

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatvorená medzi

Názov: **Obec Trenčianska Turná**

Adresa: 913 21 Trenčianska Turná 86

IČO: 00312053

Štat. zástupca: Ing. Peter Mikula, starosta; tel. 032 65 852 05, email: starosta@trencianskaturna.sk

(ďalej len „Prevádzkovateľ“)

a

Názov: **SH systém, spol. s r. o.**

Adresa: Dlhé Hony 17, 911 01 Trenčín

IČO: 31442170

Zápis: Obchodný register Okresného súdu Trenčín, oddiel: Sro, vložka č. 352/R

Štat. zástupca: Ing. Juraj Hatala – konateľ, tel. +421 32 222 5100, email: shsystem@shsystem.sk

(ďalej len „Dodávateľ“)

(ďalej Prevádzkovateľ a Dodávateľ spoločne ako „Zmluvné strany“)

Článok I

Úvodné ustanovenia

1. Prevádzkovateľ je v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o kybernetickej bezpečnosti“) prevádzkovateľom základnej služby. Prevádzkovateľ je súčasne aj správcom informačných technológií verejnej správy podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o informačných technológiách vo verejnej správe“).
2. Prevádzkovateľ základnej služby je podľa § 19 zákona o kybernetickej bezpečnosti povinný uzatvoriť s dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „Zmluva“).
3. Zmluva stanovuje základné úlohy a princípy spolupráce Zmluvných strán, s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Prevádzkovateľa a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany Prevádzkovateľa.
4. Zmluvné strany uzatvárajú túto Zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na zmluvný vzťah založený zmluvou, objednávkou alebo iným právny úkonom uzavretým medzi Dodávateľom a Prevádzkovateľom (ďalej len „Prevádzková zmluva“).

5. Pre účely tejto zmluvy sa za kybernetický incident považuje kybernetický bezpečnostný incident podľa zákona o kybernetickej bezpečnosti, t. j. akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:
- a) strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému;
 - b) obmedzenie alebo odmietnutie dostupnosti základnej služby;
 - c) vysoká pravdepodobnosť kompromitácie činností základnej služby;
 - d) ohrozenie bezpečnosti informácií.
6. Dodávateľ prehlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tejto Zmluvy.
7. V prípade vzniku nákladov na strane Dodávateľa v súvislosti s plnením povinností podľa tejto Zmluvy (čl. IV a čl. V) ako aj zákona o kybernetickej bezpečnosti, tieto náklady znáša Dodávateľ.

Článok II

Vymedzenie základných pojmov

Na účely tejto zmluvy sa rozumie

- a) sieťou elektronická komunikačná sieť ktorú tvoria prenosové systémy, ktoré môžu, ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej správe kapacity, prípadne prepájacie alebo smerovacie zariadenia a iné prostriedky, vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými vlnami, optickými alebo inými elektromagnetickými prostriedkami vrátane družicových sietí, pevných sietí s prepájaním okruhových a s prepájaním paketov vrátane internetu, mobilných sietí, elektrických vedení určených na prenos a distribúciu elektriny v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na druh prenášaných informácií;
- b) informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov;
- c) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi;
- d) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni;
- e) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom;
- f) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná;
- g) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené;
- h) kybernetickou bezpečnosťou 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;

- i) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami;
- j) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť;
- k) kybernetickým bezpečnostným incidentom 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
 - 1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému;
 - 2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby;
 - 3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby, alebo
 - 4. ohrozenie bezpečnosti informácií;
- l) základnou službou služba, ktorá je zaradená v zozname základných služieb a
 - 1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, alebo
 - 2. je prvkom kritickej infraštruktúry, pričom prvkom kritickej infraštruktúry najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia;
- m) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena l);
- n) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov;
- o) bezpečnostnými opatreniami sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Článok III

Predmet zmluvy

- 1. Predmetom tejto Zmluvy je určenie práv, povinností a záväzkov Zmluvných strán pri plnení bezpečnostných opatrení a notifikačných opatrení realizovaných v nadväznosti na Prevádzkovú zmluvu.
- 2. Miestom plnenia tejto Zmluvy sú najmä pracovisko alebo sídlo Prevádzkovateľa, pracovisko alebo sídlo Dodávateľa, alebo pracoviská a sídla subdodávateľov. V prípade zmeny alebo doplnenia sídla alebo pracoviska zo strany Zmluvných strán, vykonajú tak Zmluvné strany oznamom, zaslaným e-mailom na kontaktné osoby uvedené v článku VI tejto Zmluvy, najneskôr do 30 dní od vykonania tejto zmeny.

3. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu nadobudnutia účinnosti tejto Zmluvy až do skončenia platnosti Prevádzkovej zmluvy, pokiaľ z právnych predpisov nevyplývajú určité ďalšie povinnosti pre Dodávateľa aj po skončení platnosti Prevádzkovej zmluvy.

Článok IV

Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje dodržiavať bezpečnostnú politiku Prevádzkovateľa v rozsahu, v akom súvisí s prevádzkovaním základnej služby Prevádzkovateľa a v akom ju je možné aplikovať na poskytované služby v zmysle Prevádzkovej zmluvy. Prevádzkovateľ sa zaväzuje predložiť Dodávateľovi bezpečnostnú politiku do 5 kalendárnych dní odo dňa nadobudnutia účinnosti zmluvy. V prípade zmeny alebo dopĺňania bezpečnostnej politiky sa Prevádzkovateľ zaväzuje Dodávateľa bezodkladne informovať o ich obsahu a rozsahu, najneskôr však do 5 kalendárnych dní odo dňa prijatia zmien alebo doplnkov.
2. Dodávateľ berie na vedomie, že bezpečnostná politika Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám, týkajúcim sa prevádzky sietí a informačných systémov Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne potvrdí, že sa oboznámil s aktualizovanou bezpečnostnou politikou.
3. Dodávateľ sa zaväzuje chrániť všetky informácie, súvisiace s prevádzkovaním základnej služby poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.
4. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek kladených na Prevádzkovateľa podľa zákona o kybernetickej bezpečnosti alebo Vyhlášky NBÚ, a to zaslaním e-mailu na kontaktnú osobu Prevádzkovateľa uvedenú v tejto Zmluve.
5. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve.
6. Dodávateľ je ďalej povinný :
 - a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa;
 - b) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa („incidenty“);
 - c) zasielať Prevádzkovateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak;
 - d) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa;
 - e) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Prevádzkovej zmluvy a tejto Zmluvy alebo budú mať prístup k informáciám Prevádzkovateľa;
 - f) v prípade vzniku kybernetických incidentov systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch;

- g) po skončení tejto Zmluvy vrátiť, previesť, príp. zničiť všetky informácie, ku ktorým má Dodávateľ počas trvania zmluvy s Prevádzkovateľom prístup;
 - h) okrem už uvedeného prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, 10, 11, 12, 13, 14 a 15 vyhlášky NBÚ v rozsahu špecifikovanom v bezpečnostnej politike Prevádzkovateľa.
7. Dodávateľ môže zapojiť do poskytovania služieb na základe Prevádzkovej zmluvy ďalšieho dodávateľa, ak mu to vyplýva z ustanovení Prevádzkovej zmluvy.
 8. Dodávateľ je povinný informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia, realizované Dodávateľom na účely plnenia tejto Zmluvy, a to zaslaním emailu na kontaktnú osobu Prevádzkovateľa.
 9. Dodávateľ je povinný počas trvania Zmluvy mať a udržiavať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie účelu Zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti tak, aby bol naplnený účel Zmluvy.
 10. Dodávateľ je povinný najneskôr do 5 pracovných dní odo dňa nadobudnutia účinnosti Zmluvy doručiť Prevádzkovateľovi zoznam svojich zamestnancov s označením ich pracovnej funkcie, ktorí sa budú podieľať na jej plnení a/alebo budú mať prístup k informáciám Prevádzkovateľa.
 11. Dodávateľ je tiež povinný do 5 pracovných dní odo dňa nadobudnutia účinnosti Zmluvy doručiť Prevádzkovateľovi zoznam svojich subdodávateľov, ktorí sa budú podieľať na plnení Zmluvy a/alebo budú mať prístup k informáciám Prevádzkovateľa, ako aj oznámiť prevádzkovateľovi každú zmenu v tomto zozname, a to elektronickou formou na emailovú adresu kontaktnej osoby Prevádzkovateľa, uvedenú v článku VII tejto Zmluvy.

Článok V

Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident v rozsahu, v ktorom sa týka služieb poskytovaných Prevádzkovateľovi, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov v zmysle bezpečnostnej politiky Prevádzkovateľa.
2. Ak v čase hlásenia incidentu stále trvajú prejavy incidentu, Dodávateľ odošle Prevádzkovateľovi neúplné hlásenie aj s informáciou, že ide o neúplné hlásenie. Dodávateľ neúplné hlásenie bezodkladne doplní po obnove riadnej prevádzky siete a všetkých informačných systémov Prevádzkovateľa.
3. Dodávateľ je povinný riešiť kybernetický incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení kybernetického incidentu na mieste, reakciou na kybernetický incident a podporou reakcií na kybernetický incident (ďalej len „reaktívne opatrenia“).
4. Pri riešení kybernetických incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa spolupracovať s Prevádzkovateľom, Národným bezpečnostným úradom SR a inými príslušnými orgánmi 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.

5. Dodávateľ je povinný v čase kybernetického incidentu zabezpečiť dôkaz alebo dôkazný prostriedok o bezpečnostnom incidente tak, aby tento mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi, v zmysle bezpečnostnej politiky Prevádzkovateľa.
6. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie reaktívnych opatrení na riešenie kybernetického incidentu a ich výsledok.
7. Po vyriešení kybernetického incidentu je dodávateľ na výzvu Prevádzkovateľa v určenej lehote povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu v rozsahu, v ktorom sa kybernetický incident týkal služieb poskytovaných Prevádzkovateľovi Dodávateľom (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 návrhu nových ochranných opatrení.
8. Po schválení ochranných opatrení Prevádzkovateľom je dodávateľ povinný ochranné opatrenia bez zbytočného odkladu vykonať, po ich vykonaní preveriť ich účinnosť a výsledok oznámiť Prevádzkovateľovi.

Článok VI

Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, súvisiacich s prevádzkovaním základnej služby, o ktorých sa dozvie v súvislosti s plnením úloh podľa tejto Zmluvy, najmä nevyužiť ani nesprístupniť tretím osobám žiadne skutočnosti, informácie, poznatky, podklady alebo iné záležitosti, o ktorých bol počas platnosti tejto Zmluvy informovaný alebo o ktorých sa dozvedel počas plnenia tejto Zmluvy a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po zániku tejto Zmluvy alebo Prevádzkovej zmluvy bez časového obmedzenia.
2. Dodávateľ je povinný písomne zaviazat všetky osoby, svojich zamestnancov, subdodávateľov a ich zamestnancov, ktoré sú zúčastnené na plnení tejto Zmluvy, zachovávať mlčanlivosť v zmysle článku VI. ods. 1. tejto Zmluvy. Dodávateľ v plnej miere zodpovedá za dodržiavanie záväzku mlčanlivosti týmito osobami aj po zániku Zmluvy alebo Prevádzkovej zmluvy, t. j. aj po zániku ich pracovnoprávného alebo obdobného vzťahu.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.
4. Dodávateľ je povinný chrániť všetky informácie, súvisiace s prevádzkovaním základnej služby, ktoré mu boli poskytnuté Prevádzkovateľom, a to najmä pred ich neoprávneným vymazaním, zmenou alebo pred ich poskytnutím neoprávnenej osobe.

Článok VII

Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s Prevádzkovateľom e-mailom na kontaktné údaje zmluvných strán alebo iným vhodným spôsobom, pričom vo všetkých prípadoch musí byť prenos informácií uskutočnený za podmienok umožňujúcich chránený prenos informácií.
2. Prevádzkovateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti: _____, manažér kybernetickej bezpečnosti, tel. _____, e-mail: _____.

3. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti: , konateľ spoločnosti, tel.: e-mail:.
4. Kontaktné osoby podľa odsekov 2 alebo 3 tohto článku môže príslušná Zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej Zmluvnej strane v písomnej forme.

Článok VIII

Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený kedykoľvek vykonať u Dodávateľa audit, zameraný na overenie plnenia povinností dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov, na základe zákona o kybernetickej bezpečnosti a tejto Zmluvy.
2. Prevádzkovateľ môže audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu realizuje Prevádzkovateľom poverená tretia osoba.
3. Prípadné nedostatky zistené auditom, je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
4. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
5. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi 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 a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
6. Prevádzkovateľ je povinný oznámiť Dodávateľovi najmenej tri pracovné dni vopred svoj zámer vykonať u Dodávateľa audit.
7. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje Dodávateľa zodpovednosti za plnenie jeho povinností vyplývajúcich z tejto Zmluvy.
8. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
9. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.
10. Prevádzkovateľ 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 „BOZP“) a ochrany pred požiarom na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdoľadanie požiarov (ďalej len „PO“), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu, zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne

informovať zamestnancov Prevádzkovateľa 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.

11. Náklady, ktoré vzniknú Prevádzkovateľovi v súvislosti s výkonom auditu znáša v plnej výške Prevádzkovateľ.

Článok IX

Zodpovednosť

1. Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto Zmluvy môže spôsobiť Prevádzkovateľovi škody, pričom v prípade škôd ako dôsledkov incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Dodávateľa podľa tejto Zmluvy neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá Prevádzkovateľovi maximálne do výšky 3-násobku priemernej mesačnej platby za posledných 12 mesiacov za služby podľa Prevádzkovej zmluvy.

Článok X

Záverečné ustanovenia

1. Táto zmluva sa uzatvára na dobu určitú, na dobu trvania Prevádzkovej zmluvy podľa čl. 1 ods. 4 tejto Zmluvy.
2. Zmluvu je možné ukončiť:
 - a) písomnou dohodou zmluvných strán;
 - b) výpoveďou ktorejkoľvek zmluvnej strany, pričom výpovedná lehota je rovnaká ako je stanovené v Prevádzkovej zmluve a začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane;
 - c) odstúpením od zmluvy. Od zmluvy môže odstúpiť ktorákoľvek zo zmluvných strán v prípade podstatného porušenia zmluvy druhou zmluvnou stranou. Podstatným porušením zmluvy je porušenie ustanovení článku V tejto Zmluvy. Odstúpenie od zmluvy je účinné okamihom doručenia písomného odstúpenia druhej zmluvnej strane, príp. odmietnutím prevziať odstúpenie od tejto Zmluvy.
 - d) Ukončenie tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po ukončení tejto Zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy, ku ktorému dôjde do ukončenia tejto Zmluvy.
3. S ohľadom na § 8 ods. 2 písm. p.) Vyhlášky NBÚ, po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa všetky licencie, práva alebo súhlasy, potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto Zmluvy.
4. Táto Zmluva sa môže meniť iba dohodou Zmluvných strán v písomnej forme.
5. Ak by sa dôvod neplatnosti vzťahoval len na časť tejto Zmluvy, bude neplatnou len táto časť.
6. Táto Zmluva tvorí úplnú dohodu medzi Zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto Zmluvy zanikajú všetky predchádzajúce písomné a ústne zmluvy, súvisiace

s predmetom tejto Zmluvy a žiadna zo Zmluvných strán sa nemôže dovolávať zvláštnych, v tejto Zmluve neuvedených, ústnych dojednaní a dohôd.

7. Táto Zmluva bola vyhotovená v troch rovnopisoch, dvoch vyhotoveniach pre Prevádzkovateľa, jedného pre Dodávateľa.
8. V prípade, ak právne predpisy prikazujú Prevádzkovateľovi povinné zverejňovanie zmlúv v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov v spojení s § 47a Občianskeho zákonníka č. 40/1964 Zb. a táto Zmluva nespadá pod niektorú z výnimiek uvedených v právnych predpisoch, nadobúda platnosť dňom podpisu oboma Zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia, v ostatných prípadoch je Zmluva účinná dňom jej podpisu.
9. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

V dňa

V dňa

Za Prevádzkovateľa:

Za Dodávateľa:

Ing. Peter Mikula, starosta
Obec Trenčianska Turná

Ing. Juraj Hatala, konateľ
SH systém, spol. s r. o.