Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností ST 202434

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zmluva“) medzi:

Dodávateľ:

Názov:	**STAPRO SLOVENSKO s.r.o.**
Sídlo:	Hroncova 3, 040 01 Košice
Štatutárny zástupca:	Ing. Adrián Petrik
IČO:	31 710 549
DIČ:	2020483982
IČ DPH:	SK2020483982
Kontaktná osoba:	Ing. Miroslav Molčák
Email:	molcak@stapro.sk
Zapísaný:	Obchodný register Mestského súdu Košice, oddiel: Sro, vložka č. 6435/V

(ďalej len „dodávateľ")

a

Prevádzkovateľ základnej služby:

Názov:	**Univerzitná nemocnica Bratislava**
Sídlo:	Pažítková 1835/4, 82101 Bratislava
Štatutárny zástupca:	MUDr. Alexander Mayer, PhD., MPH, MHA
IČO:	31813861
DIČ:	2021700549
Kontaktná osoba:	Adam Lojkó
Email:	adam.lojko@unb.sk

(ďalej len **„prevádzkovateľ základnej služby")**

(prevádzkovateľ základnej služby a dodávateľ spoločne ďalej ako „zmluvné strany")

Článok 1
Úvodné ustanovenia

1.1. Univerzitná nemocnica Bratislava je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o kybernetickej bezpečnosti"). Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby.

1.2. Prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom túto zmluvu podľa zákona o kybernetickej bezpečnosti.

1.3. Zmluvné strany uzatvárajú túto zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na „Zmluva o poskytovaní služieb podpory a rozvoja pre moduly e Zdravie a pripojenia do klasifikačného systému v rámci nemocničného informačného systému Stapro MEDEA a ďalšie Zmluvnými stranami dohodnuté služby“ uzatvorenú medzi zmluvnými stranami č. **ST202431** (ďalej len „dodávateľská zmluva“), ktorá definuje konkrétny rozsah činností dodávateľa, a na základe ktorej dodávateľ poskytuje prevádzkovateľovi základnej služby výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby.

1.4. Plnenie bezpečnostných opatrení a notifikačných povinností zmluvnými stranami v oblasti kybernetickej bezpečnosti podľa tejto zmluvy sa vyžaduje počas celej doby trvania tejto zmluvy, pokiaľ zo zmluvy nevyplývajú povinnosti pre dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľskej zmluvy.

Článok 2
Predmet zmluvy

2.1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na dodávateľskú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby (s ktorými priamo súvisí výkon činností dodávateľa na základe dodávateľskej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by mohli negatívne ovplyvniť siete a informačné systémy prevádzkovateľa základnej služby a minimalizovať dopad a vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby prevádzkovateľa.

Článok 3
Práva a povinnosti zmluvných strán

3.1. Dodávateľ sa zaväzuje dodržiavať prevádzkovateľom základnej služby vydanú bezpečnostnú politiku a bezpečnostné smernice, s ktorými bol dodávateľ preukázateľne oboznámený (ďalej aj ako „bezpečnostná politika“), a ktorých zoznam tvorí prílohu č. 1 tejto zmluvy a bezpečnostné požiadavky uvedené v tejto zmluve.

3.2. Dodávateľ súhlasí s tým, že bezpečnostná politika prevádzkovateľa základnej služby sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa základnej služby a aktuálnym bezpečnostným rizikám a hrozbám týkajúcim sa dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na kvalitu, dostupnosť a bezpečnosť základnej služby prevádzkovateľa. Prevádzkovateľ základnej služby je povinný bezodkladne oboznámiť dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené.

3.3. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia prevádzkovateľa základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v článku 4. tejto zmluvy tak, aby boli naplnené ciele tejto zmluvy.

3.4. Bezpečnostné opatrenia prevádzkovateľa základnej služby sa môžu meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa základnej služby, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov prevádzkovateľa základnej služby. Prevádzkovateľ základnej služby je povinný bezodkladne oboznámiť dodávateľa s aktualizovanými bezpečnostnými opatreniami s dôrazom na zmeny v nich uvedené.

3.5. Dodávateľ vyhlasuje, že má potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role, opatrenia a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie účelu tejto zmluvy.

3.6. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

3.7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi základnej služby v určenej lehote nie kratšej ako 5 pracovných dní.

3.8. Zoznam zamestnancov dodávateľa, subdodávateľa a tretích osôb, ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa tejto zmluvy a ktorí budú mať prístup k informáciám prevádzkovateľa základnej služby (ďalej len „zoznam osôb“) tvorí prílohu č. 2 tejto zmluvy. Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby každú zmenu v zozname osôb podľa tohto bodu bezodkladne na mailovú adresu kontaktnej osoby prevádzkovateľa základnej služby.

3.9. Dodávateľ je povinný písomne informovať prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom na účely plnenia tejto zmluvy.

3.10. Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom incidente. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

3.11. Na výkon činností, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľskej zmluvy a/alebo tejto zmluvy, môže dodávateľ poveriť len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v prílohe č. 2 tejto zmluvy.

3.12. Odplata za plnenie povinností dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto zmluvy, sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom základnej služby dodávateľovi podľa dodávateľskej zmluvy.

Článok 4
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

4.1. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v rámci prevencie pred kybernetickými incidentmi, ktoré by mohli mať nepriaznivý dopad na základnú službu prevádzkovateľa, jeho informačné systémy a siete. Dodávateľ sa zaväzuje:

a) zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení dodávateľskej zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby,
b) sledovať výstrahy a varovania slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne, zasielať prevádzkovateľovi základnej služby včasné varovania pred incidentmi, ktoré by mohli negatívne ovplyvniť prevádzkovanie základnej služby prevádzkovateľa a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb alebo znižovanie kybernetických rizík,
c) monitorovať a vyhodnocovať také bezpečnostné riziká, ktoré by mohli mať nepriaznivý dopad na základnú službu prevádzkovateľa základnej služby,
d) predchádzať vzniku incidentov,
e) spolupracovať s prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.
f) chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.
g) hlásiť všetky skutočnosti, informácie, zmeny, ktoré môžu mať vplyv na túto zmluvu. Uvedené dodávateľ hlási formou elektronickej pošty do 2 dní od zistenia danej skutočnosti,
h) dodržiavať a prijať bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti, a to najneskôr do 20 pracovných dní. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

4.2. Pre oblasť technických zraniteľností informačných systémov a zariadení dodávateľ najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, prostredníctvom nasledujúcich opatrení:

a) Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
b) Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
c) Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

4.3. Pre oblasť riadenia bezpečnosti sietí a informačných systémov, ktoré dodávateľ využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, realizuje dodávateľ opatrenia:

a) Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len

servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom.

b) Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
c) Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
d) Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.
e) Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
f) Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
g) Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
h) Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.
i) Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
j) Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
k) Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.
l) Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.
m) Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.
n) Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.
o) Vykonávanie pravidelného alebo nepretržiFtého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

4.4. Pre oblasť riadenia prístupov, ktoré dodávateľ využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, realizuje dodávateľ nasledovné opatrenia:

a) Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
b) Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
c) Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám;

prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.

d) Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
e) Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
f) Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).
g) Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
h) Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

4.5. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje dodávateľ nasledovné opatrenia, pričom najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na výkon činnosti pre prevádzkovateľa základnej služby:

a) Oboznámenie sa s postupmi prevádzkovateľa základnej služby pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči prevádzkovateľovi základnej služby.
b) Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb prevádzkovateľovi základnej služby.
c) Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
d) Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.
e) Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov prevádzkovateľa základnej služby.
f) Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s prevádzkovateľom základnej služby.

g) Dodávateľ je povinný bezodkladne hlásiť každý incident prevádzkovateľovi základnej služby spôsobom určeným prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov.
h) Dodávateľ je povinný na žiadosť prevádzkovateľa základnej služby spolupracovať s Národným bezpečnostným úradom a na tento účel poskytnúť potrebnú súčinnosť a všetky informácie, ktoré by mohli byť dôležité pre riešenie incidentu.
i) Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz o bezpečnostnom incidente tak, aby tento mohol byť použitý v trestnom konaní a poskytnúť ho prevádzkovateľovi základnej služby.
j) Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
k) Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi základnej služby vykonanie a implementovanie nápravného opatrenia.

4.6. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje dodávateľ opatrenia podľa § 15 vyhlášky NBÚ č. 362/2018 Z. z., ktoré dodávateľ využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, najmä implementuje centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb prevádzkovateľovi základnej služby.

4.7. Dodávateľ vyjadruje súhlas s dodržiavaním uvedených bezpečnostných opatrení.

Článok 5
Mlčanlivosť

5.1. Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením dodávateľskej zmluvy a tejto zmluvy a ktoré nie sú verejne známe.

5.2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.

5.3. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu alebo obchodného vzťahu.

5.4. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. tieto podľa pokynu prevádzkovateľa základnej služby zničiť.

Článok 6
Kontaktné osoby na úseku kybernetickej bezpečnosti

6.1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom základnej služby spôsobom určeným prevádzkovateľom základnej služby, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

6.2. Prevádzkovateľ základnej služby určuje nasledovnú kontaktnú osobu pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti: Adam Lojkó – manažér kybernetickej bezpečnosti, email: adam.lojko@unb.sk

6.3. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti: Ing. Miroslav Molčák, e-mail: dpo@stapro.sk, tel.: +421905417456

Článok 7
Spoločné ustanovenia

7.1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi.

7.2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať negatívny vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by mohli narušiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

7.3. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy bezodkladne.

7.4. V prípade, ak dodávateľ poruší svoje povinnosti alebo záväzky v zmysle tejto zmluvy voči prevádzkovateľovi základnej služby, vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty a dodávateľ sa zaväzuje uhradiť zmluvnú pokutu vo výške 5000,- EUR za každé jedno porušenie.

7.5. V prípade, ak dodávateľ plní dodávateľskú zmluvu prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov. Dodávateľ je povinný vopred informovať prevádzkovateľa základnej služby o zapojení nového dodávateľa (teda subdodávateľa), a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom emailu na kontakt uvedený v záhlaví tejto zmluvy. Dodávateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb prevádzkovateľovi základnej služby nového subdodávateľa bez predchádzajúceho výslovného písomného súhlasu prevádzkovateľa základnej služby. Novému dodávateľovi (subdodávateľovi) je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto zmluve. Zodpovednosť voči prevádzkovateľovi základnej služby nesie dodávateľ, ak nový subdodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení alebo hlásenia bezpečnostných incidentov.

7.6. Dodávateľ je povinný hlásiť prevádzkovateľovi základnej služby ďalšie informácie požadované prevádzkovateľom základnej služby na plnenie jeho povinnosti vyplývajúcich zo zákona o kybernetickej bezpečnosti, najmä

a) informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované prevádzkovateľom základnej služby alebo Národným bezpečnostným

úradom a ústredným orgánom od prevádzkovateľa základnej služby za účelom splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm. c) zákona o kybernetickej bezpečnosti,

b) informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,

c) informácie potrebné na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm. e) zákona o kybernetickej bezpečnosti oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

d) informácie v potrebnom rozsahu na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 27 ods. 10 zákona o kybernetickej bezpečnosti.

Článok 8
Audit kybernetickej bezpečnosti

8.1. Prevádzkovateľ základnej služby je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov tejto zmluvy.

8.2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.

8.3. Prevádzkovateľ základnej služby môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti prevádzkovateľa základnej služby pri výkone auditu realizuje prevádzkovateľom základnej služby poverená tretia osoba.

8.4. Dodávateľ je povinný pri audite spolupracovať s prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

8.5. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi základnej služby súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.

8.6. Prevádzkovateľ základnej služby je povinný oznámiť dodávateľovi svoj zámer realizovať u neho audit najmenej päť pracovných dní vopred.

8.7. Dodávateľ je povinný písomne informovať prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom.

Článok 9
Záverečné ustanovenia

9.1. Táto zmluva sa uzatvára na dobu určitú, a to počas celého obdobia platnosti a účinnosti dodávateľskej zmluvy. Prevádzkovateľ základnej služby je oprávnený od tejto zmluvy odstúpiť v prípadoch, ak dodávateľ porušuje svoje povinnosti vyplývajúce z tejto zmluvy.

9.2. Po ukončení tejto zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

9.3. Táto zmluva sa spravuje právnym poriadkom Slovenskej republiky. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka a súvisiacimi predpismi.

9.4. Táto zmluva sa môže meniť alebo ukončiť iba dohodou zmluvných strán v písomnej forme.
Táto zmluva bola vyhotovená v troch rovnopisoch, z ktorých dva rovnopisy obdrží prevádzkovateľ základnej služby a jeden rovnopis obdrží dodávateľ.

9.5. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv.

9.6. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah tejto zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.

V Bratislave dňa .....

Za dodávateľa:

Ing. Adrián Petrik, konateľ

V Bratislave dňa .....

Za prevádzkovateľa základnej služby:

MUDr. Alexander Mayer, PhD., MPH, MHA

Príloha č. 1
Bezpečnostná dokumentácia

a) Bezpečnostné podmienky pre dodávateľov a iné tretie strany UNB (Bezpečnostné podmienky pre dodávateľov a iné tretie strany UNB v1.1.pdf),

Príloha č. 2
Zoznam osôb a pracovných rolí dodávateľa

Meno	**Názov oddelenia / tímu**	**Rola**
Ing. Adrián Petrik	Vedenie spoločnosti	riaditeľ a konateľ spoločnosti
Mgr. Maroš Gajdošík	Oddelenie obchodu a marketingu	obchodný manažér
Ing. Peter Pošefko	Tím podpory	vedúci tímu, senior konzultant
Ing. František Kupec	Tím podpory	senior konzultant, konzultant-analytik
Ing. Igor Černák	Tím podpory	senior konzultant, konzultant-analytik
Ing. Andrej Mitro	Tím podpory	senior konzultant, konzultant-analytik
Ing. Ivan Hnát	Tím Logistika	senior konzultant
RNDr. Jana Šutá, MBA	Oddelenie riadenia projektov	vedúca oddelenia riadenia projektov
Ing. Miroslav Molčák	Oddelenie riadenia projektov	senior konzultant, projektový manažér
Ing. Roman Mihaľ, PhD.	Oddelenie IT podpory	vedúci oddelenia, IT špecialista
Ing. Daniel Dzúrik	Oddelenie IT podpory	IT špecialista, správca IS
Mgr. Maroš Frankovič	Oddelenie IT podpory	IT špecialista, správca IS, nákupca
Ing. Miroslav Ilčin	Oddelenie IT podpory	IT špecialista, správca IS, nákupca