KRESTON SLOVAKIA

ZMLUVA O ZABEZPEČENÍ PLNENIA KYBERNETICKÝCH BEZPEČNOSTNÝCH OPATRENÍ A NOTIFIKAČNÝCH POVINNOSTÍ

knowing you.

Táto **ZMLUVA O ZABEZPEČENÍ PLNENIA KYBERNETICKÝCH BEZPEČNOSTNÝCH OPATRENÍ A NOTIFIKAČNÝCH POVINNOSTÍ** (ďalej len „**Zmluva**") sa uzatvára v súlade s ust. § 269 ods. 2 zákona č. 513/1991 Zb., Obchodný zákonník a zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov nižšie uvedeného dňa, mesiaca a roka medzi nasledovnými zmluvnými stranami:

ZMLUVNÉ STRANY

(A) **Psychiatrická nemocnica Philippa Pinela**, so sídlom Malacká cesta 63, 90201 Pezinok, IČO: 30 801 397, zriadený zriaďovacou listinou MZ SR č. 03472-21/2006-SP zo dňa 1.6.2006 (ďalej len ako „**Prevádzkovateľ základnej služby**");

a

(B) **Kreston Slovakia Technology, s.r.o.**, so sídlom Mlynské nivy 49, 821 09 Bratislava, IČO: 53 647 785, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel: Sro, vložka č.: 151580/B (ďalej len ako „**Dodávateľ**");

(Prevádzkovateľ základnej služby a Dodávateľ ďalej spoločne len ako „**Zmluvné strany**" a každý z nich vo všeobecnosti jednotlivo len ako „**Zmluvná strana**").

1. DEFINÍCIE A VÝKLAD

1.1. Pokiaľ nie je v tejto Zmluve uvedené inak, nasledovné pojmy majú tento význam:

1.1.1. **Dôverné informácie** akékoľvek verejne neprístupné informácie týkajúce sa Projektu a tiež akékoľvek dôverné alebo citlivé informácie získané Dodávateľom v dôsledku aktivít uskutočňovaných v súvislosti s Projektom, a to bez ohľadu na to, či súvisia s Projektom priamo alebo nepriamo a zároveň bez ohľadu na to, či sú tieto údaje, informácie alebo oznamy obchodnej, ekonomickej, prevádzkovej, marketingovej, finančnej, organizačnej, technickej, vedeckej, administratívnej alebo inej povahy a bez ohľadu na to, v akej forme a akým spôsobom sú podané alebo zachytené (verbálne, písomne, elektronicky alebo inak), vrátane všetkých informácií, oznámení, projektovej dokumentácie, správ z priebehu Projektu, údajov, know-how, procesov, dizajnov, fotografií, nákresov, špecifikácií, počítačových programov, vzoriek a akýchkoľvek iných materiálov, týkajúcich sa Projektu. Pre účely vylúčenia akýchkoľvek pochybností Zmluvné strany vyhlasujú, že Dôverné informácie zahŕňajú aj takú časť/také časti analýz, kompilácií, štúdií alebo iných dokumentov pripravených Zmluvnými stranami alebo ich poradcami, resp. ich zamestnancami, ktoré obsahujú alebo sú odvodené/získané z vyššie uvedených informácií o Projekte či z diskusií a rokovaní Zmluvných strán;

1.1.2.	**Dostupnosť**	znamená záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná;
1.1.3.	**Dôvernosť**	znamená záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom;
1.1.4.	**Hrozba**	znamená každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť;
1.1.5.	**Identifikované základné služby**	znamená identifikované základné služby Prevádzkovateľa základnej služby podľa Zákona o kybernetickej bezpečnosti, ktorými sú na účely tejto Zmluvy: ▪ Informačné systémy verejnej správy; ▪ Nemocničné informačné systém; ▪ Laboratórne informačné systémy;
1.1.6.	**Integrita**	znamená záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené;
1.1.7.	**Kybernetická bezpečnosť**	znamená stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov;
1.1.8.	**Kybernetický bezpečnostný incident**	znamená akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je: ▪ strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby; ▪ vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby; ▪ ohrozenie bezpečnosti informácií;
1.1.9.	**Obchodný zákonník**	znamená zákon č. 513/1991 Zb., Obchodný zákonník, v znení neskorších predpisov;

1.1.10.	**Občiansky zákonník**	znamená zákon č. 40/1964 Zb., Občiansky zákonník, v znení neskorších predpisov;
1.1.11.	**Oprávnené osoby**	znamená osoby, ktoré disponujú informáciami o Projekte na základe svojho postavenia alebo splnomocnenia (napríklad ako osoby poverené riadiť a/alebo spravovať Projekt), prípadne ktorým Prevádzkovateľ základnej služby udelil osobitné poverenie alebo splnomocnenie na účasti na Projekte a/alebo sa zúčastňujú na Projekte titulom poskytovania subdodávateľských vzťahov, poradenských, servisných alebo iných služieb, a sú oprávnené poskytnúť Dodávateľovi informácie klasifikované ako dôverné podľa tejto Zmluvy;
1.1.12.	**Projekt**	znamená projekt "**Pasportizácia IT prostredia v medicínskych zariadeniach MZ SR**", realizovaný na základe č. zmluvy 745/2022 pre Ministerstvo zdravotníctva SR, časť projektu: "Analýza rizík a nedostatkov v správe informačných technológií VS v MZ SR" (č. realizačnej zmluvy SE-VO-2022/001671-035);
1.1.13.	**Riešenie kybernetického bezpečnostného incidentu**	znamená všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov;
1.1.14.	**Riziko**	znamená miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami;
1.1.15.	**Tretie osoby**	znamená akékoľvek fyzické alebo právnické osoby, ktoré nedisponujú zákonným oprávnením alebo súhlasom Prevádzkovateľa základnej služby na to, aby boli oboznámené s Dôvernými informáciami;
1.1.16.	**Zákon o kybernetickej bezpečnosti**	znamená č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

1.2. Pri výklade Zmluvy sa použijú nasledovné výkladové pravidlá:

1.2.1. pokiaľ z kontextu nevyplýva niečo iné, akékoľvek slovo v jednotnom čísle zahŕňa aj jeho tvar v množnom čísle a naopak;

1.2.2. pokiaľ z kontextu nevyplýva niečo iné, akékoľvek slovo v mužskom rode zahŕňa aj ženský rod a naopak;

1.2.3. pokiaľ z kontextu nevyplýva niečo iné, akýkoľvek odkaz v tejto Zmluve na právne predpisy sa vykladá ako odkaz na tieto právne predpisy v znení ich neskorších zmien a dodatkov;

1.2.4. nadpisy tejto Zmluvy slúžia len na orientáciu, avšak nemajú vplyv na výklad Zmluvy.

2. ÚVODNÉ USTANOVENIA

2.1. Zmluvné strany uzatvárajú túto Zmluvu týkajúcu sa Projektu v nadväznosti na zmluvu č. 745/2022, uzatvorenú medzi Ministerstvom zdravotníctva SR a spoločnosťou stengl a.s. ako hlavným dodávateľom a Dodávateľom ako zmluvným subdodávateľom hlavného dodávateľa stengl a.s. (podľa oznámenia o doplnení subdodávateľa zo dňa 01.11.2022), pričom cieľom Projektu je zmapovanie aktuálneho stavu pripravenosti organizácií v pôsobnosti MZ SR z pohľadu efektívnosti, zabezpečenia kontinuity a stavu informačných technológií za účelom vzdialeného pripájania sa a vzdialenej správy prístrojov podaných v súlade s vyššie uvedenou zmluvou.

2.2. Prevádzkovateľ základnej služby na účely realizácie Projektu Dodávateľom rešpektuje zmluvné vzťahy Ministerstva zdravotníctva SR a Dodávateľa ako priameho subdodávateľa a z toho vyplývajúce poskytnutie súčinnosti zo strany Prevádzkovateľa základnej služby s cieľom realizácie analytickej časti Projektu.

2.3. Prevádzkovateľ základnej služby je povinný uzavrieť túto Zmluvu na účely splnenia svojej povinnosti podľa ust. § 19 ods. 2 Zákona o kybernetickej bezpečnosti, nakoľko predmet plánovanej činnosti Dodávateľa priamo súvisí s Dostupnosťou, Dôvernosťou a Integritou prevádzky sietí a informačných systémov Prevádzkovateľa základnej služby.

2.4. Zmluvné strany zároveň majú záujem na tom, aby akékoľvek a všetky informácie, ktoré si poskytnú v rámci Projektu zostali chránené ako dôverné.

2.5. Pre vylúčenie pochybností, Zmluvné strany si potvrdzujú, že predmetom Projektu a analytických činností Dodávateľa nie je spracovanie žiadnych osobných údajov. 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 (www.kreston.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.

3. PREDMET ZMLUVY

3.1. Predmetnom tejto Zmluvy je stanovenie práv a povinností Zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností v zmysle Zákona o kybernetickej bezpečnosti.

3.2. Dodávateľ sa zároveň zaväzuje zachovávať mlčanlivosť a dôvernosť Dôverných informácií, ak mu budú zo strany Prevádzkovateľa základnej služby poskytnuté, a poskytovať im náležitú ochranu, aby nedošlo k ich prezradeniu Tretím osobám alebo ich sprístupneniu verejnosti, k ich zneužitiu alebo k akejkoľvek neoprávnenej manipulácii s nimi.

4. POVINNOSTI DODÁVATEĽA

4.1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené ciele tejto Zmluvy a požiadavky Zákona o kybernetickej bezpečnosti. Zoznam bezpečnostných opatrení Prevádzkovateľa základnej služby a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti sprístupní Prevádzkovateľ základnej služby Dodávateľovi po podpise tejto Zmluvy a Dodávateľ sa zaväzuje ich dodržiavať v celom rozsahu. Zároveň je Dodávateľ povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby, s ktorými ho Prevádzkovateľ základnej služby preukázateľne písomne oboznámil. Dodávateľ súhlasí s tým, že bezpečnostné politiky Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa základnej služby a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby.

4.2. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve tak, aby boli v súlade so Zákonom o kybernetickej bezpečnosti, bezpečnostnými opatreniami a bezpečnostnými politikami Prevádzkovateľa základnej služby. Zoznam kontaktov Zmluvných strán je uvedený v prílohe č. 1 tejto Zmluvy.

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

4.4. 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 hlavným objednávateľom Projektu, pričom na žiadne ďalšie peňažné plnenia Dodávateľ

za plnenie povinností podľa tejto Zmluvy od Prevádzkovateľa základnej služby nemá nárok.

4.5. Dodávateľ sa zaväzuje, že všetky činnosti a plnenia podľa tejto Zmluvy zabezpečí riadne a včas spravidla vlastnými kapacitami, pričom v prípade, ak do akejkoľvek časti Projektu zapojí svojho subdodávateľa (ďalej len ako „**Subdodávateľ**") úplne alebo čiastočne zabezpečujúceho plnenie tejto Zmluvy, budú sa na tohto Subdodávateľa primerane vzťahovať povinnosti Dodávateľa uvedené v tejto Zmluve. Dodávateľ je plne zodpovedný voči Prevádzkovateľovi základnej služby za plnenie povinností Subdodávateľa podľa tejto Zmluvy tak, ako by ich poskytoval sám.

4.6. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy v súlade so Zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

4.7. Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby tak, aby nebola narušená ich Dostupnosť, Dôvernosť, Integrita a autentickosť.

4.8. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy na zabezpečenom priestore tak, aby nebola narušená ich Dôvernosť, Integrita a autentickosť.

5. BEZPEČNOSTNÉ OPATRENIA

5.1. 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.

5.2. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

5.3. 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.

5.4. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu v organizácii. Bezpečnostné opatrenia musia zahŕňať najmenej:

(i) detekciu kybernetických bezpečnostných incidentov,

(ii) evidenciu kybernetických bezpečnostných incidentov,

(iii) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,

(iv) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,

(v) prepojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania, ak sa táto povinnosť vzťahuje, resp. sa bude vzťahovať na Prevádzkovateľa základnej služby.

5.5. Obsah a štruktúra bezpečnostnej dokumentácie:

(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.

5.6. Dodávateľ sa zaväzuje počas trvania tejto Zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto Zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto Zmluvy.

5.7. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí sa budú podieľať na realizácií Projektu a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby, je uvedený v prílohe č. 1 tejto Zmluvy. Dodávateľ je povinný písomne oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa § 12 ods. 1 Zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení úloh spojených s Projektom.

5.8. Dodávateľ sa zaväzuje stanoviť postupy plnenia svojich povinností podľa tejto Zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu

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

5.9. 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.

5.10. V prípade, ak Dodávateľ spôsobí Prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. Pre odstránenie pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti z dôvodov na strane Dodávateľa alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.

6. PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

6.1. Dodávateľ sa zaväzuje v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby (ďalej len ako „**Incidenty**"):

(i) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa základnej služby,

(ii) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na realizácii Projektu alebo budú mať prístup k informáciám Prevádzkovateľa základnej služby,

(iii) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov Incidentov všeobecne,

(iv) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,

(v) predchádzať vzniku Incidentov,

(vi) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o Incidentoch,

(vii) prijímať od Prevádzkovateľa základnej služby varovania pred Incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,

(viii) zasielať Prevádzkovateľovi základnej služby včasné varovania pred Incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak,

(ix) spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby.

6.2. Dodávateľ sa zaväzuje dokumentovať svoju činnosť podľa tejto Zmluvy (vrátane evidovania Incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť Prevádzkovateľa základnej služby mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.

7. POSTUP PRI RIEŠENÍ INCIDENTOV

7.1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý Incident Prevádzkovateľovi základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie Incidentov. Ak do okamihu hlásenia Incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie Incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

7.2. Dodávateľ sa zaväzuje riešiť Incidenty najmä odozvou alebo inou reakciou na Incident, ohraničením Incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení Incidentu na mieste, reakciou na Incident a podporou reakcií na Incident (ďalej len ako „**Reaktívne opatrenie**"). Pri riešení Incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby a Národným bezpečnostným úradom 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.

7.3. Dodávateľ sa zaväzuje v čase Incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby.

7.4. Dodávateľ sa zaväzuje oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s Incidentom mohlo dôjsť k spáchaniu trestného činu.

7.5. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie Reaktívneho opatrenia a jeho výsledok.

7.6. Po vyriešení Incidentu je Dodávateľ na výzvu Prevádzkovateľa základnej služby v určenej lehote povinný predložiť Prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu Incidentu (ďalej len ako „**Ochranné opatrenia**") na schválenie.

7.7. Po schválení Ochranného opatrenia Prevádzkovateľom základnej služby, je Dodávateľ povinný Ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní Ochranného opatrenia Dodávateľom, je Dodávateľ povinný preveriť jeho účinnosť.

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, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy.

8.2. Dodávateľ je povinný predložiť záverečnú správu o výsledkoch auditu, ktorý vykonal u neho Prevádzkovateľ, Národnému bezpečnostnému úradu (NBÚ) spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

8.3. Prípadné nedostatky zistené auditom od Prevádzkovateľa základnej služby je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní alebo v lehote, s ktorou Dodávateľ písomne súhlasil v auditnej správe vytvorenej Prevádzkovateľom.

8.4. Prevádzkovateľ základnej služby môže audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba, ktorá je povinná zachovávať povinnosť mlčanlivosti o všetkých skutočnostiach zistených pri audite vo vzťahu k tretím osobám.

8.5. Dodávateľ sa zaväzuje pri audite spolupracovať s Prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, prípadne poskytnúť ďalšiu potrebnú súčinnosť.

8.6. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.

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

8.8. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej 30 (tridsať) pracovných dní vopred svoj zámer realizovať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto Zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.

8.9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.

8.10. Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku 9. tejto Zmluvy sa uplatňujú primerane.

8.11. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len ako „**BOZP**") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len ako „**PO**"), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ sa zaväzuje preukázateľne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia, vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

9. OCHRANA DÔVERNÝCH INFORMÁCIÍ

9.1. Dodávateľ sa týmto zaväzuje po dobu realizácie Projektu, na to nadväzujúcich zmluvných vzťahov a prebiehajúcich rokovaní medzi Zmluvnými stranami ako aj po ich skončení:

9.1.1. zachovávať mlčanlivosť o všetkých Dôverných informáciách, ktoré mu boli alebo budú poskytnuté či akokoľvek sprístupnené Prevádzkovateľom základnej služby alebo ktoré sú mu známe, alebo sa mu stanú známymi v súvislosti s akýmikoľvek rokovaniami s Prevádzkovateľom základnej služby týkajúcimi sa Projektu;

9.1.2. nepoužiť Dôverné informácie pre vlastný prospech alebo prospech Tretích osôb;

9.1.3. využívať Dôverné informácie výlučne na účely realizácie Projektu;

9.1.4. sprístupniť Dôverné informácie výlučne Oprávneným osobám;

9.1.5. sprístupniť Dôverné informácie príslušným štátnym alebo iným podobným orgánom verejnej moci (napr. súdom, daňovým orgánom) len na takom základe a v takom rozsahu, v akom to od Dodávateľa bude požadovať platný právny poriadok Slovenskej republiky, pričom Dodávateľ sa zaväzuje bezodkladne informovať Prevádzkovateľa

základnej služby o takejto požiadavke na sprístupnenie Dôverných informácií a jej obsahu a zároveň vynaložiť maximálne úsilie na získanie dostatočného ubezpečenia, že dôvernosť takto sprístupnených Dôverných informácií bude náležitým spôsobom zabezpečená;

9.1.6. reprodukovať, kopírovať, zhŕňať alebo distribuovať Dôverné informácie, či už vcelku alebo čiastočne, iba za podmienok uvedených v tejto Zmluve, pokiaľ sa Strany písomne nedohodnú inak;

9.1.7. neprezradiť ani nesprístupniť Dôverné informácie Tretím osobám ani verejnosti, pričom za porušenie tejto povinnosti sa nepovažuje sprístupnenie Dôverných informácií ďalším osobám, ktoré budú písomne zaviazané dodržiavať mlčanlivosť v súlade s podmienkami tejto Zmluvy za predpokladu, že Dôverné informácie potrebujú poznať z dôvodu ich účasti na realizácii Projektu;

9.1.8. dodržiavať a prijať zodpovedajúce technické, organizačné a iné opatrenia potrebné na ochranu Dôverných informácií, ktoré mu boli alebo budú poskytnuté alebo sprístupnené, pred neoprávnenou manipuláciou s nimi, a chrániť aktíva obsahujúce Dôverné informácie pred kybernetickým útokom v zmysle Zákona o kybernetickej bezpečnosti, ak je uvedené aplikovateľné.

9.2. Dodávateľ zodpovedá za konanie osôb podľa ods. 9.1.7 tejto Zmluvy tak, ako keby narábal s Dôvernými informáciami priamo sám.

9.3. Po skončení Projektu Dodávateľ vráti Prevádzkovateľovi základnej služby Dôverné informácie, ak mu boli tieto poskytnuté, a zabezpečí splnenie takejto povinnosti akoukoľvek Oprávnenou osobou, ktorej Dôverné informácie poskytol, pokiaľ sa s Prevádzkovateľom základnej služby nedohodne inak. Spoločnosť si nenechá v držbe žiadne kópie Dôverných informácií a tieto buď odovzdá Prevádzkovateľovi základnej služby podľa predchádzajúcej vety alebo ich, pokiaľ to nie je technicky možné, v rovnakej lehote bezpečným spôsobom zlikviduje. Pre vylúčenie pochybností, tie Dôverné informácie, ktoré je Dodávateľ povinný uchovať si na účely kontroly realizácie Projektu, budú uchované Dodávateľom po dobu piatich (5) rokov odo dňa ukončenia realizácie Projektu, ak v zmysle príslušných právnych predpisov nebude stanovená dlhšia lehota pre realizáciu kontroly Projektu.

9.4. Záväzok mlčanlivosti týkajúci sa Dôverných informácií podľa tejto Zmluvy sa nevzťahuje na prípady, keď existuje zákonná povinnosť oznámiť Dôverné informácie súdu, štátnemu orgánu alebo inému (na to oprávnenému) orgánu verejnej správy.

9.5. Dodávateľ je povinný oznámiť Prevádzkovateľovi základnej služby každú neoprávnenú manipuláciu s Dôvernými informáciami na svojej strane alebo Treťou osobou ihneď potom, ako túto skutočnosť zistí a zaväzuje sa vyvinúť v spolupráci s Prevádzkovateľom základnej služby maximálne úsilie na to, aby sa odstránili následky takejto neoprávnenej manipulácie, aby sa zabránilo ďalšej neoprávnenej manipulácii a tiež sa zabezpečili a obnovili všetky opatrenia potrebné na ochranu Dôverných informácií.

10. OZNÁMENIA A DORUČOVANIE, KONTAKTNÉ OSOBY

10.1. Všetky oznámenia súvisiace s touto Zmluvou sa uskutočnia písomne a považujú sa za riadne doručené, ak ich Zmluvná strana doručí druhej Zmluvnej strane akýmkoľvek z nasledovných spôsobov:

(i) osobným doručením;

(ii) zaslaním doporučenou poštou alebo prostredníctvom kuriéra.

10.2. Oznámenia podľa odseku 10.1 tejto Zmluvy sú považované za doručené momentom ich prevzatia, odmietnutia prevzatia alebo po uplynutí desiatich (10) dní odo dňa ich odovzdania na prepravu, ak sa jedná o doručovanie podľa odseku 10.1(ii) vyššie.

10.3. Oznámenia budú doručované na adresy uvedené v záhlaví Zmluvy a v prípade, že Zmluvná strana písomne oznámi inú adresu, na takúto inú adresu.

10.4. Dodávateľ sa zaväzuje komunikovať pri plnení povinností podľa tejto Zmluvy s Prevádzkovateľom základnej služby spôsobom určeným Prevádzkovateľom základnej služby, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

10.5. Prevádzkovateľ základnej služby ako aj Dodávateľ určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy. Kontaktné osoby podľa prílohy č. 1 tejto Zmluvy môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia tohto článku o doručovaní.

11. TRVANIE A UKONČENIE ZMLUVY

11.1. Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpisu oboma Zmluvnými stranami.

11.2. Táto Zmluva je uzatvorená na dobu určitú – do doby ukončenia realizácie Projektu.

11.3. Zmluvné strany sa dohodli, že túto Zmluvu je možné ukončiť aj písomnou dohodou Zmluvných strán.

11.4. Prevádzkovateľ základnej služby je oprávnený od tejto Zmluvy písomne odstúpiť v prípadoch:

(i) podstatného porušenia tejto zmluvy zo strany Dodávateľa;

(ii) ak je na Dodávateľa vyhlásený konkurz, alebo bola povolená reštrukturalizácia, alebo ak bolo vyhlásenie konkurzu odmietnuté alebo zrušené pre nedostatok majetku;

(iii) ak je Dodávateľ v likvidácii.

11.5. Za podstatné porušenie Zmluvy sa považuje:

(i) porušenie povinností uvedených v článku 4 odsekov 1 a 8, článku V odsekov 3 a 4, článku 7 a článku 9 tejto Zmluvy;

(ii) ak Dodávateľ vedel v čase uzavretia Zmluvy alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel Zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola zmluva uzavretá, že Prevádzkovateľ základnej služby nebude mať záujem na plnení povinností pri takom porušení Zmluvy;

(iii) Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto Zmluvy.

11.6. Túto Zmluvu je možné vypovedať Prevádzkovateľom základnej služby písomnou výpoveďou, aj bez uvedenia dôvodu, pričom výpovedná lehota je jeden (1) mesiac a začína plynúť prvým dňom mesiaca po mesiaci, v ktorom bola výpoveď Dodávateľovi doručená.

11.7. Ukončenie 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.

12. ZÁVEREČNÉ USTANOVENIA

12.1. Akékoľvek dodatky a zmeny tejto Zmluvy sú platné len v písomnej forme, po ich odsúhlasení a podpísaní oboma Zmluvnými stranami.

12.2. Ak by sa jednotlivé ustanovenia tejto Zmluvy celkom alebo čiastočne stali neúčinnými alebo ak v tejto Zmluve niektoré ustanovenie celkom chýba, nie je tým dotknutá účinnosť ostatných ustanovení. Namiesto neúčinného alebo chýbajúceho ustanovenia dohodnú Zmluvné strany také účinné ustanovenie, ktoré čo najviac zodpovedá zmyslu a účelu neúčinného alebo chýbajúceho ustanovenia.

12.3. V prípade zmeny údajov obsiahnutých v záhlaví tejto Zmluvy je tá Zmluvná strana, ktorej sa zmena týka, povinná bezodkladne písomne oznámiť túto skutočnosť druhej Zmluvnej strane spolu s uvedením aktuálnych údajov.

12.4. Táto Zmluva sa vyhotovuje v dvoch (2) rovnopisoch, po jednom rovnopise pre každú Zmluvnú stranu.

12.5. Zmluvné strany vyhlasujú, že sú plne spôsobilé k právnym úkonom, text tejto Zmluvy je určitým a zrozumiteľným vyjadrením ich vážnej a slobodnej vôle byť ňou viazaní, a že Zmluvu pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom k nej pripájajú svoje vlastnoručné podpisy.

12.6. K tejto Zmluve sa pripája príloha č. 1 – Zoznam kontaktov a pracovných rolí.

[PODPISY NASLEDUJÚ NA POSLEDNEJ STRANE]

[PODPISOVÁ STRANA]

Zmluvné strany pripájajú svoje podpisy k tejto Zmluve nižšie:

Poskytovateľ základnej služby:

V _Pezinku_ dňa _17.4.2023

_____
Psychiatrická nemocnica Philippa Pinela
Ing. Martin Hromádka, PhD.
konateľ

Dodávateľ:

V Bratislave dňa _____

_____
Kreston Slovakia Technology, s.r.o.
Dott. Andrej Aleksiev, PhD.
konateľ

Príloha č. 1
Zoznam kontaktov a pracovných rolí

Kontakty Poskytovateľa základnej služby

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	E-mail
Ľubomír Tilňák	Vedúci OIT		0905 624618	admin@pnpp.sk

Kontakty Dodávateľa

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	E-mail
Andrej Aleksiev	Kreston Technology partner a CTO	Incident management, eskalácia	+421 915 572 775	andrej.aleksiev@kreston.sk
Július Činčala	Kreston Technology partner		+421 911 515 276	julius.cincala@kreston.sk
Veronique Čapkovičová	Projektový manažér	Incident management, eskalácia	+421 904 920 275	veronika.capkovicova@kreston.sk
Branislav Baranovský	Konzultant pre IT bezpečnosť	Incident management, eskalácia	+421 907 782 144	branislav.baranovsky@kreston.sk
Marek Uličný	Konzultant pre IT bezpečnosť		+421 907 918 232	marek.ulicny@kreston.sk
Alexander Varga	Konzultant pre IT bezpečnosť, technik pre inštaláciu sieťových sond			alexander.varga@kreston.sk
Peter Matej	Konzultant pre IT bezpečnosť		+421 903 627 493	peter.matej@kreston.sk
Miloš Masiarik	Konzultant pre IT bezpečnosť		+421 903 246 186	milos.masiarik@kreston.sk
Martin Matuška	Konzultant pre IT bezpečnosť, technik pre inštaláciu sieťových sond	Technická podpora k technologickým zariadeniam	+421 917 999 808	martin.matuska@kreston.sk