Servisná zmluva č. 26/23/Rk/S

TÁTO SERVISNÁ ZMLUVA (ĎALEJ LEN „ZMLUVA") BOLA UZATVORENÁ V ZMYSLE USTANOVENÍ §269 A NASL. OBCHODNÉHO ZÁKONNÍKA Č.513/1991 ZB. V ZNENÍ NESKORŠÍCH PREDPISOV, NIŽŠIE UVEDENÉHO DŇA, MESIACA A ROKA, MEDZI TÝMITO ZMLUVNÝMI STRANAMI:

Obchodné meno:	**Vodárenská spoločnosť Ružomberok, a. s.**
Sídlo:	Pri Váhu 6, Ružomberok 034 06
IČO:	36 672 271
DIČ:	2022239043
IČ DPH:	SK2022239043
Štatutárny zástupca:	Ing. Milan Mojš, prokurista
IBAN:	SK 60 5600 0000 0083 3928 0001
BIC:	KOMASK2X

Zapísaná v obchodnom registri Okresného súdu Žilina, oddiel: Sa, vložka č. 10545/L

(ďalej len „**Objednávateľ**" alebo „**Klient**")

Obchodné meno:	**Applied Technologies s. r. o.**
Sídlo:	Mostná 13, 949 01 Nitra
IČO:	47239824
DIČ:	2023544908
IČ DPH:	SK2023544908
Štatutárny zástupca:	Ing. Peter Šingliar, konateľ
IBAN:	SK40 1100 0000 0029 4900 4648
BIC:	TATRSKBX

Zapísaná v obchodnom registri Okr. súdu Nitra, odd. Sro, vl. č. 39365/N

(ďalej len „**Poskytovateľ**")

(Poskytovateľ a Objednávateľ spolu ďalej len „Zmluvné strany")

ZMLUVNÉ STRANY SA DOHODLI NA NASLEDUJÚCOM:

1. Predmet Zmluvy

1.1. Poskytovateľ sa zaväzuje v rozsahu a za podmienok ustanovených v tejto Zmluve poskytovať Objednávateľovi servisné Služby v oblasti informačných technológií (ďalej len „Služby" alebo „Mesačný paušál"), súvisiace so zabezpečením prevádzky a rozvoja serverovej a sieťovej a počítačovej infraštruktúry Objednávateľa (ďalej len „Infraštruktúra").

1.2. Technická špecifikácia Infraštruktúry je uvedená v Prílohe č. 1 tejto Zmluvy.

1.3. Popis Služieb a spôsob ich plnenia v rámci predmetu zmluvy je bližšie popísaný v Prílohe č. 2 tejto Zmluvy.

1.4. Záväzok Objednávateľa je za poskytnuté Služby riadne platiť Poskytovateľovi Odmenu, podľa článku 2 tejto Zmluvy.

1.5. Termín začatia plnenia zmluvy začína dňom: 01. 06. 2023.

2. Odmena, platobné a fakturačné podmienky

2.1. Objednávateľ sa zaväzuje zaplatiť Poskytovateľovi Odmenu za poskytovanie Služieb za každý kalendárny mesiac, na základe predloženej faktúry - daňového dokladu Poskytovateľa, vystaveného s náležitosťami podľa zákona o DPH č.222/2004 v znení neskorších predpisov.

2.2. Zmluvné strany sa dohodli na rozsahu a cenách za Služby, podľa Prílohy č. 3 a Prílohy č. 4 tejto Zmluvy.

2.3. Všetky ceny sú uvedené bez DPH, prípadne s DPH v sadzbe platnej ku dňu nadobudnutia platnosti zmluvy. Fakturovaná DPH z ceny predmetu Zmluvy sa riadi právnym predpisom upravujúcim sadzbu DPH platným v čase poskytnutia Služby.

2.4. Poskytovateľ vystaví a doručí Objednávateľovi faktúru, ktorej údaje budú zhodné s údajmi, uvedenými v tejto Zmluve. Podkladom faktúry bude výkaz vykonaných činností za príslušný mesiac odsúhlasený IT manažérom objednávateľa, v prípade jeho práceneschopnosti výkaz činností odsúhlasí jeho priamy nadriadený zamestnanec.

2.5. Poskytovateľ má právo doručiť daňový doklad – faktúru aj v elektronickej podobe, prostredníctvom e-mail-u.

2.6. Splatnosť faktúry je 30 dní odo dňa jej doručenia objednávateľovi.

3. Práva, povinnosti a sankcie

3.1. Poskytovateľ je povinný neodkladne a včas informovať Objednávateľa písomnou správou o všetkých jemu známych skutočnostiach, ktoré by mohli viesť k ohrozeniu normálneho fungovania Infraštruktúry.

3.2. Objednávateľ je povinný zabezpečiť a poskytnúť povereným osobám Poskytovateľa súčinnosť potrebnú na vyriešenie a odstránenie prípadného problému vzniknutého pri vykonávaní Služieb.

3.2.1. Zabezpečenie primeraného a bezpečného prístupu k Infraštruktúre, v rozsahu potrebnom k vykonávaniu Služieb, nie len počas pracovnej doby, ale aj mimo nej (mimo pracovnej doby najmä v prípade mimoriadnych udalostí; prípadne po vzájomnej dohode Zmluvných strán);

3.2.2. Zabezpečenie prístupových práv a vzdialeného prístup ku Infraštruktúre tak, aby zástupca Poskytovateľa mohol vykonávať Služby definované Zmluvou bez toho, aby pri práci vznikali prestoje na strane Objednávateľa alebo Poskytovateľa.

3.3. Objednávateľ môže požadovať plnenie Služieb počas jedného kalendárneho mesiaca aj nad rámec rozsahu hodín zahrnutých v mesačnom paušále, a to po vzájomnej dohode s Poskytovateľom a na základe podmienok čerpania Služieb nad rámec Mesačného paušálu uvedených v Prílohe č. 2.

3.3.1. Maximálny počet človekohodín čerpaných nad rámec mesačného paušálu počas jedného kalendárneho mesiaca je 100 človekohodín.

3.4. Poskytovateľ môže z vlastnej iniciatívy vykonať plnenie Služieb počas jedného kalendárneho mesiaca aj nad rámec rozsahu hodín zahrnutých v Mesačnom paušále na základe podmienok čerpania Služieb nad rámec Mesačného paušálu uvedených v Prílohe č. 2, ak:

3.4.1. sa jedná o odvrátenie mimoriadnej situácie za účelom ochrany Infraštruktúry Objednávateľa;

3.4.2. sa jedná o bezprostredné predchádzanie vzniku situácie s výrazne negatívnym vplyvom na infraštruktúru Objednávateľa;

3.4.3. Objednávateľ po predošlom návrhu takéto čerpanie odsúhlasil.

3.5. V prípade, že Poskytovateľ neposkytne zmluvne dohodnuté Služby, definované v Prílohe č. 2 Zmluvy, Objednávateľ má právo požiadať Poskytovateľa o vrátenie pomernej časti zaplatenej Odmeny za Služby, za mesiac, v ktorom Služby neboli poskytnuté. Objednávateľ má možnosť uplatniť svoje právo na sankciu podaním písomnej žiadosti Poskytovateľovi, najneskôr v mesiaci nasledujúcom po mesiaci, v ktorom mú Služby neboli riadne poskytnuté. Podanie žiadosti Objednávateľa na uplatnenie práva na sankciu, nemá odkladný účinok na zaplatenie Odmeny za poskytované Služby.

3.6. Poskytovateľ nebude v omeškaní, ak záväzok na plnenie predmetu tejto Zmluvy nemohol riadne a včas splniť pre okolnosti, ktoré po uzatvorení tejto Zmluvy vznikli v dôsledku ním nepredvídateľných a neodvrátiteľných skutočností mimoriadnej povahy (vyššia moc) alebo na žiadosť Objednávateľa. Poskytovateľ je povinný bez meškania informovať Objednávateľa o vzniku akejkoľvek prekážky, ktorá mú bráni alebo sťažuje v realizácii predmetu Zmluvy.

3.7. V prípade, že sa Objednávateľ oneskorí s platbou za Odmenu podľa stanov tejto Zmluvy o viac ako 14 dní, Poskytovateľ je oprávnený pozastaviť výkony vyplývajúce z tejto Zmluvy až do splnenia pohľadávky. Upozornenie o pozastavení výkonov Poskytovateľ odošle písomne Objednávateľovi najmenej 10 dní pred pozastavením týchto výkonov. Poskytovateľ v tomto prípade nepreberá žiadnu zodpovednosť za bezpečnosť prevádzky a akékoľvek škody, ktoré vzniknú Objednávateľovi alebo tretej osobe v dôsledku pozastavenia jeho výkonov.

4. Mlčanlivosť

4.1. Všetky skutočnosti obchodnej, ekonomickej alebo technickej povahy, súvisiace s Objednávateľom, ktoré nie sú bežne dostupné, a s ktorými príde Poskytovateľ do styku, sú obchodným tajomstvom. Poskytovateľ sa zaväzuje, že iným subjektom nevyzradí, nesprístupní, pre seba alebo iného nevyužije tieto skutočnosti. Všetky získané informácie takejto povahy udrží v prísnej tajnosti a obmedzí ich prezradenie iba tým zamestnancom, ktorí sú oprávnení v súvislosti s obsahom zmluvy, tieto informácie mať. V prípade porušenia obchodného tajomstva podľa § 51 Obchodného zákonníka, použije Objednávateľ právne prostriedky ochrany proti nekalej súťaži. Poskytovateľ sa zaväzuje dodržať právo na ochranu obchodného tajomstva po dobu platnosti tejto zmluvy a ďalšie tri roky po jej ukončení.

4.2. Všetky skutočnosti obchodnej, ekonomickej alebo technickej povahy, súvisiace s Poskytovateľom, ktoré nie sú bežne dostupné, a s ktorými príde Objednávateľ do styku, sú obchodným tajomstvom. Objednávateľ sa zaväzuje, že iným subjektom nevyzradí, nesprístupní, pre seba alebo iného nevyužije tieto skutočnosti. Všetky získané informácie takejto povahy udrží v prísnej tajnosti a obmedzí ich prezradenie iba tým zamestnancom, ktorí sú oprávnení v súvislosti s obsahom zmluvy, tieto informácie mať. V prípade porušenia obchodného tajomstva podľa § 51 Obchodného zákonníka, použije Poskytovateľ právne prostriedky ochrany proti nekalej súťaži. Objednávateľ sa zaväzuje dodržať právo na ochranu obchodného tajomstva po dobu platnosti tejto zmluvy a ďalšie tri roky po jej ukončení.

5. Ochrana osobných údajov

5.1. V prípade, ak dôjde k prístupu Zmluvnej strany k osobným údajom, týkajúcim sa druhej zmluvnej strany (ďalej len „osobné údaje"):

5.1.1. je táto Zmluvná strana povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku, tie nesmie využiť pre vlastné účely, ani pre účely tretích osôb a ich nesmie zverejniť, poskytnúť, ani sprístupniť žiadnym tretím osobám,

5.1.2. táto Zmluvná strana osobné údaje nesmie kopírovať, rozmnožovať, rozširovať, poskytovať, sprístupňovať, zverejňovať, ani ďalej akokoľvek spracúvať,

5.1.3. musí táto Zmluvná strana počas trvania zmluvy dodržiavať také opatrenia, aby nedošlo k strate, poškodeniu osobných údajov, ich úniku, prezradeniu, rozšíreniu, zneužitiu alebo inému neoprávnenému prístupu alebo neoprávnenej manipulácii s osobnými údajmi, a to aj nedbanlivostným konaním.

5.2. Povinnosť ochrany osobných údajov nie je časovo obmedzená a trvá aj po skončení trvania zmluvy, okrem prípadov, kedy poskytnutie, sprístupnenie alebo zverejnenie osobných údajov ustanovuje zákon alebo rozhodnutie súdu.

6. Ostatné ustanovenia

6.1. Poskytovateľ poskytne Služby týkajúce sa predmetu tejto zmluvy prednostne vlastným pracovníkom. Poskytovateľ si vyhradzuje právo rozhodovať podľa svojho uváženia o pridelení svojich zástupcov na poskytnutie jednotlivých Služieb Objednávateľovi. V prípadoch, keď je to podmienkou výrobcu, môžu niektoré Služby byť vykonávané autorizovaným pracovníkom výrobcu, so súhlasom Objednávateľa. Za plnenie týchto Služieb rovnako zodpovedá Poskytovateľ.

6.2. Zástupca Poskytovateľa poučí poverených pracovníkov Objednávateľa o tom, ktoré zásahy do Poskytovateľom spravovaných zariadení sú vyhradené pre zástupcu Poskytovateľa. Objednávateľ zabezpečí, aby jeho pracovníci rešpektovali tieto pokyny Poskytovateľa.

6.3. Všetky prípadné spory, ktoré vzniknú z tejto Zmluvy, vrátane sporov o jej platnosť, výklad alebo ukončenie, sú Zmluvné strany povinné prednostne riešiť vzájomnými zmierovacími rokovaniami a dohodami. V prípade, že sa vzájomné spory Zmluvných strán vzniknuté v súvislosti s plnením záväzkov podľa Zmluvy alebo v súvislosti s ňou nevyriešia, Zmluvné strany sa dohodli, že všetky spory budú riešené podľa právneho poriadku Slovenskej republiky.

6.4. Poskytovateľ sa zaväzuje neodkladne po uzavretí tejto zmluvy uzatvoriť s klientom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, ktorej účelom je zabezpečiť splnenie povinnosti klienta ako prevádzkovateľa základnej služby uzatvoriť pri uzatvorení zmluvy s poskytovateľom ako dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby zmluvu 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 počas celej doby platnosti tejto zmluvy.

7. Záverečné ustanovenia

7.1. Táto Zmluva sa uzatvára na dobu určitú, a to 48 mesiacov odo dňa nadobudnutia účinnosti zmluvy.

7.2. Táto Zmluva nadobúda platnosť dňom podpisu oboma Zmluvnými stranami (rozhodujúci je deň neskoršieho podpisu). Zmluva nadobúda účinnosť dňom nasledujúcom po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR.

7.3. Zmluvné strany sa dohodli, že výpoveď zmluvy možno uplatniť kedykoľvek, bez udania dôvodu, s 3-mesačnou výpovednou lehotou. Výpoveď začína plynúť 1. dňom kalendárneho mesiaca nasledujúceho po kalendárnom mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.

7.4. Túto Zmluvu je možné meniť alebo dopĺňať, iba písomnými dodatkami, odsúhlasenými oboma Zmluvnými stranami.

7.5. Ani jedna zo Zmluvných strán nie je oprávnená previesť práva a povinnosti zo Zmluvy, ako ani postúpiť pohľadávku vzniknutú zo Zmluvy na tretiu osobu, bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany.

7.6. Tato Zmluva je vyhotovená v dvoch exemplároch, po jednom exemplári pre každú Zmluvnú stranu.

7.7. Neoddeliteľnou súčasťou tejto zmluvy sú prílohy:

7.7.1. Technická špecifikácia Infraštruktúry

7.7.2. Popis Služieb a spôsob ich plnenia

7.7.3. Rozsah a cena Služieb v rámci mesačného paušálu

7.7.4. Cenník Služieb nad rámec mesačného paušálu

Za Objednávateľa:

V Ružomberku dňa 29.5.2023

Podpis, pečiatka:

VODÁRENSKÁ SPOLOČNOSŤ RUŽOMBEROK, a.s. Pri Váhu 1 034 06 RUŽOMBEROK

Ing. Milan Mojš

Prokurista, riaditeľ spoločnosti

Za Poskytovateľa:

V Ružomberku dňa 29.5.2023

Podpis, pečiatka:

Applied Technologies

Applied Technologies s. r. o.
Mostná 13, 949 01 Nitra
IČO: 47239824, DIČ: 2023544908
IČ DPH: SK2023544908

Ing. Peter Šingliar, konateľ

Príloha č. 1 – Technická špecifikácia Infraštruktúry

počet	položka
2ks	Server s príslušenstvom
1ks	Storage
2ks	Záložný zdroj UPS
<=5ks	Prvky sieťovej infraštruktúry
<=2ks	NAS
<=20ks	Virtuálny server
<=50 ks	Kancelársky počítač/notebook s OS Windows a s príslušenstvom

Servisná zmluva č. 26/23/Rk/S

Príloha č. 2 – Popis Služieb a spôsob ich plnenia

1. Poskytovateľ bude vykonávať tieto Služby pre Objednávateľa (ďalej aj „Klient"): vykonávanie nižšie uvedených služieb sa bude realizovať výhrade so súhlasom IT manažéra VSR, a.s. alebo riaditeľa spoločnosti

a) vykonávať funkciu pomocného správcu informačných technológií v objektoch a v priestoroch klienta, pričom je poskytovateľ povinný sa riadiť ustanoveniami internej smernice objednávateľa č. S-VSR-59 Smernica pre informačný systém. Smernica bude poskytovateľovi dostupná k nahliadnutiu v priestoroch objednávateľa.
b) odborné poradenstvo klientovi v oblasti informačných technológií a predkladať návrhy na zlepšenie stavu informačných technológií IT manažérovi klienta,
c) predkladať návrhy na odstránenie zistených nedostatkov na úseku informačných technológií u klienta,
d) na základe požiadavky klienta sa zúčastňovať pracovných porád u klienta,
e) údržba a servis počítačových sietí na pracoviskách klienta,
f) údržba a servis doménových serverov klienta, okrem upgrade operačných systémov, či migrácie týchto serverov na novšie verzie,
g) údržba existujúceho stavu serverovej infraštruktúry za podmienky zabezpečenia servisu od výrobcov hardvéru, softvéru – t.j.:
    a. zabezpečenie komunikácie s poskytovateľom servisu hardvéru a softvéru
    b. nie upgrade firmware servera a UPS, update/upgrade VMware, Veeam a OS na novšie verzie, či ich reinštalácie alebo rekonfigurácie
h) aktualizovanie OS, antivírových programov;
i) iné Služby súvisiace s informačnými technológiami na základe požiadavky klienta, po dohode s poskytovateľom

1. Poskytovateľ je povinný chrániť práva a oprávnené záujmy klienta, konať pri tom svedomito a v zmysle platných právnych predpisov.
2. Poskytovateľ sa zaväzuje poskytovať Služby v oblasti informačných technológií podľa potrieb klienta, najneskôr však do 4 hodín od výzvy, a to počas pracovných dní v čase od 8:00 do 16:00.
3. Služby je možné vykonávať na mieste, telefonicky, ako aj vzdialeným pripojením, ak to charakter činnosti umožňuje.
4. V prípade vyčerpania stanoveného mesačného paušálu sa ďalšie činnosti budú realizovať prednostne vzdialeným pripojením, ak to charakter činností umožňuje.
   a) Poskytovateľ zapíše vykonané činnosti do výkazu vykonaných činností s rozdelením na činnosti počas pracovnej doby Poskytovateľa a mimo pracovnej doby Poskytovateľa; pracovná doba Poskytovateľa je uvedená v Prílohe č.4.
   b) Poskytovateľ poskytne výkaz vykonaných činností na nahliadnutie Objednávateľovi na požiadanie bez zbytočného odkladu.
   c) Poskytovateľ do 5 pracovných dní po ukončení kalendárneho mesiaca vyzve Objednávateľom oprávnenú osobu podľa poradia v tabuľke Oprávnených osôb uvedenej v tejto prílohe na odsúhlasenie výkazu vykonaných činností, a tento bude tvoriť podklad pre fakturáciu za uplynutý kalendárny mesiac, a to výpočtom podľa počtu človekohodín a cenníkových cien za človekohodinu podľa Prílohy č.4.

5. Klient zabezpečí vytvorenie/prevzatie a odovzdanie prístupových údajov (vždy sa myslí administrátorský prístup) k infraštruktúre minimálne v rozsahu (ak existuje dané zariadenie, systém alebo oblasť v rámci Infraštruktúry):
   a) Heslo lokálneho administrátora pre klientske PC
   b) Heslo sieťového administrátora (domain admin a podobne, ak existuje)
   c) Heslo pre prístup k sieťovým prvkom (router, switch, firewall, miktortik, iné sieťové prvky)
   d) Heslo pre prístup k sieťovým úložiskám (NAS, iné)

e) Heslo pre prístup k serverovej infraštruktúre:
   a. Heslo do ESXi (vSphere klient)
   b. Heslo do vCenter
   c. Heslo do iDRAC servera
   d. Heslo do sieťového rozhrania UPS
   e. Heslo do Veeam Backup
   f. Heslo k operačným systémom serverov
   g. Iné relevantné heslá
f) Heslá k správe aplikácií
   a. Veeam Endpoint Backup / Veeam Agent for Windows
   b. ESET alebo iný antivírus
   c. Iné klientske alebo bezpečnostné aplikácie
g) Prístupové údaje správcu k doménam (web stránka, webmail,...)
h) Prístupové údaje do e-mailovej schránky
i) Iné heslá, prístupové údaje – podľa okolností
j) Prístupové údaje do portálov dodávateľov (napr. ESET, Microsoft, VMware, Veeam, a iné)
k) Informácie o licenčných kľúčoch k PC a serverom, ktoré sa nachádzajú v listinnej podobe (Windows, Office a iné)

Poskytovateľ vykonáva Služby v pracovných dňoch (PON-PIA) v čase medzi 8-16h, formou :

- diaľkovej správy,
- telefonicky,
- fyzickou prítomnosťou na Mieste plnenia, definovanom touto Zmluvou.

Poskytovateľom oprávnene osoby – administrátori :

administrátor	**kontakt**
Ing. Peter Šingliar	**podpora@apptech.sk; +421 948 373 563**
Alternatívny kontakt: Ing. Martin Masár	it@apptech.sk; +421 948 598 062

Objednávateľom oprávnene osoby – administrátori, vedúci pracovníci, poverení pracovníci:

Kontaktná osoba	**kontakt**
Ing. Martin Pudiš – IT manažér, administrátor	**martin.pudis@vsr.sk; +421 918 897 425**
Alternatívny kontakt: Ing. Juraj Hasák	juraj.hasak@vsr.sk; +421 911 383 752

Príloha č. 3 – Rozsah a cena Služieb v rámci mesačného paušálu

Položka	Predmet	Cena za jednotku (bez DPH)	Počet	Cena spolu (bez DPH)	DPH (20%)	Cena spolu (s DPH)
1	servisné Služby v oblasti informačných technológií*	35,00 €	**16 hodín mesačne**	560,00 €	112,00 €	672,00 €
SPOLU				560,00 €	112,00 €	672,00 €

*Uvedený rozsah a cena Služieb sa týka obdobia jedného kalendárneho mesiaca.

Najmenšia časová jednotka poskytovania Služby je štvrťhodina, započítava sa každá začatá štvrťhodina.

Všetky ceny sú uvedené bez DPH, prípadne s DPH v sadzbe platnej ku dňu nadobudnutia platnosti zmluvy. Fakturovaná DPH z ceny predmetu Zmluvy sa riadi právnym predpisom upravujúcim sadzbu DPH platným v čase poskytnutia Služby.

Príloha č. 4 – Cenník Služieb

Platný od: 1. 12.2019

Služba	**Cena v Eur bez DPH/hod.**
Človekohodina (nad rámec predplatených Služieb) počas pracovnej doby Poskytovateľa	40,-
Človekohodina mimo pracovnej doby Poskytovateľa	55,-

Pracovná doba Poskytovateľa je 08:00 – 16:00 hod SEČ.

Najmenšia časová jednotka poskytovanej Služby je štvrťhodina, započítava sa každá začatá štvrťhodina.

Všetky ceny sú uvedené bez DPH. Fakturovaná DPH z ceny predmetu Zmluvy sa riadi právnym predpisom upravujúcim sadzbu DPH platným v čase poskytnutia Služby.

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov /ďalej aj len „**Zmluva**"/ medzi zmluvnými stranami

Prevádzkovateľ základnej služby:	**Vodárenská spoločnosť Ružomberok, a.s.**
Sídlo:	Pri Váhu 6, 034 06 Ružomberok
IČO:	36 672 271
Zapísaná:	v Obchodnom registri Okresného súdu Žilina, oddiel: Sa, vložka č.: 10545/L
Konajúca prostredníctvom:	Ing. Milan Mojš, prokurista
e-mail:	milan.mojs@vsr.sk

a

Dodávateľ:	**Applied Technologies s. r. o.**
Sídlo:	Mostná 13 949 01 Nitra
IČO:	47239824
Zapísaná:	v Obchodnom registri Okresného súdu Nitra, oddiel: Sro, vložka č. 39365/N
Konajúca prostredníctvom:	Ing. Peter Šingliar, konateľ
e-mail:	obchod@apptech.sk

/ďalej spolu aj len „**zmluvné strany**"/

Článok I.
Účel Zmluvy

1.1 Účelom tejto Zmluvy je zabezpečiť splnenie povinnosti prevádzkovateľa základnej služby uzatvoriť pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby zmluvu 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 /ďalej aj len „**zákon**"/ počas celej doby platnosti Zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby zo dňa 31.01.2019 /ďalej aj len „**zmluva o poskytnutí činností**"/.

Článok II.
Definícia pojmov

2.1. **Sieťou a informačným systémom** sa rozumie elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,

2.2. **Kybernetickým priestorom** sa rozumie 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,

2.3. **Kontinuitou** sa rozumie strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

2.4. **Dôvernosťou** sa rozumie záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

2.5. **Dostupnosťou** sa rozumie záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
2.6. **Integritou** sa rozumie záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
2.7. **Kybernetickou bezpečnosťou** sa rozumie 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,
2.8. **Rizikom** sa rozumie miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
2.9. **Hrozbou** sa rozumie každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
2.10. **Kybernetickým bezpečnostným incidentom** sa rozumie 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 alebo digitálnej služby,
   c. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
   d. ohrozenie bezpečnosti informácií.
2.11. **Základnou službou** sa rozumie služba, ktorá je zaradená v zozname základných služieb a
   a. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona,
   b. je informačným systémom verejnej správy v zmysle § 2 ods. 1 písm. b) zákona č. 275/2006 Z. z. v znení zákona č. 570/2009 Z. z. alebo
   c. je prvkom kritickej infraštruktúry v zmysle ust. § 2 písm. a) zákona č. 45/2011 Z. z.
2.12. **Prevádzkovateľom základnej služby** sa rozumie orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k) zákona.
2.13. **Riešením kybernetického bezpečnostného incidentu** všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov

Článok III.
Rozsah činnosti dodávateľa

3.1 Dodávateľ sa v súlade s čl. 2 Zmluvy o dielo č. 1/01/2019 zo dňa 31.01.2019 zaviazal vykonávať pre prevádzkovateľa základnej služby počas zmluvného obdobia pozáručný servis kompletného systému vodárenského dispečingu a vodárenských objektov objednávateľa a vykonávať profylaktické práce kompletného systému vodárenského dispečingu, ktorým sú monitorované a riadené vodárenské objekty prevádzkovateľa základnej služby.

Článok IV.
Povinnosť dodávateľa dodržiavať bezpečnostnú politiku prevádzkovateľa základnej služby a prijať bezpečnostné opatrenia

4.1 Dodávateľ sa zaväzuje dodržiavať platné bezpečnostné politiky prevádzkovateľa základnej služby, ktoré sú normatívne upravené v dokumentoch prevádzkovateľa základnej služby.
4.2 Dodávateľ vyhlasuje, že sa s bezpečnostnou politikou prevádzkovateľa základnej služby oboznámil a vyjadruje súhlas s bezpečnostnou politikou prevádzkovateľa základnej služby.

4.3 Dodávateľ je povinný a zaväzuje sa chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby.

4.4 Dodávateľ sa zaväzuje dodržiavať a prijať bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona, a to najneskôr v lehote do 6 mesiacov odo dňa podpisu tejto Zmluvy. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

4.5 Dodávateľ je povinný oboznámiť prevádzkovateľa základnej služby s prijatými bezpečnostnými opatreniami a umožniť prevádzkovateľovi základnej služby vykonať audit dodávateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení dodávateľom s bezpečnostnou politikou prevádzkovateľa základnej služby. V prípade, ak výsledkom auditu bude nesúlad dodávateľom prijatých bezpečnostných opatrení so zákonom alebo s bezpečnostnou politikou prevádzkovateľa základnej služby, je dodávateľ povinný najneskôr v lehote 30 pracovných dní odo dňa zistenia nesúladu zabezpečiť nápravu.

Článok V.
Špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma dodávateľ a vyjadrenie súhlasu s nimi

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

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

5.2 Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje dodávateľ nasledovné opatrenia:

a. Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom.
b. Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
c. Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
d. Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.
e. Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
f. Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
g. Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.

h. Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.
i. Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
j. Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
k. Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.
l. Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.
m. Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.
n. Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.
o. Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

5.3 Pre oblasť riadenia prístupov realizuje dodávateľ nasledovné opatrenia:
a. Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
b. Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
c. Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.
d. Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
e. Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
f. Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).
g. Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.

h. Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

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

a. Oboznámenie sa s postupmi prevádzkovateľa základnej služby pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči prevádzkovateľovi základnej služby.

b. Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb prevádzkovateľovi základnej služby.

c. Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.

d. Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetický bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; reviziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.

e. Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov prevádzkovateľa základnej služby.

f. Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s prevádzkovateľom základnej služby.

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

Článok VI.
Ďalšie povinnosti dodávateľa

6.1 Dodávateľ sa zaväzuje poskytnúť prevádzkovateľovi základnej služby zoznam pracovných rolí dodávateľa s uvedením identifikačných údajov osôb zastávajúcich niektorú z pracovných úloh v rozsahu (meno, priezvisko, kontakt), ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby.

6.2 Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny.

6.3 Dodávateľ sa zaväzuje zabezpečiť a odovzdať prevádzkovateľovi základnej služby písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby

zúčastnenej na predmete plnenia zmluvy o poskytnutí činností a tejto Zmluvy /ďalej aj len „**zúčastnená osoba**"/; ktoré bude zúčastnenou osobou osobne vlastnoručne podpísané; každá zúčastnená osoba je povinná zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa zákona dozvedela a ktoré nie sú verejne známe. Povinnosť zúčastnenej osoby zachovávať mlčanlivosť podľa tohto bodu tejto Zmluvy trvá aj po skončení právneho vzťahu medzi zúčastnenou osobou a dodávateľom; tým nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

Článok VII.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u dodávateľa

7.1 Prevádzkovateľ základnej služby je oprávnený vykonávať kontrolnú činnosť a audit u dodávateľa, a to v rozsahu a za účelom kontroly plnenia povinnosti dodávateľa v zmysle zákona a tejto Zmluvy.

7.2 Prevádzkovateľ základnej služby je oprávnený vykonať kontrolnú činnosť a audit u dodávateľa prostredníctvom osoby, ktorej identifikačné údaje je prevádzkovateľ základnej služby povinný dodávateľovi včas oznámiť.

7.3 Prevádzkovateľ základnej služby je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu pravidelne raz za kalendárny rok; v prípade podozrenia z porušenia tejto Zmluvy alebo zákona; v prípade nedodržania bezpečnostných opatrení a v prípade žiadosti dozorného orgánu podľa zákona.

7.4 Prevádzkovateľ základnej služby informuje o termíne vykonania auditu alebo kontroly dodávateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 dní pred vykonaním auditu alebo kontroly. Dodávateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 dní odo dňa zaslania oznámenia. Pokiaľ dodávateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.

7.5 Prevádzkovateľ základnej služby je oprávnený vykonávať audit u dodávateľa nasledovne, pričom zmluvné strany majú pri výkone kontrolných činností a auditu naslednové práva a povinnosti:

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

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

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

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

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

f. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi základnej služby súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich

zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.

g. Vykonanie alebo nevykonanie auditu prevádzkovateľom základnej služby nezbavuje dodávateľa zodpovednosti za plnenie povinností dodávateľa vyplývajúcich z tejto zmluvy.

h. Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.

i. Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

j. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov dodávateľa v rámci výkonu auditu musia dodržiavať pokyny dodávateľa týkajúce sa uvedených priestorov na úseku BOZP a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie 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 základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne dodávateľ. Dodávateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch dodávateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory dodávateľa.

7.6 Dodávateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť prevádzkovateľovi základnej služby na účely kontroly a auditu v zmysle ust. § 28 a 29 zákona.

7.7 Dodávateľ je povinný v lehote určenej prevádzkovateľom základnej služby prijať opatrenia na nápravu nedostatkov zistených auditom u prevádzkovateľa základnej služby a poskytnúť potrebnú súčinnosť prevádzkovateľovi základnej služby na ich odstránenie.

Článok VIII.
Podmienky a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa a podmienky a možnosti zapojenia subdodávateľa prostredníctvom dodávateľa.

8.1 Dodávateľ je povinný dodržiavať podmienky zapojenia nového dodávateľa do poskytovania služieb tak, ako sú upravené v tejto Zmluve.

8.2 Dodávateľ je povinný vopred informovať prevádzkovateľa základnej služby o zapojení nového dodávateľa, a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom emailu na kontakt uvedený v záhlaví tejto Zmluvy.

8.3 Dodávateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb prevádzkovateľovi základnej služby nového dodávateľa bez predchádzajúceho výslovného písomného súhlasu prevádzkovateľa základnej služby.

8.4 Ak dodávateľ zapojí do vykonávania činností spojených s poskytovaním služieb prevádzkovateľovi základnej služby nového dodávateľa, tomuto novému dodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Zmluve. Zodpovednosť voči prevádzkovateľovi základnej služby nesie dodávateľ, ak

nový dodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

Článok IX.
Povinnosť dodávateľa hlásiť kybernetický bezpečnostný incident a ďalšie informácie prevádzkovateľovi základnej služby vrátane povinností dodávateľa pri riešení kybernetického bezpečnostného incidentu

9.1 Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie tejto Zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

9.2 Dodávateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident v zmysle zákona a informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.

9.3 Dodávateľ je povinný bezodkladne informovať prevádzkovateľa základnej služby podľa bodu 9.2 tohto článku tejto Zmluvy hlásením kybernetického bezpečnostného incidentu prostredníctvom zaslania hlásenia na e-mailovú adresu uvedenú v záhlaví tejto Zmluvy v rozsahu nasledovných informácií:

a. informácie o tom, kto hlási kybernetický bezpečnostný incident:
   - identifikačné údaje dodávateľa,
   - funkcia a pracovné zaradenie osoby dodávateľa, ktorá hlási kybernetický bezpečnostný incident,
   - identifikačné údaje ďalších organizácií dotknutých kybernetickým bezpečnostným incidentom,

b. informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu:
   - kategória kybernetického bezpečnostného incidentu (bezpečnostný incident I. stupňa, bezpečnostný incident II. stupňa, bezpečnostný incident III. stupňa),
   - typ závažného kybernetického bezpečnostného incidentu
     - nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
     - škodlivý kód (vírus, malvér, ransomvér),
     - získavanie informácií (skenovanie site, odpočúvanie, sociálne inžinierstvo),
     - pokus o prienik do systému,
     - podozrenie na úspešný prienik do systému vrátane APT,
     - nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby),
     - neoprávnený prístup k informáciám, únik informácií, poškodenie informácií,
     - podvod (neautorizované využitie prostriedkov, porušenia autorských práv),
     - zraniteľnosť (ich existencia),
     - iné,
   - časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu
     - čas začiatku incidentu (ak je známy), čas a spôsob zistenia incidentu, informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,
   - detailný opis priebehu závažného kybernetického bezpečnostného incidentu a jeho prvotná príčina,
   - popis rozsahu škôd,
   - odhad závažnosti dopadu závažného kybernetického bezpečnostného incidentu na užívateľov základnej služby,

c. informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom:
   - prvotne zasiahnuté aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby,
   - informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity služby alebo činnosti, a či je zariadenie v čase podávania hlásenia v prevádzke.

d. informácie o riešení závažného kybernetického bezpečnostného incidentu,
   - stav riešenia závažného kybernetického bezpečnostného incidentu,
   - informácia o vykonaní nápravných opatrení smerujúcich k riešeniu hláseného závažného kybernetického bezpečnostného incidentu,
   - opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,
   - popis možných negatívnych dopadov, opatrení a možných dôsledkov závažného kybernetického bezpečnostného incidentu,
   - výsledok opatrení,
   - dátum a čas realizácie opatrení.

9.4 Dodávateľ je povinný hlásiť prevádzkovateľovi základnej služby ďalšie informácie požadované prevádzkovateľom základnej služby na plnenie jeho povinnosti vyplývajúcich zo zákona, najmä je povinný poskytnúť prevádzkovateľovi základnej služby

a. informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované prevádzkovateľom základnej služby alebo Národným bezpečnostným úradom a ústredným orgánom od prevádzkovateľa základnej služby za účelom splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm.c) zákona,

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

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

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

9.5 Prevádzkovateľ základnej služby je oprávnený požadovať od dodávateľa vykonanie reaktívneho opatrenia a dodávateľ je povinný vykonať reaktívne opatrenie v prípadoch, kedy bola prevádzkovateľovi základnej služby uložená povinnosť vykonať reaktívne opatrenie Národným bezpečnostným úradom v zmysle zákona.

9.6 Dodávateľ je povinný bezodkladne prevádzkovateľovi základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok a poskytnúť prevádzkovateľovi základnej služby všetku potrebnú súčinnosť pri splnení povinnosti prevádzkovateľa základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok pred Národným bezpečnostným úradom.

9.7 Prevádzkovateľ základnej služby je oprávnený požadovať od dodávateľa návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu, a to najmä v prípadoch, kedy Národný bezpečnostný úrad požaduje od prevádzkovateľa základnej služby návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu /ďalej aj len **„ochranné opatrenie"**/. Ochranné

opatrenie je prijímané na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

9.8 Dodávateľ je povinný bezodkladne prevádzkovateľovi základnej služby predložiť navrhované ochranné opatrenie na schválenie. Po schválení ochranného opatrenia Národným bezpečnostným úradom určí prevádzkovateľ základnej služby lehotu na vykonanie schváleného ochranného opatrenia.

9.9 V prípade, ak dodávateľ základnej služby nenavrhne ochranné opatrenie v lehote určenej prevádzkovateľom základnej služby alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný poskytnúť všetku potrebné súčinnosť prevádzkovateľovi základnej služby, ktorý je povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

Článok X.
Trvanie Zmluvy, podmienky a spôsob ukončenia Zmluvy

10.1 Zmluva sa uzatvára na dobu platnosti a účinnosti zmluvy o poskytnutí činností špecifikovanej v čl. III. tejto Zmluvy.

10.2 Zmluvné strany môžu túto Zmluvu ukončiť vždy písomnou dohodou zmluvných strán; Zmluva zaniká dňom dohodnutým v písomnom vyhotovení dohody o ukončení tejto Zmluvy, nikdy nie pred uplynutím účinnosti zmluvy o poskytnutí činností. V prípade, ak zmluvné strany dohodnú deň ukončenia Zmluvy pred dnom uplynutia účinnosti zmluvy o poskytnutí činností, táto Zmluva zaniká súčasne so zánikom účinnosti zmluvy o poskytnutí činností.

10.3 Prevádzkovateľ základnej služby je oprávnený písomne odstúpiť od tejto Zmluvy v prípade, ak dodávateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy.

10.4 Prevádzkovateľ základnej služby je oprávnený písomne vypovedať túto Zmluvu, ak

a. dodávateľ neodôvodnene odmietne výkon kontrolnej činnosti a auditu prevádzkovateľom základnej služby,
b. dodávateľ postúpi svoje práva a povinnosti na ďalšieho dodávateľa v rozpore s touto Zmluvou,
c. na majetok dodávateľa je vyhlásený konkurz, exekúcia, dodávateľ vstúpil do likvidácie, preruší, alebo iným spôsobom ukončí svoju podnikateľskú činnosť,
d. dodávateľ, alebo osoba oprávnená konať v jeho mene je právoplatne odsúdená za trestný čin spáchaný v súvislosti s výkonom jeho činnosti, alebo s podnikaním,
e. dodávateľ stratí predpoklady na plnenie tejto Znluvy.

Výpovedná lehota je jeden mesiac a začína plynúť prvého dňa mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.

10.5 Dodávateľ je povinný po ukončení Zmluvy vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup prevádzkovateľovi základnej služby.

10.6 Dodávateľ je povinný po ukončení Zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok dodávateľa ostáva v platnosti aj po ukončení Zmluvy po dobu 5 rokov.

Článok XI.
Sankcie, zmluvné pokuty a náhrada škody

11.1 V prípade, ak dodávateľ poruší svoje povinnosti v zmysle tejto Zmluvy voči prevádzkovateľovi základnej služby, a to najmä povinnosť

a. dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
b. dodržiavať a prijímať bezpečnostné opatrenia minimálne v rozsahu najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona,

c. prijať bezpečnostnú dokumentáciu, ktorá musí byť pravidelne aktualizovaná a zodpovedať reálnemu stavu,
d. oboznámiť prevádzkovateľa základnej služby s prijatými bezpečnostnými opatreniami a umožniť prevádzkovateľovi základnej služby vykonať audit dodávateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení dodávateľom s bezpečnostnou politikou prevádzkovateľa základnej služby,
e. najneskôr v lehote 30 pracovných dní odo dňa zistenia nesúladu dodávateľom prijatých bezpečnostných opatrení so zákonom alebo s bezpečnostnou politikou prevádzkovateľa základnej služby zabezpečiť nápravu,
f. oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny,
g. zabezpečiť a odovzdať prevádzkovateľovi základnej služby písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia; ktoré bude zúčastnenou osobou osobne vlastnoručne podpísané v zmysle bodu 6.3 tejto Zmluvy,
h. podľa článku IX. tejto Zmluvy,

vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 30.000,- EUR.

11.2 Prevádzkovateľ základnej služby je oprávnený uplatniť si zmluvné pokuty a náhradu škody kedykoľvek v priebehu plnenia predmetu Zmluvy, ako aj po zániku Zmluvy v prípade, ak porušenie zmluvných podmienok stanovených touto Zmluvou zistí po zániku zmluvného vzťahu vyplývajúceho zo Zmluvy.

11.3 V prípade, ak dodávateľ poruší svoje povinnosti podľa čl. X., ods. 10. 6 tejto Zmluvy, vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 100.000,- EUR.

11.4 Uplatnením ktorejkoľvek zmluvnej pokuty alebo zmluvných pokút v zmysle tohto článku nie je dotknutý nárok prevádzkovateľa základnej služby na náhradu vzniknutej škody v celom rozsahu a právo na uplatnenie ďalšej zmluvnej pokuty podľa tejto Zmluvy. Prevádzkovateľ môže uplatňovať náhradu škody a zmluvnej pokuty kumulatívne, prevádzkovateľ základnej služby má nárok na zaplatenie zmluvnej pokuty a súčasne náhrady škody v plnom rozsahu. Prevádzkovateľ základnej služby je oprávnený jednostranne započítať voči dodávateľovi svoje pohľadávky vzniknuté z titulu zmluvnej pokuty a/alebo náhrady škody uplatnenej podľa tejto Zmluvy.

Článok XII.
Záverečné ustanovenia

12.1 Táto Zmluva nadobúda platnosť dňom podpisu obidvoma zmluvnými stranami a účinnosť dňom nasledujúcom po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády SR.

12.2 Táto Zmluva sa vyhotovuje v dvoch rovnopisoch, 1 x pre prevádzkovateľa základnej služby a 1 x pre dodávateľa. Akékoľvek dodatky a zmeny tejto Zmluvy sú platné len v písomnej forme, po ich odsúhlasení a podpísaní oboma zmluvnými stranami.

12.3 V prípade, že sa niektoré z ustanovení tejto Zmluvy stane neplatným, zmluvné strany sa zaväzujú nahradiť neplatné ustanovenie ustanovením platným tak, aby zodpovedalo účelu tejto Zmluvy a najmä vôli zmluvných strán pri uzatváraní tejto Zmluvy. Zostávajúce ustanovenia Zmluvy sú takouto zmenou nedotknuté.

12.4 Táto Zmluva sa riadi právnym poriadkom Slovenskej republiky, najmä ustanoveniami zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a vyhláškou č. 362/2018 Z.z. Národného bezpečnostného úradu z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

12.5 Práva a povinnosti zmluvných strán neupravené v tejto Zmluve sa riadia zmluvou o poskytnutí činnosti špecifikovanej v čl. III tejto Zmluvy, vyhláškou NBÚ, alebo inými právnymi predpismi vydanými v súlade so zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti a zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti.

12.6 Zmluvné strany vyhlasujú, že ich zmluvná voľnosť nebola žiadnym spôsobom obmedzená.

12.7 Zmluvné strany vyhlasujú, že táto Zmluva nebola uzavretá v tiesni ani za nápadne nevýhodných podmienok a ani v omyle.

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

V Ružomberku dňa 29.5.2023

VODÁRENSKÁ SPOLOČNOSŤ
RUŽOMBEROK, a.s.
Pri Váhu 6
03406 RUŽOMBEROK

Vodárenská spoločnosť Ružomberok, a.s.
Ing. Milan Mojš
prokurista

V Ružomberku dňa 29.5.2023

Applied Technologies
Applied Technologies s. r. o.
ná 13, 949 01 Nitra
DIČ: 2023544908

Applied Technologies s. r. o.
Ing. Peter Šingliar
konateľ