Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená podľa ust. § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „**Obchodný zákonník**“) a podľa § 19 ods. 2 a 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z. z. (ďalej ako „**ZoKB**“)

medzi

Odberateľom:

Obchodné meno:	Poliklinika Senica n.o.
Sídlo:	Sotinská 1588, 90501 Senica
IČO:	36084212
DIČ/IČ DPH:	SK2021701154
Zapísaný:	v registri neziskových organizácií na KÚ v Trnave 3.dec. 2002 pod. č. VVS/NO-12/20002

(ďalej len **„Odberateľ“**)

a

Dodávateľom:

Obchodné meno:	Ing. Roman Mach – IT ROBEA
Sídlo:	J. Mudrocha 1351/18, 90501 Senica
IČO:	43020348
DIČ/IČ DPH:	1026248498
Registrácia:	Okresný úrad Senica, č. registra 240-16514

(ďalej len **„Dodávateľ**“ a spoločne s Odberateľom ako „**zmluvné strany“**)

(ďalej len ako „**zmluva**“)

Preambula

1. Odberateľ má postavenie prevádzkovateľa základnej služby v zmysle ZoKB, a to nasledovnej základnej služby: Laboratórne služby. Odberateľ musí podľa príslušných právnych predpisov zaistiť bezpečnosť sietí a informačných systémov, ktoré používa, pričom za týmto účelom je podľa ZoKB povinný prijať a aplikovať príslušné bezpečnostné opatrenia a plniť povinnosti pri oznamovaní kybernetických bezpečnostných incidentov. Požiadavky týkajúce sa bezpečnosti a oznamovania incidentov musí Odberateľ zachovávať bez ohľadu na to, či údržbu svojich sietí a informačných systémov vykonáva interne, alebo prostredníctvom externej osoby - Dodávateľa.
2. Dodávateľ ako externý dodávateľ služieb vykonáva činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Odberateľa (ďalej aj len ako „**služby**“). Služby Dodávateľ vykonáva na základe uzatvorenej zmluvy: Servisná zmluva o vykonávaní servisných služieb výpočtovej techniky, zo dňa 8.7.2008 (ďalej aj len ako „**Hlavná zmluva**“).
3. Odberateľ ako prevádzkovateľ základnej služby je povinný uzatvoriť s Dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa § 19 ods. 2 ZoKB.
4. Bez existencie tejto zmluvy Dodávateľ nemôže pre Odberateľa vykonávať služby, ktoré priamo súvisia s prevádzkou sietí a informačných systémov, to znamená, že skončenie platnosti tejto zmluvy spôsobuje nemožnosť plnenia podľa Hlavnej zmluvy v rozsahu činností podľa tohto bodu.
5. Pojmy použité v tejto zmluve majú rovnaký význam, ktorý majú podľa ZoKB a v prípade ich výslovnej nezhody sa použijú ustanovenia ZoKB, ktoré sú im významom najbližšie.
6. Účelom tejto zmluvy je zabezpečenie kybernetickej bezpečnosti sietí a informačných systémov Odberateľa ako prevádzkovateľa základnej služby počas ich životného cyklu, predchádzanie kybernetickým bezpečnostným incidentom na kontinuitu prevádzkovania základnej služby zo strany Odberateľa, a to v spolupráci s Dodávateľom.

I. Predmet zmluvy

1. Predmetom tejto zmluvy je úprava vzájomných práv a povinností zmluvných strán pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na Hlavnú zmluvu.
2. Dodávateľ sa zaväzuje vykonávať služby podľa Hlavnej zmluvy aj v plnom súlade s touto zmluvou a všeobecne záväznými právnymi predpismi, najmä ZoKB a v ich medziach tak, aby nedošlo k porušeniu bezpečnosti sietí a informačných systémov Odberateľa.
3. Dodávateľ je povinný vykonávať služby a činnosti definované v tejto zmluve v súlade s platnými všeobecne záväznými právnymi predpismi, sledujúc účel tejto zmluvy.
4. Dodávateľ vyhlasuje, že žiadne povinnosti podľa tejto zmluvy ho nezbavujú zodpovednosti za plnenie vlastných povinností, ktoré mu vyplývajú zo ZoKB a ostatných právnych predpisov vydaných v súlade alebo na vykovanie ZoKB.
5. Dodávateľ vyhlasuje, že sa pred uzatvorením tejto zmluvy podrobne oboznámil so všetkými bezpečnostnými opatreniami a notifikačnými povinnosťami, ktoré od neho Odberateľ vyžaduje plniť podľa tejto zmluvy, a to s ich predmetom, rozsahom a povahou, a vyhlasuje, že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek a splnenie povinností podľa tejto zmluvy.

II. Záväzky a povinnosti Dodávateľa

1. Dodávateľ sa zaväzuje pred začatím poskytovania služieb oboznámiť sa a dodržiavať bezpečnostnú politiku kybernetickej bezpečnosti – 5 Riadenie dodávateľských vzťahov, ktorú má Odberateľ prijatú (ďalej len „**Bezpečnostná politika kybernetickej bezpečnosti – dodávateľ**“) v časti, v ktorej sa služba Dodávateľa týka zásahu do siete a/alebo informačných systémov základnej služby, vymedzenej v čl. I. tejto zmluvy. Bezpečnostná politika kybernetickej bezpečnosti – dodávateľ, bola pred podpisom tejto zmluvy Dodávateľovi poskytnutá v potrebnom rozsahu. Obsah Bezpečnostná politika kybernetickej bezpečnosti – dodávateľ je dôverný a podlieha povinnosti mlčanlivosti v zmysle čl. V. tejto zmluvy.
2. Dodávateľ súhlasí s tým, že Bezpečnostná politika kybernetickej bezpečnosti – dodávateľ, môže byť priebežne menená a aktualizovaná, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Odberateľa a aktuálnym hrozbám, ktoré by mohli mať potenciálne nepriaznivý vplyv na základnú službu Odberateľa. Dodávateľ sa zaväzuje oboznámiť sa a dodržiavať aj všetky aktualizácie a doplnenia Bezpečnostnej politiky kybernetickej bezpečnosti – dodávateľa, ktoré budú voči Dodávateľovi záväzné dňom nasledujúcim po dni, v ktorom mu boli poskytnuté na oboznámenie, ak nebude Odberateľom určený neskorší dátum.
3. Dodávateľ podpisom tejto zmluvy vyjadruje svoj súhlas s Bezpečnostnou politikou kybernetickej bezpečnosti – dodávateľa, s ktorou sa oboznámil.
4. Dodávateľ sa zaväzuje, že bude chrániť všetky informácie poskytnuté Odberateľom, najmä chrániť ich dôvernosť, integritu, autentickosť, dostupnosť a obsah pri ich spracovaní a akomkoľvek nakladaní s nimi. Po skončení poskytovania služieb podľa Hlavnej zmluvy, vždy však najneskôr do 3 pracovných dní od skončenia tejto zmluvy vrátiť, previesť alebo zlikvidovať (zničiť) všetky informácie, ktoré boli Dodávateľovi za účelom plnenia Hlavnej zmluvy alebo tejto zmluvy poskytnuté alebo ku ktorým mal Dodávateľ v súvislosti s plnením Hlavnej zmluvy prístup. Likvidáciu môže vykonať len vo vzťahu k informáciám, pri ktorých sa tak s Odberateľom dohodne, inak platí, že Dodávateľ informácie vráti alebo prenesie na Odberateľa, a to vrátane všetkých kópií, záloh, vyhotovení, ktoré mal k dispozícii. Pokiaľ ide o prístupy do informačných systémov, sietí, v ktorých sa informácie nachádzajú, tieto prístupy vráti a dňom skončenia zmluvného vzťahu sa Dodávateľovi zakazuje akokoľvek vstupovať do systémov a sietí Odberateľa.
5. Dodávateľ sa zaväzuje držiavať a prijímať primerané bezpečnostné opatrenia podľa ust. § 20 ZoKB v spojení s Vyhláškou Národného bezpečnostného úradu SR č. 362/2018 Z. z., ktorou sa

ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len ako „**Vyhláška NBÚ č. 362/2018 Z. z.**“).

6. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia minimálne v rozsahu a podľa špecifikácie, ktorá je obsiahnutá v Prílohe č. 1 tejto zmluvy - Bezpečnostné opatrenia, ktorá je neoddeliteľnou súčasťou tejto zmluvy. Dodávateľ podpisom tejto zmluvy vyjadruje svoj súhlas s bezpečnostnými opatreniami. Odberateľ je oprávnený kedykoľvek počas trvania tejto zmluvy jednostranne zmeniť/aktualizovať/doplniť rozsah a špecifikáciu bezpečnostných opatrení, a to aj bez potreby uzatvorenia dodatku k tejto zmluve. Táto zmena sa uskutoční a je voči Dodávateľovi účinná a záväzná odo dňa nasledujúceho po dni, v ktorom Odberateľ doručí Dodávateľovi nové znenie Prílohy č. 1 tejto zmluvy.
7. Ak niektoré bezpečnostné opatrenie podľa Prílohy č. 1 nie je Dodávateľ schopný plniť presne podľa stanoveného rozsahu a špecifikácie, je oprávnený, avšak len po dohode s Odberateľom, takéto bezpečnostné opatrenie nahradiť iným, ktoré však bude garanciou bezpečnosti sietí a IS Odberateľa minimálne v obdobnom rozsahu ako bolo pôvodne stanovené bezpečnostné opatrenie. Takáto zmena musí byť vykonaná a odsúhlasená písomne.
8. Dodávateľ je povinný najneskôr do 5 pracovných dní od účinnosti tejto zmluvy, doručiť Odberateľovi zoznam všetkých pracovných rolí Dodávateľa, ktoré sa budú podieľať na plnení Hlavnej zmluvy a tejto zmluvy alebo budú mať prístup k informáciám Odberateľa, ktorý sa jeho doručením Odberateľovi stane súčasťou tejto zmluvy. Dodávateľ je povinný najneskôr do 5 pracovných dní od účinnosti tejto zmluvy, doručiť Odberateľovi úplný zoznam svojich zamestnancov, ktorí sa budú podieľať na plnení Hlavnej zmluvy a tejto zmluvy alebo budú mať prístup k informáciám Odberateľa, a každú zmenu v personálnom obsadení je Dodávateľ povinný písomne oznámiť. Všetky osoby podľa tohto bodu musia slobodne a vážne poskytnúť, a na znak tohto vlastnoručne podpísať záväzok (vyjadrenie) zachovávať mlčanlivosť podľa § 12 ods. 1 ZoKB. Splnenie povinnosti podľa predchádzajúcej vety zabezpečuje a eviduje Dodávateľ, ktorý zodpovedá za to, že služby budú poskytované výlučne len osobami, ktoré poskytli záväzok mlčanlivosti. Dodávateľ na žiadosť Odberateľa kedykoľvek preukáže splnenie tejto povinnosti.
9. Dodávateľ sa zaväzuje hlásiť Odberateľovi všetky potrebné informácie, ktoré si Odberateľ vyžiada pri zabezpečovaní požiadaviek kladených na Odberateľa podľa ZoKB alebo Vyhlášky NBÚ č. 362/2018 Z. z., a to spôsobom a formou podľa čl. IX. tejto zmluvy.
10. Dodávateľ je povinný nahlásiť Odberateľovi akékoľvek zmeny, ktoré môžu mať vplyv na túto zmluvu, na predmet plnenia alebo rozsah povinností podľa tejto zmluvy, či prípadne na správnosť, platnosť alebo aktuálnosť niektorého vyhlásenia alebo záväzku Dodávateľa, alebo na jeho schopnosť plniť túto zmluvu. Rovnako je povinný hlásiť všetky zmeny v jeho identifikačných údajoch a údajoch, ktoré majú vplyv na plnenie bezpečnostných opatrení podľa tejto zmluvy.
11. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby bol naplnený účel tejto zmluvy vymedzený v Preambule.
12. Dodávateľ je ďalej povinný:
    a. zabezpečiť vlastnú kybernetickú bezpečnosť, aby prostredníctvom neho nebolo možné zasiahnuť siete a informačné systémy Odberateľa,
    b. poskytovať Odberateľovi všetku potrebnú súčinnosť pri zabezpečovaní kybernetickej bezpečnosti Odberateľa,
    c. sledovať hrozby, ktoré sa týkajú Dodávateľa, ktoré sú spôsobilé ohroziť kybernetickú bezpečnosť Odberateľa a upozorniť Odberateľa na existenciu alebo výskyt takejto hrozby (t.j. aplikuje výstrahu a varovanie pred hroziacim incidentom),
    d. informovať Odberateľa o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
    e. okrem bezpečnostných opatrení podľa Prílohy č. 1, prijať a dodržiavať bezpečnostné opatrenia pre oblasť:

i. technických zraniteľností systémov a zariadení,
ii. riadenia bezpečnosti sietí a informačných systémov,
iii. riadenia prístupov,
iv. riešenia kybernetických bezpečnostných incidentov,
v. monitorovania, testovania bezpečnosti a bezpečnostných auditov,

to všetko v rozsahu podľa ust. § 8, 10, 12, 14 a 15 Vyhlášky NBÚ č. 362/2018 Z. z.

13. Dodávateľ môže zapojiť do poskytovania služieb na základe Hlavnej zmluvy subdodávateľa ak mu toto oprávnenie vyplýva z Hlavnej zmluvy počas doby jej platnosti a účinnosti. V prípade, ak Dodávateľ plní Hlavnú zmluvu úplne alebo aj len sčasti prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Odberateľa ako prevádzkovateľa základnej služby, je Dodávateľ povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy, ZoKB a Vyhlášky NBÚ č. 362/2018 Z. z. aj u svojich subdodávateľov a to v rovnakom rozsahu, ako je sám Dodávateľ povinný na základe tejto zmluvy. Títo subdodávatelia musia byť pred začatím poskytovania služby zaviazaní všetkými povinnosťami a záväzkami tak, ako je zaviazaný Dodávateľ v tejto zmluve a Hlavnej zmluve. Za splnenie, resp. prípadné nesplnenie/porušenie týchto povinností a záväzkov subdodávateľa zodpovedá v celom rozsahu Dodávateľ.
14. Dodávateľ je povinný zabezpečiť, aby Odberateľ mohol vykonať audit kybernetickej bezpečnosti v súlade s ustanoveniami tejto zmluvy aj u týchto subdodávateľov.

III. Rozsah činností Dodávateľa pri poskytovaní služieb

1. Dodávateľ bude pre Odberateľa vykonávať služby, pri ktorých je oprávnený vykonávať len nasledovné činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov Odberateľa:
   - Profylaxia zariadení v sieti.
   - Kontrola a údržba technického stavu hardvéru.
   - Inštalácia a údržba softvéru.
   - Telefonickú podporu v pracovnej dobe od 8 : 00 do 17 : 00.
   - Komunikácia s dodávateľom technológií.
   - Drobné a stredné opravy výpočtovej techniky, inštaláciu softvéru, údržbu laboratórnych systémov (podľa pokynov týchto systémov).
2. Vývoj a akvizícia siete a informačného systému základnej služby Odberateľa sa uskutočňuje s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii Odberateľa.

IV. Reaktivita pri riešení incidentov

1. Dodávateľ je povinný bezodkladne od okamihu, kedy sa dozvie (najneskôr do 24 hodín) nahlásiť Odberateľovi každý kybernetický bezpečnostný incident (ďalej aj len ako „**incident**“), o ktorom sa dozvie, a to spôsobom určeným touto zmluvou. Dodávateľ následne určí závažnosť incidentu.
2. Ak v čase hlásenia incidentu stále trvajú účinky incidentu, Dodávateľ je povinný odoslať Odberateľovi neúplné hlásenie aj s informáciou, že ide o neúplné hlásenie. Dodávateľ neúplné hlásenie bezodkladne doplní po obnove riadnej prevádzky siete a informačných systémov Odberateľa.
3. Dodávateľ bude využívať nasledovné spôsoby riešenia incidentov: odozva, ohraničenie incidentov a ich účinkov, náprava nepriaznivých účinkov incidentov, asistenciou pri riešení incidentu, reakciou na incident, podporou reakcie na incident, či iné vhodné činnosti spojené s nápravou incidentov (ďalej aj len ako „**reakčné opatrenia**“), a to aj bez výzvy Odberateľa, ak sa o incidente dozvie.
4. Dodávateľ pri riešení incidentov poskytne všetku potrebnú súčinnosť Odberateľovi, Národnému bezpečnostnému úradu SR, či inými príslušným orgánom a za týmto účelom

poskytne všetky informácie, ktoré nie sú dôvernými informáciami, ktoré by mohli mať vplyv a byť nápomocné pri riešení incidentu alebo odstraňovaní jeho následkov.

5. Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom alebo inom konaní, ku ktorému v súvislosti s incidentom došlo, resp. mohlo dôjsť a poskytnúť ho Odberateľovi aj bez potreby vyzvania.
6. Dodávateľ je povinný oznámiť Odberateľovi skutočnosti, že v súvislosti s incidentom mohlo dôjsť ku spáchaniu trestného činu.
7. Dodávateľ je povinný bezodkladne oznámiť a preukázať Odberateľovi prijatie alebo vykonanie reakčného opatrenia a jeho výsledok.
8. Dodávateľ bez zbytočného odkladu oznámi Odberateľovi prijatie reakčných opatrení. Ak o to Odberateľ požiada, po vyriešení incidentu je Dodávateľ v určenej lehote povinný predložiť Odberateľovi návrh opatrení na zabránenie ďalšieho pokračovania či opakovaného výskytu incidentu (ďalej aj len ako „**ochranné opatrenie**") na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Odberateľom na návrhu vhodného a efektívneho ochranného opatrenia. Po schválení ochranného opatrenia Odberateľom je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní ochranného opatrenia je Dodávateľ povinný preveriť jeho účinnosť.

V. Mlčanlivosť

1. Zmluvné strany sa v zmysle § 12 ZoKB zaväzujú zachovávať mlčanlivosť o podmienkach spolupráce podľa tejto zmluvy, ako aj o všetkých skutočnostiach týkajúcich sa druhej zmluvnej strany, jej činností, obchodných podmienok, rovnako skutočnosti, ktoré sa týkajú plnenia Hlavnej zmluvy alebo tejto zmluvy a pod., ktoré im boli sprístupnené počas trvania tejto zmluvy alebo ktoré sa im stali známe iným spôsobom. Uvedené sa týka najmä skutočností týkajúcich sa kybernetickej bezpečnosti a osobných údajov pracovníkov/ zamestnancov alebo iných dotknutých osôb, ktoré spracúva niektorá zo zmluvných strán. Povinnosť mlčanlivosti trvá aj po skončení tejto zmluvy alebo Hlavnej zmluvy bez časového obmedzenia.
2. Výnimky z povinností podľa tohto článku tejto Zmluvy upravuje ZoKB či iné príslušné všeobecne záväzné právne predpisy.
3. Na účely tejto zmluvy treba dôvernou informáciou rozumieť tiež akékoľvek informácie bez ohľadu na formu ich sprístupnenia, ktoré nie sú verejne prístupné, a/alebo ich niektorá zo zmluvných strán označí ako dôverné, ako aj iné údaje obchodného, finančného, prevádzkového, technického a/alebo iného charakteru, poskytnuté v ústnej, písomnej a/alebo elektronickej podobe a/alebo tvoriace predmet obchodného, daňového alebo bankového tajomstva zmluvnej strany, ktoré poskytne jedna zmluvná strana druhej zmluvnej strane v súvislosti s predmetom tejto zmluvy. Dôvernými sú aj informácie obsiahnuté v bezpečnostnej politike kybernetickej bezpečnosti, jeho bezpečnostnej dokumentácii pre oblasť kybernetickej bezpečnosti, vrátane prijatých bezpečnostných opatrení a obsah všetkých informačných systémov Odberateľa. V prípade pochybností, či určitá informácia je dôvernou informáciou sa má za to, že ide o dôvernú informáciu.
4. Zmluvná strana je povinná s dôvernými informáciami nakladať s primeranou starostlivosťou a dobromyseľne, nesmie takéto dôverné informácie prezradiť tretej osobe a ani ich použiť v rozpore s účelom, na ktorý boli poskytnuté, využiť ich pre svoje potreby, vo svoje prospech a/alebo v prospech tretích strán.
5. Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej zmluvnej strany nevyužijú pre seba a/alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k takýmto informáciám, to neplatí ak tak musia učiniť na účely splnenia zákonnej povinnosti.
6. Dodávateľ sa zaväzuje, že s dôvernými informáciami bude bezpečne narábať, zabezpečí ich dostatočnú ochranu pred akoukoľvek ich stratou, odcudzením, zničením, neoprávneným prístupom, náhodným či iným poškodením či iným neoprávneným využívaním alebo

spracovaním. Dodávateľ je povinný v prípade straty, odcudzenia, zničenia, neoprávneného prístupu k dôverným informáciám túto skutočnosť bezodkladne oznámiť Odberateľovi.

VI. Kontrolné činnosti a audity

1. Odberateľ je oprávnený vykonať u Dodávateľa audit zameraný na preverenie plnenia povinností Dodávateľa podľa tejto zmluvy a preverenie účinnosti prijatých bezpečnostných opatrení, na overenie technickej, technologickej a personálnej spôsobilosti Dodávateľa na vykonávanie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa. Dodávateľ poskytne Odberateľovi všetku potrebnú súčinnosť.
2. Audit sa uskutoční po predchádzajúcej dohode termínu a miesta jeho vykonania, pričom Dodávateľ zabezpečí prítomnosť kontaktnej osoby pre oblasť kybernetickej bezpečnosti na celom trvaní auditu. Ak sa nepodarí dosiahnuť dohodu o termíne alebo mieste auditu, stanoví ho jednostranne Odberateľ a tento termín alebo miesto oznámi Dodávateľovi v súlade s čl. IX. ods. 2 tejto zmluvy. Dodávateľ je povinný v tomto termíne a v určenom mieste umožniť riadny výkon auditu. Odberateľ môže vykonať aj neohlásený audit v prípade, kedy Dodávateľ zjavne nekomunikuje alebo neposkytuje súčinnosť dožadovanú Odberateľom, alebo ak má Odberateľ dôvodné pochybnosti o riadnom plnení tejto zmluvy zo strany Dodávateľa.
3. Neumožnenie vykonať audit sa bez ďalšieho považuje za podstatné porušenie tejto zmluvy a u Dodávateľa sa prezumuje vyvrátiteľná domnienka, že Dodávateľ porušuje túto zmluvu.
4. Odberateľ môže vykonaním auditu poveriť/splnomocniť aj tretiu osobu, ktorá je povinná sa pred začatím auditu Dodávateľovi legitimovať a preukázať svoje oprávnenie audit v mene Odberateľa vykonať. Dodávateľ je povinný tejto osobe umožniť vykonať audit.
5. Dodávateľ je povinný pri audite spolupracovať s Odberateľom, najmä mu sprístupniť svoje priestory v ktorých dochádza ku plneniu Hlavnej zmluvy alebo tejto zmluvy, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy. Prevádzkovateľ je oprávnený vyžiadať si na konzultáciu a vyjadrenie osoby, ktoré sa u Dodávateľa podieľajú na plnení predmetu Hlavnej zmluvy alebo tejto zmluvy a klásť im otázky.
6. Je povinnosťou dodávateľa pri audite preukázať Odberateľovi súlad s touto zmluvou, a riadne a včasné splnenie povinností v oblasti kybernetickej bezpečnosti podľa tejto zmluvy, preukázať prijatie a plnenie bezpečnostných opatrení a dodržiavanie Bezpečnostnej politiky kybernetickej bezpečnosti – dodávateľa, dodržiavanie povinnosti mlčanlivosti, aktuálnosť a úplnosť svojej bezpečnostnej dokumentácie a pod.
7. Odberateľ a osoby, ktoré v jeho mene vykonávajú audit sú viazané mlčanlivosťou o všetkých skutočnostiach, ktoré sa pri audite dozvedia, pričom všetky tieto skutočnosti sa považujú za dôverné informácie.
8. Ani vykonanie ani nevykonanie auditu v žiadnom prípade nezbavuje Dodávateľa zodpovednosti za riadne plnenie jeho povinností podľa tejto zmluvy, ZoKB, Vyhlášky NBÚ a iných všeobecne záväzných právnych predpisov, ktoré sa týkajú problematiky bezpečnosti sietí a informačných systémov Odberateľa.
9. Odberateľ a osoby ním určené pri návšteve priestorov Dodávateľa v rámci auditu sú povinné dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej ako „**BOZP**“) a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej ako „**PO**“), s ktorými boli v súlade s týmto bodom oboznámené oproti písomnému potvrdeniu týchto osôb, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, znáša Odberateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v celom rozsahu Dodávateľ.
10. Ak budú auditom zistené akékoľvek nedostatky, Odberateľ uloží Dodávateľovi povinnosť tieto nedostatky odstrániť, môže mu uložiť povinnosť prijať ďalšie bezpečnostné opatrenia alebo

vykonať určité úkony, v takom prípade je Dodávateľ povinný postupovať podľa pokynov Odberateľa a zistené nedostatky odstrániť bezodkladne, inak v určenej lehote, čo zároveň preukáže Odberateľovi.

VII. Doba trvania zmluvy

1. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu nadobudnutia účinnosti tejto zmluvy až do skončenia platnosti a účinnosti Hlavnej zmluvy, pokiaľ z právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti Hlavnej zmluvy.
2. Táto zmluva sa uzatvára na dobu určitú, na dobu trvania Hlavnej zmluvy.
3. Zmluvné strany sa dohodli, že zmluva zaniká:
   a. na základe písomnej dohody zmluvných strán,
   b. ukončením vzájomnej spolupráce medzi Odberateľom a Dodávateľom na základe Hlavnej zmluvy, t.j. ukončením Hlavnej zmluvy, aj bez potreby vykonania osobitného úkonu,
   c. jednostranným písomným odstúpením Odberateľa od zmluvy z dôvodov uvedených v tejto zmluve alebo z dôvodu iného závažného porušenia právnych predpisov alebo podstatného porušenia zmluvných povinností Dodávateľa alebo opakovaného porušenia zmluvných povinností Dodávateľa hoci aj menej závažným spôsobom, ak bol na ich riadne plnenie najskôr písomne upozornený, pričom účinky odstúpenia nastávajú dňom doručenia odstúpenia na adresu Dodávateľa, uvedenú v záhlaví tejto zmluvy alebo novú (zmenenú) adresu oznámenú Dodávateľom podľa tejto zmluvy.
4. Túto zmluvu nie je možné vypovedať.
5. Zmluvné strany sa dohodli, že skončením platnosti tejto zmluvy nie je dotknutá platnosť ustanovení o náhrade škody, sankciách za porušenie zmluvy, povinnosti mlčanlivosti, ods. 6 tohto článku zmluvy, ako ani iných ustanovení z ktorých zmyslu vyplýva, že majú zostať v platnosti aj po skončení tejto zmluvy, resp. že sa vzťahujú na obdobie po skončení platnosti tejto zmluvy.
6. Podľa ust. § 8 ods. 2 písm. p) Vyhlášky NBÚ č. 362/2018 Z. z., po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Odberateľa všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovania základnej služby Odberateľa na Odberateľa, pričom tento záväzok Dodávateľa zostáva platný a účinný aj po dobu piatich rokov po ukončení tejto zmluvy.

VIII. Zodpovednosť za škody a sankčné mechanizmy pri porušení zmluvy

1. Riadne a včasné neplnenie zmluvných a zákonných povinností Dodávateľa v súlade s touto zmluvou a príslušnými právnymi predpismi môže spôsobiť Odberateľovi škody, pričom Dodávateľ v plnom rozsahu zodpovedá Odberateľovi za všetky škody, vrátane škôd, ktoré sú dôsledkom incidentu, ktoré vzniknú v dôsledku porušenia ako aj nesplnenia alebo omeškania so splnením, ktorejkoľvek jeho povinnosti v zmysle tejto zmluvy (zodpovednosť za výsledok). Zodpovednosť za škodu podľa tohto článku sa bude bližšie spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. pre vylúčenie akýchkoľvek pochybností sa ustaľuje medzi zmluvnými stranami, že za škodu sa považujú aj sankcie uložené príslušnými dozornými, kontrolnými alebo inými príslušnými orgánmi (subjektmi). V prípade uloženia akejkoľvek sankcie podľa predchádzajúcej vety, v súvislosti s porušením zmluvných alebo zákonných povinností Dodávateľom alebo jeho subdodávateľom, je Dodávateľ povinný uhradiť Odberateľovi sumu uloženej sankcie v príslušnej časti, v ktorej sa sankcia týka porušenia povinnosti Dodávateľa. Finančná sankcia sa považuje za škodu a ak sankcia nemá finančnú povahu za škodu sa považujú náklady vynaložené v spojení s dôsledkami alebo vykonaním uloženej sankcie.

2. V prípade porušenia ktorejkoľvek povinnosti a /alebo záväzku Dodávateľa z tejto zmluvy má Odberateľ nárok na zaplatenie zmluvnej pokuty vo výške 1.000,- EUR za každé jednotlivé porušenie. V prípade ak sa jedná o opakované porušenie, ktorého sa Dodávateľ dopustí napriek predchádzajúcemu upozorneniu Odberateľa, je povinný zaplatiť zmluvnú pokutu vo výške 5.000,- EUR za každé jednotlivé porušenie. Sumy pokút sú uvedené bez DPH. Zaplatením zmluvnej pokuty nie je dotknutý nárok Prevádzkovateľa na náhradu škody vzniknutej v súvislosti s predmetným porušením v plnej výške. Zaplatením zmluvnej pokuty nie je Dodávateľ nijako zbavený svojej povinnosti splniť povinnosť alebo záväzok, za porušenie ktorého mu bola uložená pokuta a rovnako ani povinnosti odstrániť stav porušenia povinností, resp. jeho dôsledky.
3. Dodávateľ zodpovedá aj za škody a porušenia, ktorých sa dopustí jeho subdodávateľ, v celom rozsahu.
4. Náhrada škody a zmluvná pokuta je splatná na základe písomnej výzvy Odberateľa doručenej Dodávateľovi, v lehote určenej vo výzve, nie kratšej ako 30 dní od doručenia výzvy.
5. Ak Dodávateľ poruší svoju povinnosť podľa tejto zmluvy, je povinný bezodkladne po zistení tejto skutočnosti upustiť od porušovania zmluvy a prijať všetky opatrenia na to, aby odstránil následky porušenia a zabránil prípadným škodám, hrozbám, incidentom, ktoré v súvislosti s porušením môžu vzniknúť.

IX. Komunikácia a doručovanie

1. Komunikácia vo veciach týkajúcich sa plnenia tejto zmluvy, na úseku kybernetickej bezpečnosti, bude prebiehať prostredníctvom určených kontaktných osôb zmluvných strán, ktorými sú:
   za Odberateľa: Ing. Jozef Mikuš, riaditeľ, [redacted]
   za Dodávateľa: Ing. Roman Mach, IT manažér, [redacted]
   (ďalej aj len ako „**kontaktné osoby**“).
   Zmluvné strany sú povinné bezodkladne oznámiť druhej zmluvnej strane zmenu kontaktnej osoby alebo jej kontaktných údajov, inak zodpovedajú za škody spôsobené nesplnením tejto povinnosti druhej strane. Zmena kontaktnej osoby alebo jej údajov môže byť vykonaná aj bez potreby uzatvorenia dodatku k tejto zmluve. Kontaktné osoby sa musia zaviazať povinnosťou mlčanlivosti podľa § 12 ods. 1 ZoKB.
2. Kontaktné osoby budú komunikovať najmä vo veciach podávania oznámení, hlásení, vrátane hlásení informácií majúcich vplyv na túto zmluvu, a informácií požadovaných Odberateľom na plnenie jeho povinností podľa ZoKB, a informácií v súvislosti s dosiahnutím účelu tejto zmluvy, a to aj pri plnení úloh pri zabezpečovaní reaktivity podľa článku IV. tejto zmluvy. Kontaktné osoby sú určené na účely plnenia notifikačných povinností podľa tejto zmluvy. Pre vylúčenie pochybností sa ustaľuje, že kontaktné osoby nie sú oprávnené vykonávať právne úkony smerujúce k založeniu, zmene alebo skončeniu právneho vzťahu medzi zmluvnými stranami.
3. Komunikácia, hlásenia, oznámenia, kde nie je podľa ZoKB alebo tejto zmluvy výslovne požadovaná písomná forma, budú poskytované formou elektronickej komunikácie v čitateľnej forme (najmä šifrovanou emailovou komunikáciou alebo osobitne určeným komunikačným prostriedkom – ak taký bude určený) alebo písomne. Komunikácia a prenos informácií musí byť chránený. V situáciách, ktoré vyžadujú okamžité poskytnutie informácií, najmä pri ich poskytnutí telefonicky alebo ústne, tieto musia byť bezodkladne doplnené oznámením/hlásením v elektronickej alebo písomnej forme. Komunikácia musí prebiehať preukázateľne. Elektronická komunikácia (oznámenie, hlásenie, pokyn a pod.) sa bude považovať za doručenú okamihom, kedy adresát komunikácie (kontaktná osoba) odošle potvrdenie o doručení správy, pričom za dostatočné sa bude považovať aj automatické potvrdenie zaslané serverom adresáta. To však platí len ak bola komunikácia uskutočnená na určený kontakt.
4. V prípadoch, kedy táto zmluva alebo Hlavná zmluva výslovne vyžaduje písomnú formu komunikácie alebo pri právnych úkonoch, ktorými sa zakladá, dopĺňa, mení alebo ukončuje táto

zmluva alebo jej časť sa vyžaduje písomná forma komunikácie, ktorá musí byť doručená ako písomná zásielka v súlade s nasledovným bodom tohto článku.

5. Písomné zásielky budú doručované osobne k rukám osoby oprávnenej na preberanie zásielok za zmluvnú stranu, ktorá je adresátom zásielky alebo na adresy zmluvných strán uvedené v záhlaví tejto zmluvy, pričom dôkazom o doručení je doručenka s pečiatkou pošty/kuriérskej spoločnosti alebo vlastnoručný podpis osoby oprávnenej na preberanie zásielok, prípadne potvrdenie o doručení doporučenej zásielky. Pokiaľ si zmluvná strana, ktorej je zásielka určená, z akéhokoľvek dôvodu (adresát neznámy, neprevzal v odbernej lehote, odsťahoval sa a pod.) zásielku neprevezme v odbernej lehote, považuje sa zásielka za doručenú ku dňu kedy bol uskutočnený prvý neúspešný pokus o doručenie zásielky jej adresátovi, aj keď sa adresát o tom (doručovaní, uložení na pošte atď.) nedozvedel. Ak adresát odmietne zásielku prevziať, považuje sa táto za doručenú dňom, kedy bolo prevzatie zásielky odmietnuté.

X. Záverečné ustanovenia

1. Táto zmluva nadobúda platnosť dňom jej podpisu oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv.
2. Táto zmluva sa stáva súčasťou bezpečnostnej dokumentácie Odberateľa.
3. Pre vylúčenie akýchkoľvek pochybností platí, že všetky a akékoľvek plnenia, činnosti a úkony vykonávané pri plnení tejto zmluvy alebo v súvislosti s touto zmluvou, zmluvné strany vykonajú bezodplatne a bez nároku na akékoľvek náhrady.
4. Táto zmluva je vyhotovená v dvoch písomných vyhotoveniach s platnosťou originálu, po jednom vyhotovení pre každú zo zmluvných strán.
5. Akékoľvek zmeny a doplnenia tejto zmluvy je možné vykonávať výlučne formou písomných dodatkov podpísaných oboma zmluvnými stranami.
6. Pokiaľ akékoľvek ustanovenie tejto zmluvy alebo jej časti je, alebo ak sa stane neplatné alebo právne neúčinné, neovplyvní takáto neplatnosť alebo právna neúčinnosť ostatné ustanovenia tejto zmluvy. Zmluvné strany sa dohodli, že neplatné ustanovenie nahradia bezodkladne účinným, ktoré sa čo najviac hospodársky i vecne priblíži sledovanému účelu.
7. Právne vzťahy medzi zmluvnými stranami, ktoré nie sú upravené v tejto zmluve resp. právne vzťahy vznikajúce na základe plnenia predmetu tejto zmluvy, sa spravujú Hlavnou zmluvou, ZoKB, Vyhláškou NBÚ č. 362/2018 Z. z., Obchodným zákonníkom a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky. Rozhodné právo je slovenské.
8. V prípade akýchkoľvek súdnych sporov z tejto zmluvy je daná právomoc súdov Slovenskej republiky. V prípadoch, kedy sa miestna príslušnosť neurčí podľa zákona č, 160/2015 Z. z. Civilného sporového poriadku, príslušným bude vecne a miestne príslušný súd podľa sídla Odberateľa, pokiaľ právny poriadok Slovenskej republiky voľbu príslušného súdu v danej situácii umožňuje, resp. ju nevylučuje.
9. Zmluvné strany si túto zmluvu, vrátane jej príloh pred jej podpisom dôkladne prečítali, jej obsahu porozumeli a súhlasia s ním, na znak čoho ju vlastnoručne slobodne a vážne podpísali.

V Senici dňa 11.7.2023

Za Odberateľa:

.....

Poliklinika Senica n.o.

Ing. Jozef Mikuš, riaditeľ

Za Dodávateľa:

.....

Ing. Roman Mach – IT ROBEA

PRÍLOHA Č. 1

ku

Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorenej dňa 11.7.2023 (ďalej len ako „**zmluva**“)

medzi

Odberateľom:

Obchodné meno:	Poliklinika Senica n.o.
Sídlo:	Sotinská 1588, 90501 Senica
IČO:	36084212
DIČ/IČ DPH:	SK2021701154
Zapísaný:	v registri neziskových organizácií na KÚ v Trnave 3.dec. 2002 pod. č. VVS/NO-12/20002

(ďalej len **„Odberateľ“**)

a

Dodávateľom:

Obchodné meno:	Ing. Roman Mach – IT ROBEA
Sídlo:	J. Mudrocha 1351/18, 90501 Senica
IČO:	43020348
DIČ/IČ DPH:	1026248498
Registrácia:	Okresný úrad Senica, č. registra 240-16514

(ďalej len **„Dodávateľ**“ a spoločne s Odberateľom ako „**zmluvné strany“**)

ktorá je neoddeliteľnou súčasťou zmluvy, podľa článku II. ods. 6 zmluvy.

BEZPEČNOSTNÉ OPATRENIA

Dodávateľ je povinný prijať a dodržiavať minimálne nasledovné bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Dodávateľ berie na vedomie, že odberateľ je zaradený do zoznamu prevádzkovateľov základnej služby v sektore: **Zdravotníctvo**, podsektore: **Zdravotnícke zariadenia** a prevádzkuje základnú službu: **Laboratórne služby**.

e) Minimálne opatrenia pre oblasť technických zraniteľností

Dodávateľ je pre Odberateľa povinný v informačných systémoch a sieťach, ktoré sú prepojené s prevádzkovateľom základnej služby alebo môžu spôsobiť bezpečnostný incident ovplyvňujúci prevádzku základnej služby Odberateľa, zabezpečovať:

- identifikáciu technických zraniteľností vo vlastnej infraštruktúre, a to napr. prostredníctvom nástoja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, technických prostriedkov a ich častí a/alebo prostredníctvom sledovania verejných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov, ktoré Dodávateľ používa.
- V závislosti od spôsobu a rozsahu poskytovanej služby, aj nevyhnutné ďalšie opatrenia uvedené v §20 ods. 3, písm. e) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

f) Minimálne opatrenia pre oblasť riadenia bezpečnosti sietí a IS

Dodávateľ je pre Odberateľa povinný v informačných systémoch a sieťach, ktoré sú prepojené s prevádzkovateľom základnej služby alebo môžu spôsobiť bezpečnostný incident ovplyvňujúci prevádzku základnej služby Odberateľa, zabezpečovať:

- riadenie prístupov používateľov k sieťam a informačným systémom,
- pokiaľ dodávateľ uchováva / spracováva dáta odberateľa vo svojej infraštruktúre, zabezpečuje, že prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií,
- pokiaľ dodávateľ uchováva / spracováva dáta odberateľa vo svojej infraštruktúre, zabezpečuje, že segment siete s dátami odberateľa má implementovaný systém detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
- Pokiaľ sa dodávateľ pripája do vnútornej siete odberateľa, je takéto spojenie zabezpečené prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- V závislosti od spôsobu a rozsahu poskytovanej služby, aj nevyhnutné ďalšie opatrenia uvedené v §20 ods. 3, písm. f) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

h) Minimálne opatrenia pre oblasť riadenia prístupov

Dodávateľ je pre Odberateľa povinný v informačných systémoch a sieťach, ktoré sú prepojené s prevádzkovateľom základnej služby alebo môžu spôsobiť bezpečnostný incident ovplyvňujúci prevádzku základnej služby Odberateľa, zabezpečovať:

- Dodávateľ pri riadení prístupov osôb k sieti a informačným systémom zabezpečuje, že je 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 nevyhnutných pre prevádzkovateľa základnej služby.
- Dodávateľ má zavedený vlastný logický princíp riadenia prístupov používateľov, privilegovaných používateľov alebo administrátorov, pričom vykonáva kontrolu oprávnenosti využívania prihlasovacích a autentifikačných účtov svojich zamestnancov a neaktívne, nepotrebné účty v pravidelných intervaloch kontroluje a deaktivuje.
- Dodávateľ v systéme riadenia prístupov k sieťam prevádzkovateľa základnej služby zabezpečuje prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
- V závislosti od spôsobu a rozsahu poskytovanej služby, aj nevyhnutné ďalšie opatrenia uvedené v §20 ods. 3, písm. h) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

j) Minimálne opatrenia pre oblasť riešenia kybernetických incidentov

Dodávateľ je pre Odberateľa povinný v informačných systémoch a sieťach, ktoré sú prepojené s prevádzkovateľom základnej služby alebo môžu spôsobiť bezpečnostný incident ovplyvňujúci prevádzku základnej služby Odberateľa, zabezpečovať:

- Riešiť bezpečnostné incidenty!
- Hlásiť odberateľovi bezpečnostné incidenty, ktoré majú priamy alebo nepriamy súvis s prevádzkovanou základnou službou a mohli by ohroziť dôvernosť, integritu alebo dostupnosť služby.
- Dodávateľ má zabezpečený primeraný spôsob monitoringu a analyzovania udalostí v sieťach a informačných systémoch a zavedená systém detekcie kybernetických incidentov.
- Má zavedený systém evidencie kybernetických bezpečnostných incidentov na zabezpečenie dôkazu alebo dôkazného prostriedku. Eviduje aj informácie identifikujúce kybernetický bezpečnostný incident ako napríklad lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia.
- V závislosti od spôsobu a rozsahu poskytovanej služby, aj nevyhnutné ďalšie opatrenia uvedené v §20 ods. 3, písm. j) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

k) Minimálne opatrenia pre oblasť monitorovania, testovania, audity

Dodávateľ je pre Odberateľa povinný v informačných systémoch a sieťach, ktoré sú prepojené s prevádzkovateľom základnej služby alebo môžu spôsobiť bezpečnostný incident ovplyvňujúci prevádzku základnej služby Odberateľa, zabezpečovať:

- Vytvárať a archivovať dôkazy kybernetických bezpečnostných incidentov.
- Na požiadanie, po vzájomnej dohode, umožní Dodávateľ Odberateľovi vykonať u Dodávateľa audit, ako aj kontroly vykonávané Odberateľom alebo iným audítorom, ktorého poveril Odberateľ, a prispieva k nim
- V závislosti od spôsobu a rozsahu poskytovanej služby, aj nevyhnutné ďalšie opatrenia uvedené v §20 ods. 3, písm. k) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

ZOZNAM OPRÁVNANÝCH OSÔB

Dodávateľ určí oprávnené osoby, ktoré sa môžu vzdialeným prístupom pripájať do sietí a systémov odberateľa (vypíše sa aj s konkrétnym oprávnením, pokiaľ už neboli uvedené v hlavnej zmluve)

Oprávnená osoba	**Účel pripojenia a určenie systému alebo siete kam sa povolenie udeľuje**	**Spôsob bezpečného prístupu do vnútornej siete a informačného systému Odberateľa**
Ing. Roman Mach	Správa siete a serverov	VPN s dvojfaktorovým overením