Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 35343/2025

(ďalej aj len **„Zmluva“**)
v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti
a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
medzi zmluvnými stranami

Objednávateľ:	**Západoslovenská vodárenská spoločnosť, a.s.**
(ďalej aj ako Prevádzkovateľ základnej služby)	
Sídlo:	Nábrežie za hydrocentrálou 4, 949 60 Nitra
Zápis v Obchodnom registri:	OS Nitra, Oddiel: Sro, vl. č.: 10193/N
Konajúci:	PhDr. Mgr. art. Otokar Klein, ArtD. predseda predstavenstva; Ing. Marek Illéš člen predstavenstva
BIC:	SUBASKBX
IBAN:	SK66 0200 0000 0000 0260 3112
IČO:	36550949
DIČ:	2020154609
IČ DPH:	SK2020154609
Kontaktná osoba:	
Kontaktný mail pre hlásenie incidentu: kybermanager@zsvs.sk	

a

Poskytovateľ:	**FINECA TAX OFFICE s.r.o.**
Sídlo:	**Šúdolská 68E, 949 11 Nitra**
Zápis v Obchodnom registri:	v Obchodnom registri Okresného súdu Nitra, oddiel: Sro, vložka č.: 36299/N
IBAN:	SK14 7500 0000 0040 0447 2134
BIC kód:	CEKOSKBX
IČO:	47594870
DIČ:	2023965570
IČ DPH:	SK2023965570
Kontaktná osoba:	Ing. Miriam Buliková, PhD.
Zastúpený:	Ing. Miriam Buliková, PhD., konateľ

(ďalej spolu aj len „zmluvné strany“)

Preambula

1. Objednávateľ 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“) Prevádzkovateľom základnej služby typu: „Dodávatelia a distribútori vody na pitie, varenie, prípravu potravín alebo iné domáce účely, bez ohľadu na jej pôvod a na to, či bola dodaná z distribučnej siete, cisterny alebo vo fľašiach či nádobách; s výnimkou distribútorov, u ktorých je distribúcia vody iba časťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru, ktorá sa nepovažuje za základnú službu“ v sektore „Voda a atmosféra“, podsektor „Zabezpečovanie pitnej vody“.
2. Objednávateľ je ako Prevádzkovateľ základnej služby v zmysle Zákona, § 19, odstavec 2, povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných technológií Objednávateľa a ktorá je dodávaná treťou stranou – poskytovateľom zmluvnej činnosti, uzatvoriť s treťou stranou túto Zmluvu o zabezpečení plnenia

bezpečnostných opatrení, ktoré je tretia strana povinná u seba zabezpečiť a notifikačných povinností voči Objednávateľovi pri vzniku a riešení bezpečnostného incidentu.

Článok I.
Predmet Zmluvy

1. Predmetom tejto Zmluvy je záväzok Poskytovateľa zabezpečovať plnenie bezpečnostných opatrení a notifikačných povinností v zmysle Preambuly tejto Zmluvy vyplývajúci z uzavretia zmluvy s Objednávateľom:
   ZMLUVA O POSKYTOVANÍ SLUŽIEB v oblasti daňového poradenstva, uzatvorená dňa: 05 -06- 2025
   (ďalej len „ZoD").

Článok II.
Definícia pojmov

1. Pojmy používané v tejto Zmluve (sieť a informačný systém, kybernetický priestor, kontinuita, dôvernosť, dostupnosť, integrita, kybernetická bezpečnosť, riziko, hrozba, kybernetický bezpečnostný incident, základná služba, prevádzkovateľ základnej služby, riešenie kybernetického bezpečnostného incidentu) majú význam im priradený v Zákone a jeho vykonávacích predpisoch.
2. Zmluvná činnosť – vykonanie a odovzdanie diela, ktorú Poskytovateľ realizuje na základe ZoD.

Článok III.
Obdobie trvania Zmluvy

1. Zmluva sa uzatvára na dobu určitú – na dobu platnosti a účinnosti ZoD.

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

1. Poskytovateľ sa pri realizácii zmluvnej činnosti vyplývajúcej zo ZoD zaväzuje dodržiavať platné bezpečnostné politiky Prevádzkovateľa základnej služby, ktoré sú pre Poskytovateľa ako Tretiu stranu v zmysle Zákona, normatívne upravené v dokumentoch Prevádzkovateľa základnej služby a sú prílohami k tejto Zmluve.
2. Poskytovateľ vyhlasuje, že sa s bezpečnostnou politikou Prevádzkovateľa základnej služby oboznámil a podpisom tejto Zmluvy vyjadruje súhlas s bezpečnostnou politikou Prevádzkovateľa základnej služby.
3. Poskytovateľ je povinný a zaväzuje sa chrániť všetky informácie ktoré mu Prevádzkovateľ základnej služby poskytol.
4. Poskytovateľ sa zaväzuje vo vlastnej spoločnosti prijať a dodržiavať bezpečnostné opatrenia minimálne v rozsahu podľa Článku V tejto Zmluvy.

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

Poskytovateľ prijíma bezpečnostné opatrenia vo vlastnej spoločnosti v nasledujúcich oblastiach:

1. Oblasť odhaľovania technických zraniteľností informačných systémov a zariadení, ktoré Poskytovateľ využíva pri poskytovaní služieb – Zmluvnej činnosti - Prevádzkovateľovi základnej služby. Cieľom opatrenia je odhaliť zraniteľnosť informačných systémov a zariadení skôr, než bude zneužitá a prerastie do incidentu. Opatrenie Poskytovateľ realizuje pomocou:
   a. Zavedením a prevádzkou nástrojov určených na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí a technických prostriedkov a ich častí.
   b. Využitím verejných a výrobcami poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2. Oblasť riadenia bezpečnosti sietí a informačných systémov. Cieľom opatrenia je zabrániť útočníkovi prístup k jednotlivým sieťam a informačným systémom ako aj pohyb medzi nimi. Opatrenie Poskytovateľ realizuje pomocou:
    a. Dôslednou segmentáciou a mikrosegmentáciou sietí a informačných systémov.
    b. Riadením prístupu a komunikácie medzi segmentami na princípe zásady najnižších privilégií.
    c. Vo vzdialenom prístupe využívaním dvojfaktorovej autentizácie a/alebo použitím kryptografických prostriedkov.
    d. Využitím blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
    e. Vykonávaním kontroly na prítomnosť škodlivého kódu v zariadení, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia bezpečnosti pripájaného zariadenia, to je zaplatením zmluvnej pokuty pri preukázaní vzniku incidentu pripojením nebezpečného zariadenia. Pokuty sú uvedené v článku XII.
3. Oblasť riadenia prístupov. Cieľom opatrenia je jednoznačná identifikácia prístupu osôb k sieti a informačným systémom. Opatrenie Poskytovateľ realizuje pomocou:
    a. Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade najnižších privilégií. Používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie jemu zverených úloh používateľa alebo administrátora.
    b. Vypracovaných a používaných zásad 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.
    c. Monitorovaním prístupu a používania informačného systému a riadenia vzdialeného prístupu.
    d. Riadenie procesu prideľovania jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
    e. 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.
4. Oblasť riešenia kybernetických bezpečnostných incidentov. Cieľom je detegovať a riešiť kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na výkon činnosti pre Prevádzkovateľa základnej služby. Opatrenie Poskytovateľ realizuje pomocou:
    a. Oboznámením sa s postupmi, ktoré vyžaduje Prevádzkovateľ základnej služby pri riešení kybernetických bezpečnostných incidentov
    b. Monitorovania a analyzovania udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Prevádzkovateľovi základnej služby.
    c. Riešením zistených kybernetických bezpečnostných incidentov a znížením následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Prevádzkovateľa základnej služby.
    d. Vyhodnocovaním 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. Oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov. Cieľom je predchádzanie bezpečnostných incidentov a zlepšovanie bezpečnostných opatrení. Opatrenia Poskytovateľ realizuje podľa § 15 vyhlášky NBÚ č. 362/2018 Z. z., najmä implementovaním centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov a to minimálne pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb Prevádzkovateľovi základnej služby.

Článok VI.
Rozsah činnosti Poskytovateľa

1. Poskytovateľ bude realizovať zmluvné činnosti v rozsahu podľa:
   - Predmetu zmluvy uvedeného v ZoD,
   - Prílohy, ktoré sú súčasťou ZoD.

Článok VII.
Ďalšie povinnosti Poskytovateľa

1. Poskytovateľ sa zaväzuje poskytnúť Objednávateľovi zoznam pracovných rolí Poskytovateľa s uvedením identifikačných údajov osôb zastávajúcich niektorú z pracovných úloh pri plnení zmluvnej činnosti. Zoznam obsahuje: rola, meno, priezvisko, kontakt (telefón, mail), všetkých osôb, ktoré majú mať prístup do informačných a/alebo technologických infraštruktúr a/alebo k informáciám a údajom Objednávateľa.
2. Poskytovateľ je povinný oznámiť Objednávateľovi každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny.
3. Každá osoba Poskytovateľa zúčastnená na predmete plnenia, vlastnoručne podpisuje vyjadrenie o zachovaní mlčanlivosti podľa § 12 ods. 1 Zákona. Poskytovateľ sa zaväzuje zabezpečiť a odovzdať Objednávateľovi tieto písomné vyjadrenie o zachovávaní mlčanlivosti.

Článok VIII.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u Poskytovateľa

1. Objednávateľ je v zmysle Zákona oprávnený vykonávať kontrolnú činnosť a audit u Poskytovateľa.
2. Objednávateľ je oprávnený vykonať kontrolnú činnosť a audit u Poskytovateľa prostredníctvom osoby, ktorej identifikačné údaje je Objednávateľ povinný Poskytovateľovi včas oznámiť.
3. Objednávateľ 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.
4. Objednávateľ informuje o termíne vykonania auditu alebo kontroly Poskytovateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 dní pred vykonaním auditu alebo kontroly. Poskytovateľ 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 Poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.
5. Práva a povinnosti zmluvných strán pri realizácii auditu:
   a. Objednávateľ je oprávnený vykonať u Poskytovateľa audit zameraný na overenie plnenia povinností Poskytovateľa podľa tejto Zmluvy a efektívnosti ich plnenia.
   b. Prípadné nedostatky zistené auditom je Poskytovateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
   c. Objednávateľ môže audit u Poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Objednávateľa pri výkone auditu realizuje Objednávateľom poverená tretia osoba.
   d. Poskytovateľ 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 v rozsahu podľa tejto Zmluvy.
   e. Objednávateľ je v rámci auditu oprávnený klásť otázky zamestnancom Poskytovateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
   f. Vykonanie alebo nevykonanie auditu Objednávateľom nezbavuje Poskytovateľa zodpovednosti za plnenie povinností Poskytovateľa vyplývajúcich z tejto Zmluvy.
   g. Ak Poskytovateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
   h. Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

i. Objednávateľ a jeho zamestnanci pri návšteve priestorov Poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny Poskytovateľa 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 Poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Poskytovateľ 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 Poskytovateľa.

6. Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť Objednávateľovi na účely kontroly a auditu v zmysle ust. § 28 a 29 Zákona.

Článok IX.
Podmienky a možnosti zapojenia ďalšieho Poskytovateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto Poskytovateľa a podmienky a možnosti zapojenia subPoskytovateľa prostredníctvom Poskytovateľa.

1. Poskytovateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb Prevádzkovateľovi základnej služby nového Poskytovateľa bez predchádzajúceho výslovného písomného súhlasu Prevádzkovateľa základnej služby.
2. Ak Poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb Prevádzkovateľovi základnej služby nového Poskytovateľa, tomuto novému Poskytovateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Zmluve Poskytovateľovi. Zodpovednosť voči Prevádzkovateľovi základnej služby nesie Poskytovateľ, ak nový Poskytovateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

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

1. Poskytovateľ 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.
2. Poskytovateľ informuje Prevádzkovateľa základnej služby zaslaním hlásenia o kybernetickom bezpečnostnom incidentu na e-mailovú adresu uvedenú v záhlaví tejto Zmluvy.
3. Hlásenie musí obsahovať:
    a. informácie o tom, kto hlási kybernetický bezpečnostný incident:
        - identifikačné údaje Poskytovateľa,
        - funkcia a pracovné zaradenie osoby Poskytovateľa, ktorá hlási kybernetický bezpečnostný incident,
        - identifikačné údaje ďalších organizácií, ktoré boli ešte dotknuté kybernetickým bezpečnostným incidentom u Poskytovateľa,
    b. informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu:
        - typ závažného kybernetického bezpečnostného incidentu

- nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
- škodlivý kód (vírus, malvér, ransomvér),
- získavanie informácií (skenovanie siete, 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,

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.

4. Poskytovateľ je povinný hlásiť Prevádzkovateľovi základnej služby ďalšie informácie, ktoré Prevádzkovateľ základnej služby potrebuje na plnenie svojej povinností vyplývajúcich zo Zákona, najmä:
   a. informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
   b. 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,
   c. informácie v potrebnom rozsahu na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 27 ods.10 Zákona.
5. Prevádzkovateľ základnej služby je oprávnený požadovať od Poskytovateľa 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.

Článok XI.
Podmienky a spôsob ukončenia Zmluvy

1. 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 ZoD s Objednávateľom. V prípade, ak zmluvné strany dohodnú deň ukončenia Zmluvy pred dňom uplynutia účinnosti ZoD, táto Zmluva zaniká súčasne so zánikom účinnosti ZoD.
2. Prevádzkovateľ základnej služby je oprávnený písomne odstúpiť od tejto Zmluvy v prípade, ak Poskytovateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy:

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

3. Výpovedná lehota je jeden mesiac a začína plynúť prvého dňa mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.
4. Poskytovateľ je povinný po ukončení Zmluvy vrátiť, previesť alebo rozhodnutím Objednávateľa zničiť všetky informácie, ku ktorým mal ako tretia strana počas trvania zmluvného vzťahu prístup.
5. Poskytovateľ 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 Poskytovateľa ostáva v platnosti aj po ukončení Zmluvy po dobu 5 rokov.
6. Ukončením tejto Zmluvy je Objednávateľ oprávnený ukončiť aj ZoD, ku ktorej je táto Zmluva viazaná.

Článok XII.
Sankcie, zmluvné pokuty a náhrada škody

1. V prípade, ak Poskytovateľ poruší svoje povinnosti v zmysle tejto Zmluvy voči Prevádzkovateľovi základnej služby, a to najmä povinnosť
   a. dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
   b. prijímať a dodržiavať bezpečnostné opatrenia minimálne v rozsahu špecifikovanom v Článku V tejto Zmluvy,
   c. umožniť Prevádzkovateľovi základnej služby vykonať audit Poskytovateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení Poskytovateľom s bezpečnostnou politikou Prevádzkovateľa základnej služby,
   d. nedodržania lehoty 30 pracovných dní odo dňa zistenia nesúladu Poskytovateľom prijatých bezpečnostných opatrení zistených vykonaním auditu u Poskytovateľa na zabezpečenie nápravy nesúladu so Zákonom,
   e. 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,
   f. zabezpečiť a odovzdať Prevádzkovateľovi základnej služby písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia,

   vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 30.000,- EUR.
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.
3. V prípade, ak Dodávateľ poruší svoje povinnosti podľa čl. XI. ods. 5. tejto Zmluvy, vzniká Prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 100.000,- EUR.
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 základnej služby 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 Poskytovateľovi svoje pohľadávky vzniknuté z titulu zmluvnej pokuty a/alebo náhrady škody uplatnenej podľa tejto Zmluvy.

Článok XIII.
Záverečné ustanovenia

1. Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpisu ostatnou zo zmluvných strán.
2. Táto Zmluva sa vyhotovuje v troch rovnopisoch, 2 x pre Prevádzkovateľa základnej služby a 1 x pre Poskytovateľa. Akékoľvek dodatky a zmeny tejto Zmluvy sú platné len v písomnej forme, po ich odsúhlasení a podpísaní oboma zmluvnými stranami.
3. Neoddeliteľnou súčasťou tejto zmluvy sú tieto Prílohy:
   Príloha č.1 Všeobecné požiadavky na fyzickú a informačnú bezpečnosť
   Príloha č.2 Postupy hlásenia kybernetických bezpečnostných incidentov voči PZS
   Príloha č.3 Vzor - HLÁSENIE KYBERNETICKÉHO BEZPEČNOSTNÉHO INCIDENTU.
4. 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.
5. Táto Zmluva sa riadi právnym poriadkom Slovenskej republiky, najmä ustanoveniami Obchodného zákonníka, zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení a vyhláškou č. 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
6. Zmluvné strany vyhlasujú, že ich zmluvná voľnosť nebola žiadnym spôsobom obmedzená.
7. Zmluvné strany vyhlasujú, že táto Zmluva nebola uzavretá v tiesni ani za nápadne nevýhodných podmienok a ani v omyle.
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 Nitre, dňa 05-06-2025

Objednávateľ:
Západoslovenská vodárenská spoločnosť, a.s.

PhDr. Mgr. art. Otokar Klein, ArtD.
predseda predstavenstva

V Nitre, dňa 05-06-2025

Poskytovateľ:
FINECA TAX OFFICE s.r.o.
Ing. Miriam Buliková, PhD., konateľ

Ing. Marek Illéš
člen predstavenstva