názvom „Rozšírenie NIS FONS Enterprise, oblasť Klinika, Modul eID“ na základe uzavretej Zmluvy o dielo č. 017/1/2023/046 zo dňa 23.02.2024, účinná dňa 12.03.2024.
2. V prípade rozporu medzi ustanoveniami tejto zmluvy s ustanoveniami o kybernetickej bezpečnosti obsiahnutými v jednotlivých základných kontraktoch majú prednosť ustanovenia tejto zmluvy.

3. Dodávateľ sa zaväzuje, že najneskôr ku dňu ukončenia 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.
4. Dodávateľ sa zaväzuje po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto zmluvy vrátiť, previesť alebo zničiť všetky informácie, ku ktorým mal Dodávateľ počas trvania zmluvného vzťahu prístup u Prevádzkovateľa.
5. 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.
6. Akékoľvek sankcie a pokuty uplatnené podľa tejto zmluvy, ktoré si uplatní jedna zo zmluvných strán, je druhá zmluvná strana povinná uhradiť najneskôr do 60 dní odo dňa doručenia výzvy/faktúry na úhradu pokuty bezhotovostne na číslo účtu, uvedený vo výzve/faktúre doručenej na tento účel.
7. Dodávateľ bez predchádzajúceho písomného súhlasu Prevádzkovateľa nemá právo previesť práva a povinnosti vyplývajúce z tejto zmluvy na tretiu osobu.
8. 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.
9. Táto zmluva sa riadi právom Slovenskej republiky. Právne vzťahy neupravené touto zmluvou sa spravujú príslušnými ustanoveniami zákona o kybernetickej bezpečnosti, jeho vykonávacími predpismi, Obchodným zákonníkom a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi. Na riešenie sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.
10. Zmluva je vyhotovená v štyroch vyhotoveniach, ktoré majú povahu originálu, po dvoch vyhotoveniach pre každú zmluvnú stranu.
11. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy v zmysle ustanovenia čl. II, bodu 4. tejto zmluvy:

    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.
12. Akúkoľvek zmenu alebo doplnenie tejto zmluvy je možné vykonať výlučne formou písomných dodatkov podpísaných oboma zmluvnými stranami.
13. Táto zmluva nadobúda platnosť dňom jej podpísania poslednou zo zmluvných strán a účinnosť najskôr dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv, ak v zmluve nie je dohodnutý neskorší dátum jej účinnosti.
14. 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 10.10.2024

Za Prevádzkovateľa:

MUDr. Juraj Kacian, MPH
riaditeľ FNsP Žilina

V Košiciach, dňa 14.10.2024

Za Dodávateľa:

Ing. Adrián Petrik
konateľ STAPRO SLOVENSKO s.r.o.

PRÍLOHA 1
Rozsah činností Dodávateľa v zmysle základného kontraktu

Rozsah činností Dodávateľa popisuje príloha č. 1, Supervíznej zmluvy č. ST202415, č. objednávateľa 017/1/2024/145

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, ktorého činnosť môže mať vplyv na zabezpečenie bezpečnosti sietí a informačných systémov Prevádzkovateľa alebo ktorý bude mať prístup k údajom a informáciám Prevádzkovateľa, je tento Dodávateľ/partner povinný o tejto skutočnosti informovať a požiadať o súhlas MKB v zmysle čl. VI tejto zmluvy.
3. Vzdialený prístup do IT infraštruktúry FNsP Žilina je povolený len prostredníctvom schváleného VPN prístupu. Akýkoľvek iný prístup je zakázaný. Prevádzkovateľ poskytuje službu vzdialeného prístupu pre Dodávateľa bez akýchkoľvek záruk a vyhradzuje si právo dočasne prerušiť poskytovanie služby vzdialeného prístupu v prípade podozrenia na jeho zneužitie alebo aj bez udania dôvodu. V takomto prípade Dodávateľ nie je v omeškaní s plnením služieb.
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, ktoré odsúhlasil Dodávateľ. Takýto audit musí byť ohlásený minimálne 14 dní dopredu a jeho odmietnutie bude považované za hrubé porušenie pravidiel bezpečnosti FNsP Žilina. Bližšie ustanovenia ohľadom vykonania auditu sú upravené v článku IX zmluvy.
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 IT infraštruktúry FNsP Žilina osobe, poverenej týmto Dodávateľom/partnerom, ktorá s ním ukončila pracovný alebo obdobný pracovný vzťah alebo zmluvný vzťah a ukončila tak 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), g) až i), k) a m) Zákona o kybernetickej bezpečnosti v rozsahu podľa 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. Vykonanie bezpečnostných opatrení a povinností podľa predchádzajúcej vety sa vzťahuje výlučne na zabezpečenie bezpečnostných opatrení vo vzťahu ku dodávaným a servisovaným produktom Dodávateľa na základe základnej zmluvy a vo vzťahu k ich prepojeniu do sietí a informačných systémov Prevádzkovateľa tak, aby boli naplnené ciele tejto zmluvy a bola zabezpečená kompatibilita s existujúcimi sieťami a informačnými systémami prevádzkovateľa a zachovanie úrovne bezpečnosti ustanovenej v stratégii, ktorú Prevádzkovateľ definoval v tejto prílohe

16. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia, ak sú Ministerstvom zdravotníctva SR v postavení ústredného orgánu pre sektor Zdravotníctvo vydané.

17. Dodávateľ prehlasuje, že má zavedené a implementované bezpečnostné opatrenia podľa §20 ods. 3 Zákona o kybernetickej bezpečnosti minimálne pre oblasť:

(i) riadenia prístupov,

(ii) hodnotenia zraniteľností a bezpečnostných aktualizácií,

(iii) ochrany proti škodlivému kódu,

(iv) sieťovej a komunikačnej bezpečnosti,

(v) zaznamenávania udalostí a monitorovania,

(vi) riešenia kybernetických bezpečnostných incidentov.

18. Dodávateľ sa zaväzuje, že Dodávateľ ako i jeho Subdodávatelia majú vypracovanú bezpečnostnú dokumentáciu, ktorá obsahuje:

    (i) Schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,

    (ii) Klasifikáciu informácií a kategorizáciu sietí a informačných systémov,

    (iii) Zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,

    (iv) Vykonanú analýzu rizík kybernetickej bezpečnosti.

19. Dodávateľ sa zaväzuje dodržiavať všeobecné bezpečnostné opatrenia podľa aktuálne platnej STN EN ISO/IEC 27001 (Informačné technológie. Bezpečnostné metódy, Pravidlá dobrej praxe riadenia informačnej bezpečnosti.), pričom certifikácia podľa tejto normy nie je podmienkou.

20. Dodávateľ sa zaväzuje vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na realizácií základného kontraktu 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**
Ing. Ján Taliga	Manažér kybernetickej bezpečnosti	MKB	041/5110 810	MKB@fnspza.sk
Ing. Vladimír Hirner	Security Specialista	Zmena konfigurácii Vyšetrovanie incidentov	041/5110 650	it@fnspza.sk
Mgr. Milan Mintúch	Bezpečnostný správca	Incident manažment	041/5110 810	mintuch@fnspza.sk

Dodávateľ:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou základnej služby**	**Telefónny kontakt**	**Email**
RNDr. Janka Šutá, MBA	Projektový manažér	Projektové riadenie	+421905382550	suta@stapro.sk
Ing. Miroslav Molčák	DPO	GDPR a KB	+421905417456	molcak@♪stapro.sk
Ing. Daniel Dzurík	IT špecialista	Certifikácia ISMS	+421905483510	dzurik@stapro.sk
Tomáš Kováč	Vedúci oddelenia konzultačných služieb, Hlavný analytik	Zabezpečenie služby v rámci supervíznej podpory	+421907674481	kovac@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