Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená v zmysle § 261 ods. 2 a 3 písm. b) 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 (ďalej len ako „**zmluva**")
medzi týmito zmluvnými stranami:

názov:	**Obec Miloslavov**
sídlo:	Radničné námestie 181/1, 900 42 Miloslavov
IČO:	00 304 948
DIČ:	2020662182
IČ DPH:	
bankové spojenie:	SK58 0200 0000 0028 4551 4758
zastúpený:	Milan Baďanský, starosta obce

(ďalej len „**Prevádzkovateľ**")

a

obchodné meno:	**EMELIX, s. r. o.**
sídla:	Štúrova 61, 900 01 Modra
IČO:	35 804 386
DIČ:	2020205121
IČ DPH:	SK2020205121
údaj o zápise v OR:	Obchodný register Okresného súdu Bratislava I, oddiel: Sro, vložka č. 23294/B
zastúpený:	Ing. Adrian Mikóczi, konateľ

(ďalej len „**Dodávateľ**")

PREAMBULA

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

Základnou službou prevádzkovateľa sú **informačné systémy verejnej správy**, ktoré sú v zmysle ustanovenia § 3 písm. k) prvého bodu zákona o kybernetickej bezpečnosti činnosťou v sektore **verejná správa**, podsektore informačné systémy verejnej správy, závisiace od sietí a informačných systémov, a podľa ustanovenia § 17 ods. 2 písm. b) zákona o kybernetickej bezpečnosti sú zaradené do zoznamu základných služieb.

Dodávateľ je zmluvným partnerom Prevádzkovateľa na výkon činností, ktoré priamo súvisia s prevádzkou elektronických komunikačných sietí (ďalej len „**siete**") a informačných systémov prevádzkovateľa, pričom tieto činnosti dodávateľ uskutočňuje na základe už skôr uzatvorenej zmluvy, uzatvorenej s prevádzkovateľom dňa 08.02.2021 (ďalej len „**základný kontrakt**"), ktorej predmetom je:

a) proaktívna pravidelná údržba servera a staníc podľa rozpisu v prílohe.
b) servisné práce na základe objednávky objednávateľa:
   - konzultácie a poradenstvo pri plánovaní a obstarávaní informačnej a telekomunikačnej techniky
   - dodávka hardvéru a softvéru na základe objednávky

- inštalácia a konfigurácia počítačovej siete na základe objednávky
- odstraňovanie bežných porúch (diagnostika porúch hardvéru a odstránenie softvérových porúch)
- nastavovanie sieťového prostredia
- inštalácia, reinštalácia aplikačného programového vybavenia a ovládačov periférií, optimalizácia a správne nastavenie funkčnosti,
- údržba tlačiarní
- nastavenie prístupu na internet a správa emailových kont

Zmluvné strany sa rozhodli v súlade s ustanovením § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení **rozšíriť rozsah služieb poskytovaných Dodávateľom na základe základného kontraktu, a to formou tejto zmluvy**. Prihliadnuc na značný rozsah práv a povinností, ktoré zmluvným stranám vyplývajú podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení, a ktoré nie sú predmetom úpravy základného kontraktu, zvolili si zmluvné strany tento spôsob úpravy zmluvných pomerov, nakoľko uzavretie dodatku k základnému kontraktu by mohlo pôsobiť mätúco.

A teda platí, že zmluvné dojednania základného kontraktu ostávajú touto zmluvou nedotknuté. Touto zmluvou nad rámec (popri) základného kontraktu upravujú zmluvné strany vzájomné práva a povinnosti vyplývajúce v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení.

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 cieľov tejto zmluvy.

Ak nie je uvedené inak, pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

Článok I.
Predmet zmluvy

1. Predmetom tejto zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa.
2. Táto zmluva upravuje základné princípy spolupráce zmluvných strán pri uskutočňovaní plnenia bezpečnostných opatrení – úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa počas ich životného cyklu, s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby Prevádzkovateľa (ďalej len „**ciele**“).
3. Súčasťou záväzkov Dodávateľa podľa tejto zmluvy je povinnosť Dodávateľa prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Prevádzkovateľ vyhlasuje, že súhlasí so špecifikáciou a rozsahom bezpečnostných opatrení prijímaných Dodávateľom v zmysle tejto zmluvy. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.

4. Na základe tejto zmluvy sa tiež Dodávateľ zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené jej ciele.
5. Odplata za plnenie povinností Dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto zmluvy sú v celom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa základného kontraktu a za plnenie povinností podľa tejto zmluvy Dodávateľ nemá nárok na žiadne ďalšie peňažné plnenia od Prevádzkovateľa.
6. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania základného kontraktu.

Článok II.
Prevencia kybernetických bezpečnostných incidentov

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

zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti v rozsahu potrebnom na efektívne napĺňanie cieľov tejto zmluvy.

4. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi na nahliadnutie a zhotovenie kópií.
5. Dodávateľ je povinný prijať a dodržiavať všeobecné a sektorové bezpečnostné opatrenia v dotknutých oblastiach podľa zákona o kybernetickej najmenej pre oblasť podľa § 20 ods. 3 písm. d), f), g), m), k) a p) zákona o kybernetickej bezpečnosti, a to:
   - riadenia prístupov,
   - bezpečnosti pri prevádzke informačných systémov a sietí,
   - hodnotenia zraniteľností a bezpečnostných aktualizácií,
   - riešenia kybernetických bezpečnostných incidentov,
   - zaznamenávania udalostí a monitorovania,
   - auditu, riadenia súladu a kontrolných činností.

Článok III.
Reaktivita pri hlásení incidentov

1. Dodávateľ je povinný Prevádzkovateľovi bezodkladne hlásiť každý incident o ktorom má vedomosť kontaktnej osobe pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti (čl. V. bod 3.) určeným Prevádzkovateľom, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Dodávateľ je povinný riešiť incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len **„reaktívne opatrenie"**). Pri riešení incidentu je Dodávateľ povinný na žiadosť Prevádzkovateľa spolupracovať s Prevádzkovateľom, Národným bezpečnostným úradom a Ministerstvom zdravotníctva Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.
3. Dodávateľ je povinný Prevádzkovateľovi bezodkladne oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok.
4. Dodávateľ je povinný v čase incidentu vyvinúť snahu na zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi.
5. Po vyriešení incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej k tomu primeranej lehote nie kratšej ako desať pracovných dní povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len **„ochranné opatrenia"**) na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenia v určenej lehote alebo ak sú navrhované ochranné opatrenia zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom na jeho návrhu.

6. Po schválení ochranných opatrení Prevádzkovateľom je Dodávateľ povinný ochranné opatrenia bez zbytočného odkladu vykonať. V prípade, ak takéto opatrenia budú vyžadovať vynaloženie finančných či iných nákladov, tak budú hradené v plnej výške Prevádzkovateľom
7. Po vykonaní ochranných opatrení Dodávateľom je Dodávateľ povinný preveriť ich účinnosť.

Článok IV.
Ochrana informácií a povinnosť zachovávať mlčanlivosť

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

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

1. Dodávateľ je povinný hlásiť Prevádzkovateľovi za účelom plnenia povinností Prevádzkovateľa vyplývajúcich zo zákona o kybernetickej bezpečnosti všetky ďalšie Prevádzkovateľom požadované informácie, pokiaľ sú mu známe, a to najmä informácie potrebné pre:
   a) riešenie kybernetického bezpečnostného incidentu,
   b) hlásenie závažného kybernetického incidentu,
   c) poskytnutie súčinnosti a spolupráce s Národným bezpečnostným úradom,
   d) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
   e) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka.
2. Dodávateľ je povinný realizovať hlásenia podľa predchádzajúceho ustanovenia bodu 1. tohto článku zmluvy a komunikovať s Prevádzkovateľom pri plnení povinností podľa tejto zmluvy spôsobom a formou určeným Prevádzkovateľom, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií. Zmluvné strany berú na vedomie, že hlásenia podľa bodu 1. tohto článku zmluvy ako aj poskytovanie ďalších informácií pri plnení povinností podľa tejto zmluvy si budú realizovať telefonicky, e-

mailom a/alebo písomne, pričom konkrétny spôsob a formu takého oznámenia budú voliť podľa hľadiska účelnosti a naliehavosti nahlasovaných informácií.

3. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:

meno a priezvisko:	**Hana Pokorná**
funkcia/pracovná pozícia	referent ekonomiky
telefónne číslo:	0917 775 632
e-mailová adresa:	hana.pokorna@miloslavov.sk
meno a priezvisko:	**Mgr. Martin Sitiar**
funkcia/pracovná pozícia	vedúci hospodárskej správy
telefónne číslo:	0917 368 097
e-mailová adresa:	martin.sitiar@miloslavov.sk

4. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti:

meno a priezvisko:	**Ing. Adrian Mikóczi**
funkcia/pracovná pozícia	konateľ
telefónne číslo:	0903 64 25 26
e-mailová adresa:	emelix@emelix.sk
meno a priezvisko:	**Michal Rajník**
funkcia/pracovná pozícia	technik IT
telefónne číslo:	0910 63 25 26
e-mailová adresa:	rajnik@emelix.sk

5. Zmenu kontaktných osôb na úseku kybernetickej bezpečnosti môže každá zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok VI.
Podmienky a možnosti zapojenia ďalšieho Dodávateľa

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

Článok VII.
Spoločné ustanovenia

1. Dodávateľ je povinný spracovávať informácie, o ktorých má vedomosť, že by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
2. Dodávateľ je povinný mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto zmluvy, v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
3. Dodávateľ je povinný viesť evidenciu incidentov a logov a na žiadosť Prevádzkovateľa mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
4. V prípade, ak Dodávateľ plní základný kontrakt pre Prevádzkovateľa úplne alebo čiastočne prostredníctvom svojich Subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich Subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať kontrolné činnosti a audit v súlade s ustanoveniami čl. IX. tejto zmluvy aj u takýchto Subdodávateľov, zabezpečujúcich úplne alebo čiastočne plnenie základného kontraktu pre Prevádzkovateľa namiesto Dodávateľa.

Článok VIII.
Trvanie a zánik zmluvy, sankčný mechanizmus

1. Táto zmluva sa uzatvára na dobu určitú, odo dňa jej uzatvorenia do konca trvania základného kontraktu.
2. Zmluvný vzťah na základe tejto zmluvy zanikne súčasne so zánikom základného kontraktu.
3. Túto zmluvu je možné ukončiť vždy dohodou zmluvných strán o skončení trvania zmluvy, a to ku dňu uvedenému v takej dohode.
4. Prevádzkovateľ je oprávnený od tejto zmluvy písomne odstúpiť v prípadoch, ak Dodávateľ porušuje svoje povinnosti vyplývajúce z tejto zmluvy a nápravu neuskutoční ani do 5 pracovných dní odo dňa, kedy obdržal od Prevádzkovateľa písomnú výzvu na nápravu. Možnosť ktorejkoľvek zmluvnej strany odstúpiť od tejto zmluvy zo zákonom ustanovených dôvodov týmto nie je dotknutá.
5. Zánik tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do jej zániku.
6. V prípade každého jednotlivého porušenia ktorejkoľvek povinnosti Dodávateľa, vyplývajúcej z tejto zmluvy, ktorú Dodávateľ neodstráni ani do 5 pracovných dní odo dňa, kedy obdržal od Prevádzkovateľa písomnú výzvu na nápravu, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 500,-EUR (slovami: päťsto Eur).
7. V prípade opakovaného porušenia identickej povinnosti Dodávateľa, vyplývajúcej z tejto zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 1 000,-EUR (slovami: tisíc Eur).
8. Zmluvná pokuta je splatná na základe výzvy Prevádzkovateľa na zaplatenie zmluvnej pokuty v lehote 14 dní odo dňa jej doručenia Dodávateľovi.

9. Nárok Prevádzkovateľa na náhradu škody voči Dodávateľovi, aj vo výške presahujúcej zmluvnú pokutu, nie je ustanoveniami o dojednaní zmluvnej pokuty, uplatnením zmluvnej pokuty voči Dodávateľovi ani jej zaplatením Dodávateľom dotknutý.
10. Ak vznikne Prevádzkovateľovi ujma z dôvodu výlučného pochybenia Dodávateľa, ktorý poruší svoje povinnosti v oblasti kybernetickej bezpečnosti dojednané touto zmluvou alebo uložené mu právnymi predpismi, a to tak, že Prevádzkovateľ bude na základe alebo v súvislosti s takou skutočnosťou právoplatným rozhodnutím určený, ako zodpovedná osoba za správny delikt v oblasti kybernetickej bezpečnosti alebo ochrany osobných údajov, vzniká Prevádzkovateľovi nárok na náhradu takejto ujmy voči Dodávateľovi v plnom rozsahu, vrátane prípadných ďalších vynaložených nákladov, vrátane nákladov za právne zastúpenie. Obsah predchádzajúcej vety sa uplatní a teda nárok Prevádzkovateľa voči Dodávateľovi vzniká iba vtedy, ak Prevádzkovateľ včas a riadne písomne oznámi Dodávateľovi, že začalo takéto konanie voči nemu a ďalej, ak poskytne priestor Dodávateľovi na vyjadrenie sa ku konaniu a jeho vyjadrenie pripojí do konania.
11. Ktorákoľvek zmluvná strana môže aj bez udania dôvodov túto zmluvu vypovedať s dvojmesačnou výpovednou lehotou plynúcou dňom doručenia výpovede.
12. Zmluvné strany sa dohodli, že ak je kdekoľvek v zmluve dohodnutý nárok Prevádzkovateľa požadovať od Dodávateľa náhradu škody, ujmy, zmluvnej pokuty, nákladov a pod. (ďalej len „Škoda"), tak takéto finančné plnenie nesmie v súhrne presiahnuť sumu vo výške 5.000,-€/ za každý jednotlivý prípad/porušenie, pričom celková výška Škody za ktorú Dodávateľ zodpovedá na základe tejto Zmluvy nepresiahne sumu 10.000,-€ súhrnne.

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

1. Prevádzkovateľ je oprávnený vykonať u Dodávateľa audit zameraný výlučne na overenie plnenia povinností Dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, na overenie technického, technologického vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej j a technickej oblasti u Dodávateľa pre plnenie cieľov tejto zmluvy.
2. Prevádzkovateľ je oprávnený realizovať audit u Dodávateľa sám alebo prostredníctvom tretej osoby, ktorá bude odborne spôsobilá. Za odborne spôsobilú osobu sa považuje napríklad certifikovaný audítor kybernetickej bezpečnosti (v súlade s ust. § 29 ods. 3 zákona o kybernetickej bezpečnosti), certifikovaný interný audítor informačnej bezpečnosti podľa normy ISO:IEC 27001:2013, ale osoba ktoré je držiteľom medzinárodne uznávaných certifikátov CISA, CISM, CRISC, CISSP, ITIL a pod.
3. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
4. Prevádzkovateľ ním poverené odborne spôsobilá osoba (podľa bodu 2) je v rámci auditu oprávnený klásť otázky Dodávateľovi súvisiace s plnením tejto zmluvy.
5. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad plnenia povinností Dodávateľom s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy. .
6. Prevádzkovateľ je povinný písomne oznámiť Dodávateľovi svoj zámer realizovať u Dodávateľa audit najmenej sedem pracovných dní vopred.

7. Výsledok auditu Prevádzkovateľ zaznamená do zápisnice. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote určenej Prevádzkovateľom, ktorá musí byť primeraná.
8. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy.
9. Prevádzkovateľ a ním poverená odborne spôsobilá osoba vykonávajúca audit sú povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu u Dodávateľa a ktoré nie sú verejne známe. Prevádzkovateľ je povinný zabezpečiť zachovávanie mlčanlivosti v tomto zmysle každou osobou zúčastnenou na audite u Dodávateľa. Povinnosť zachovávať mlčanlivosť trvá aj po skončení trvania tejto zmluvy a/alebo základného kontraktu.
   Prevádzkovateľ a ním poverené osoby pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len **„BOZP"**) a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len **„PO"**), s ktorými musia byť Dodávateľom oboznámení v zmysle nasledujúcich ustanovení tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ.

Článok X.
Záverečné ustanovenia

1. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto zmluvy Prevádzkovateľovi udelí, poskytne, prevedie alebo na Prevádzkovateľa postúpi všetky potrebné práva, heslá alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu s Prevádzkovateľom založeného touto zmluvou po dobu dohodnutú v trvaní päť rokov po ukončení zmluvného vzťahu.
2. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto zmluvy Prevádzkovateľovi vráti, prevedie a podľa pokynov Prevádzkovateľa prípadne aj zničí všetky informácie, ku ktorým mal Dodávateľ počas trvania zmluvného vzťahu prístup k Prevádzkovateľovi.
3. Pre prípad porušenia zmluvných povinností uvedených v bode 1. a 2. tejto zmluvy má Prevádzkovateľ nárok na zmluvnú pokutu vo výške 50,- EUR za každé porušenie povinností jednotlivo a za každý deň omeškania so splnením vyššie špecifikovaných povinností, a to až do ich úplného splnenia.
4. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto zmluvy a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na plnenie predmetu tejto zmluvy.
5. Dodávateľ bez predchádzajúceho písomného súhlasu Prevádzkovateľa nemá právo previesť práva a povinnosti vyplývajúce z tejto zmluvy na tretiu osobu.
6. Táto zmluva predstavuje úplnú dohodu zmluvných strán týkajúcu sa predmetu tejto zmluvy a nahrádza v celom rozsahu akékoľvek predchádzajúce dohody či návrhy uvádzané v korešpondencii či na rokovaniach, či už ústne alebo písomné, ku ktorým došlo pred uzatvorením tejto zmluvy a ktoré jej uzatvorením zanikajú.
7. Táto zmluva sa riadi právom Slovenskej republiky. Právne vzťahy neupravené touto zmluvou sa spravujú príslušnými ustanoveniami Obchodného zákonníka a ostatnými

všeobecne záväznými právnymi predpismi. Na riešenie sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.

8. Zmluva je vyhotovená v štyroch vyhotoveniach, ktoré majú povahu originálu, po dvoch vyhotoveniach pre každú zmluvnú stranu.
9. Akúkoľvek zmenu alebo doplnenie tejto zmluvy je možné vykonať výlučne formou písomných dodatkov podpísaných oboma zmluvnými stranami.
10. Táto zmluva je uzatvorená, vzniká a zaväzuje zmluvné strany okamihom, keď je podpísaná oboma zmluvnými stranami a súčasne zverejnená prihliadnuc na ustanovenia § 47a Občianskeho zákonníka.
11. Osoby konajúce za zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, prejav ich vôle je slobodný a vážny, určitý a zrozumiteľný a je plne v súlade s obsahom tejto zmluvy, zmluvná voľnosť zmluvných strán nie je obmedzená, zmluvu si pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom ju vlastnoručne podpísali.

V Miloslavove, dňa 18.1.2022 V Miloslavove, dňa 14.01.2022

[redacted]

Ing. Adrian Mikóczi, konateľ

za Dodávateľa

OBEC MILOSLAVOV

Milan Baďanský, starosta obce

za Prevádzkovateľa

Špecifikácia bezpečnostných opatrení v spoločnosti EMELIX, s.r.o.
ktoré spoločnosť ako dodávateľ prijme a bude udržiavania v rámci kybernetickej bezpečnosti

Dodávateľ sa zaväzuje prijať bezpečnostné opatrenia minimálne v rozsahu podľa § 20 ods. 3 písm. d), f), g), m), k) a p) zákona o kybernetickej bezpečnosti, a to v oblasti:

- riadenia prístupov,
- bezpečnosti pri prevádzke informačných systémov a sietí,
- hodnotenia zraniteľností a bezpečnostných aktualizácií,
- riešenia kybernetických bezpečnostných incidentov,
- zaznamenávania udalostí a monitorovania,
- auditu, riadenia súladu a kontrolných činností.

Dodávateľ môže uvedenú povinnosť preukázať výsledkom auditu, alebo platným certifikátom o implementovaní systému riadenia informačnej bezpečnosti podľa normy ISO:IEC 27001:2013