ZMLUVA Č. ZOS10825 O ODBORNÝCH SLUŽBÁCH

(ďalej len „**Zmluva**")

Článok č. 1. Zmluvné strany

Klient: Trnavská vodárenská spoločnosť, a.s.
Priemyselná 10, 921 79 Piešťany
Zapísaný v Obch. registri Okresného súdu Trnava, Oddiel Sa, vložka č.:10263/T

Konajúci prostredníctvom:	Ing. Vladimír Púčik, predseda predstavenstva Ivan Šiška, podpredseda predstavenstva
IČO:	36252484
DIČ:	202172264
IČ pre DPH:	SK202172264
Bankové spojenie:	VÚB, a.s.
IBAN:	SK71 0200 0000 2700 0300 2212
SWIFT:	SUBASKBX

(ďalej len „**Klient**" alebo „**Prevádzkovateľ základnej služby**")

Dodávateľ: **CeMS, s.r.o.**
Snežienkova 1/A, 971 01 Prievidza
Spoločnosť s ručením obmedzeným zapísaná v Obchodnom registri Okresného súdu Trenčín, Oddiel: Sro, Vložka č. 16830/R

Konajúci prostredníctvom:	Ing. Denis Barborík
IČO:	35 891 823
DIČ:	2021849049
IČ pre DPH:	SK2021849049
Bankové spojenie:	Tatra banka, a.s.
IBAN:	SK03 1100 0000 0026 2505 0728
SWIFT:	TATRSKBX

(ďalej len „**Dodávateľ**")

Klient a dodávateľ sa ďalej označujú jednotlivo ako „**zmluvná strana**" a spoločne ako „**zmluvné strany**".

Táto Zmluva o odborných službách sa ďalej označuje spoločne s jej prílohami ako „**zmluva**". Zmluvné strany s úmyslom byť viazané podmienkami uvedenými nižšie uzatvárajú túto zmluvu o odborných službách podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v platnom znení (ďalej len „**Obchodný zákonník**")

Zmluvné strany uzatvárajú zmluvu na predmet zákazky *„Audit kybernetickej bezpečnosti*".

Článok č. 2. Predmet zmluvy

Dodávateľ sa zaväzuje poskytnúť Klientovi služby vymedzené v Článok č. 3. tejto zmluvy v súlade s podmienkami dohodnutými v tejto zmluve (ďalej len „**Služby**") a Klient sa zaväzuje uhradiť za poskytnuté Služby dodávateľovi odmenu dohodnutú v Článok č. 5. tejto zmluvy.

Článok č. 3. Rozsah Služieb – Audit kybernetickej bezpečnosti

3.1. Predmetom zmluvy je záväzok dodávateľa vykonať audit kybernetickej bezpečnosti Klienta v súlade s podmienkami uvedenými v tejto zmluve, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon**"), Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach (ďalej len „**Vyhláška o bezpečnostných opatreniach**") a Vyhlášky Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti (ďalej len „**Vyhláška o audite**").

3.2. Dodávateľ sa v rámci auditu kybernetickej bezpečnosti zaväzuje zabezpečiť výkon auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti (ďalej len „**Audítor kybernetickej bezpečnosti**") podľa Vyhlášky o audite, ktorý spĺňa všetky požiadavky na výkon auditu. Audítor je oprávnený na výkon auditu zostaviť audítorský tím, ktorý sa môže skladať aj z audítorov v zácviku alebo technických expertov. Títo členovia tímu konajú pod priamym dohľadom a zodpovednosťou Audítora kybernetickej bezpečnosti.

3.3. Zmluvné strany sa dohodli, že predmet zmluvy sa považuje za splnený riadne a včas dňom prevzatia Záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti (ďalej len „**Správa**") podľa bodu 3.6 a 4.3 tejto zmluvy.

3.4. Audítor kybernetickej bezpečnosti sa v rámci auditu kybernetickej bezpečnosti zaväzuje poskytnúť nasledovné Služby:

- v súlade so Štandardom na výkon auditu kybernetickej bezpečnosti (ďalej len „**Metodika auditu**") a v súlade s požiadavkami Zákona a Vyhlášky o bezpečnostných opatreniach na výkon auditu kybernetickej bezpečnosti, a teda auditu sietí a informačných systémov Klienta ako prevádzkovateľa základnej služby (t. j. subjekt, ktorý prevádzkuje sieť alebo informačný systém, ktorého narušenie by mohlo mať významný dopad na poskytovanie základnej služby), za účelom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek Zákona a Vyhlášky o bezpečnostných opatreniach, ktoré definujú príslušné požiadavky na prevádzkovateľa základnej služby. Audit kybernetickej bezpečnosti zahŕňa tieto požiadavky:

  Posúdenie prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine v oblastiach:
  a. Organizácia kybernetickej a informačnej bezpečnosti,
  b. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
  c. Personálna bezpečnosť,
  d. Riadenie prístupov,
  e. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
  f. Bezpečnosť pri prevádzke informačných systémov a sietí,
  g. Hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
  h. Ochrana proti škodlivému kódu,
  i. Sieťová a komunikačná bezpečnosť,
  j. Akvizícia, vývoj a údržba informačných sietí a informačných systémov,
  k. Zaznamenávanie udalostí a monitorovanie,
  l. Fyzická bezpečnosť a bezpečnosť prostredia,
  m. Riešenie kybernetických bezpečnostných incidentov,
  n. Kryptografické opatrenia,
  o. Kontinuita prevádzky,
  p. Audit, riadenie súladu a kontrolných činností.

3.5. Klient je povinný poskytnúť dodávateľovi všetky informácie a súčinnosť potrebnú pre splnenie predmetu tejto zmluvy.

3.6. Výstupom auditu kybernetickej bezpečnosti je Správa v slovenskom jazyku vypracovaná v súlade s požiadavkami Vyhlášky o audite. Správa bude mať nasledovnú štruktúru,
  (a) Meno a priezvisko Audítora kybernetickej bezpečnosti, číslo jeho platného certifikátu ako Audítora kybernetickej bezpečnosti, dátum jeho vyhotovenia a podpis riaditeľa certifikácie Kompetenčného a certifikačného centra kybernetickej bezpečnosti,
  (b) Vymedzenie rozsahu vykonaného auditu kybernetickej bezpečnosti,
  (c) Cieľ auditu kybernetickej bezpečnosti,
  (d) Použité postupy a metodiky vykonaného auditu kybernetickej bezpečnosti,
  (e) Zhrnutie zistení výsledkov auditu kybernetickej bezpečnosti a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,
  (f) Odporúčané nápravné opatrenia Audítora kybernetickej bezpečnosti pri zistení nedostatkov,
  (g) Dokumenty, ktorými sú najmä:
    1. Kópia certifikátu Audítora kybernetickej bezpečnosti,
    2. Kópia žiadosti o výkon auditu podľa Prílohy č. 1 Vyhlášky o audite, resp. Prílohy č. 1 tejto zmluvy.
    3. Výpočet rozsahu trvania auditu a zdôvodnenie skrátenia alebo predĺženia,

4. Kontrolný záznam auditovaných bezpečnostných opatrení s vyjadrením Prevádzkovateľa základnej služby so zisteniami auditu,
5. Harmonogram auditu,
6. Zoznam posúdenej dokumentácie,
7. Uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,
8. Zhodnotenie plnenia povinností podľa Zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sieti a informačných systémov, a konkrétne uvedenie nedostatkov.

Správa bude predložená v jednom elektronickom vyhotovení štatutárnemu orgánu Klienta zabezpečeným kanálom a podpísaná kvalifikovaným elektronickým podpisom Audítora kybernetickej bezpečnosti ako aj v tlačenom vyhotovení v dvoch (2) ks štatutárnemu orgánu Klienta spôsobom podľa bodu 6.3 tejto zmluvy.

3.7. Správa bude pripravená výlučne pre informovanie štatutárneho orgánu Klienta a relevantných zainteresovaných strán Klienta na účel špecifikovaný vyššie. Štatutárny orgán Klienta je oprávnený Správu v podobe predloženej Audítorom kybernetickej bezpečnosti predložiť Národnému bezpečnostnému úradu (ďalej len „**NBÚ**"), v súlade s účelom popísaným vyššie v tejto zmluve a ďalej sprístupniť nasledujúcemu Audítorovi kybernetickej bezpečnosti vykonávajúcemu audit kybernetickej bezpečnosti u Klienta pre informačné účely. Správa ani žiadna jej časť nesmie byť distribuovaná žiadnej tretej strane (s výnimkou výslovného predchádzajúceho písomného súhlasu dodávateľa udeleného vopred), ani použitá Klientom na žiaden iný účel. Žiadna tretia strana nie je oprávnená použiť Správu alebo akékoľvek informácie v nej uvedené ani sa na ne spoliehať, pokiaľ osobitný právny predpis nestanovuje inak.

3.8. Audit kybernetickej bezpečnosti vykonáva Audítor kybernetickej bezpečnosti za obdobie, v ktorom prebiehal zber podkladov a posudzovanie stavu auditu kybernetickej bezpečnosti, pričom Audítor kybernetickej bezpečnosti nie je povinný monitorovať a zohľadňovať siete a informačné systémy Klienta ani udalosti, ktoré nastali po dátume vydania Správy a ani nie je povinný Správu aktualizovať.

3.9. Žiadne informácie, ktoré Audítor kybernetickej bezpečnosti predloží Klientovi mimo Správy, nepredstavujú jeho konečné názory ani závery. Konečné názory alebo závery sa uvedú výlučne v Správe.

3.10. Pre vylúčenie akýchkoľvek pochybností platí, že akýkoľvek nesúhlas Klienta so závermi Audítora kybernetickej bezpečnosti uvedenými v Správe sa nepovažuje za porušenie povinností dodávateľa ani Audítora kybernetickej bezpečnosti vyplývajúcich zo zmluvy a nezakladá právo Klienta na odstúpenie od zmluvy alebo iné s porušením povinnosti podľa tejto zmluvy inak súvisiace nároky, okrem prípadov, kedy pripomienky Klienta smerovali proti porušeniu zákonných povinností Audítora kybernetickej bezpečnosti.

Článok č. 4. Miesto plnenia a harmonogram poskytovania Služieb

4.1. Zmluvné strany sa dohodli, že preferovanou formou poskytovania Služieb je vzdialené poskytovanie Služieb On-Line, pokiaľ si charakter Služby alebo okolnosti nevyžadujú poskytnutie Služby na mieste - On-Site, a to v priestoroch Klienta, resp. dodávateľa. Dodávateľ sa zaväzuje vykonať audit pre Klienta v lehote **do 4 mesiacov odo dňa nadobudnutia platnosti tejto zmluvy**. Dodávateľ je zároveň povinný vypracovať a prezentovať Klientovi program auditu, a to najneskôr do jedného dňa odo dňa podpisu tejto zmluvy. Návrh správy z auditu je Dodávateľ povinný doručiť Klientovi na pripomienkovanie najneskôr do jedného dňa od ukončenia auditu.

4.2. Predpokladaný harmonogram poskytovania Služieb je nasledovný:

Fáza auditu	***Termín (pracovné dni)***
Nastavenie auditného programu	**1 deň**
Výkon auditu kybernetickej bezpečnosti	**5 dní od nastavenia auditného programu**
Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti (Správa) - Návrh	**1 deň od ukončenia výkonu auditu**

Poskytnutie pripomienok Klientom k návrhu správy	**7 dní** od doručenia návrhu správy Klientovi
Doručenie finálnej správy (po zapracovaní pripomienok)	**2 dni** od prijatia pripomienok Klienta

Tieto termíny sa môžu v odôvodnených prípadoch, ktoré nebolo možné predvídať vopred, vzhľadom na personálne potreby Klienta a Audítora kybernetickej bezpečnosti a vzhľadom na iné okolnosti, ktoré sa môžu pri poskytovaní Služby podľa tejto zmluvy vyskytnúť, zmeniť v nevyhnutnom rozsahu, pričom takéto predĺženie lehoty sa bude musieť uskutočniť dodatkom k zmluve. Príslušná lehota vyššie sa v prípade „Nastavenie auditného programu" začína počítať odo dňa účinnosti zmluvy.

V prípade, že dôjde k predĺženiu lehôt dodatkom k zmluve, príslušná predĺžená lehota začne plynúť **dňom účinnosti tohto dodatku** a ostatné lehoty začnú plynúť od ukončenia predchádzajúcej fázy auditu, ak nie je lehota daná konkrétnym dátumom.

Výsledkom akéhokoľvek oneskorenia zo strany Klienta pri poskytnutí uvedených informácií, dokumentácie a všetkých údajov potrebných pre poskytnutie Služieb podľa tejto zmluvy alebo akejkoľvek inej súčinnosti, ktorú je Klient podľa tejto zmluvy povinný poskytnúť, môže byť oneskorenie uvedeného harmonogramu poskytovania Služieb zo strany Audítora kybernetickej bezpečnosti. Audítor kybernetickej bezpečnosti sa zaväzuje informovať Klienta o akýchkoľvek skutočnostiach vedúcich k oneskoreniu v dodržaní termínov alebo o iných okolnostiach, ktoré by mohli mať nepriaznivý vplyv na poskytovanie Služieb podľa tejto zmluvy bezodkladne po tom, čo sa o nich Audítor kybernetickej bezpečnosti dozvie. V takomto prípade Audítor informačných systémov oznámi Klientovi primerane upravený harmonogram poskytovania Služieb, pričom takto oznámený upravený harmonogram (aj opakovane) sa považuje za platný harmonogram auditu kybernetickej bezpečnosti po jeho schválení oboma zmluvnými stranami vo forme podpísaného dodatku k zmluve.

4.3. Audítor kybernetickej bezpečnosti predloží návrh Správy oprávnenej osobe za Klienta určenej v bode 6.1. tejto zmluvy na vyjadrenie pred vydaním finálnej verzie Správy. Klient je oprávnený predložiť svoje pripomienky k návrhu Správy najneskôr do sedem (7) pracovných dní od predloženia príslušného návrhu Správy Audítora kybernetickej bezpečnosti. Audítor kybernetickej bezpečnosti následne, najneskôr do sedem (7) pracovných dní od ukončenia výkonu auditu a po získaní pripomienok od Klienta, vydá finálnu verziu Správy. V prípade, že sa Klient nevyjadrí vo vyššie stanovenej lehote, považuje sa návrh Správy za akceptovaný zo strany Klienta a Audítor kybernetickej bezpečnosti vydá finálnu verziu Správy. O predložení Správy spíše Klient a dodávateľ Preberací protokol, ktorý bude súčasťou faktúry podľa ustanovenia 5.3 zmluvy (ďalej len „**Preberací protokol**"). Preberací protokol bude obsahovať identifikáciu tejto zmluvy, označenie Správy, dátum podpisu Preberacieho protokolu, meno a podpis osôb uvedených v odseku 6.1. zmluvy. Zodpovednosť dodávateľa za zhotovenú Správu podľa príslušných právnych predpisov nie je jej odovzdaním dotknutá.

4.4. Klient zabezpečí pravdivé, správne a úplné informácie a dokumenty potrebné na riadne a včasné splnenie predmetu zmluvy. Klient vyhlasuje, že pred dodávateľom alebo Audítorom kybernetickej bezpečnosti nebudú zamlčané žiadne informácie, ktoré dodávateľ alebo Audítor kybernetickej bezpečnosti požadoval od klienta.

4.5. Klient je povinný určiť aspoň jedného pracovníka (ďalej „**Poverený pracovník**"), ktorý bude v pracovnom čase zodpovedný za plnenie administratívnych a iných požiadaviek na účely realizácie predmetu tejto zmluvy. Klient oznámi meno a kontaktné údaje (email, mobilné telefónne číslo) Povereného pracovníka Audítorovi kybernetickej bezpečnosti pred začatím poskytovania Služieb.

4.6. Audítor kybernetickej bezpečnosti predloží Klientovi a Poverenému pracovníkovi detailnú požiadavku na informácie a dokumentáciu minimálne v rozsahu definovanom vo Vyhláške o audite. Tieto informácie a dokumentáciu Klient doručí Audítorovi kybernetickej bezpečnosti najneskôr päť (5) dní pred začatím poskytovania Služieb, ak Audítor kybernetickej bezpečnosti neurčil neskoršiu lehotu. Audítor kybernetickej bezpečnosti nezačne poskytovať Služby, kým od Klienta neobdrží požadované informácie a dokumentáciu. Ak informácie a dokumentácia predložené Audítorovi kybernetickej bezpečnosti zo strany Klienta nie sú doručené včas alebo nebudú dostatočné alebo primerané, a Audítor kybernetickej bezpečnosti bude vyžadovať ich doplnenie, za podmienok uvedených v zmluve si Audítor kybernetickej bezpečnosti vyhradzuje právo zmeniť harmonogram poskytovania Služieb primerane podľa dostupnosti požadovaných informácií a jeho možností alebo odporučiť odklad výkonu auditu, pričom takto upravený harmonogram sa považuje za platný harmonogram auditu kybernetickej bezpečnosti po jeho schválení oboma zmluvnými stranami vo forme podpísaného dodatku k zmluve.

Článok č. 5. Cena a platobné podmienky

5.1. Zmluvné strany sa dohodli na cene za Služby uvedené v článku č. 3 na sume **6440,00 EUR bez DPH** (slovom: šesťtisícštyristoštyridsať Eur bez DPH) (ďalej len „**Cena**"). Dodávateľ je platca DPH. Cena je konečná a zahŕňa všetky náklady spojené s poskytovaním Služieb.

5.2. Cena sa bude fakturovať po ukončení poskytovania Služieb a predložení finálnej Správy Klientovi spôsobom podľa bodu 3.3 zmluvy. Faktúra bude vystavená do piatich (5.) dní odo dňa akceptácie finálnej Správy Klientovi podľa bodu 4.3 zmluvy. Faktúra je splatná do **30** dní odo dňa jej vystavenia podľa bodu 5.4. tohto článku zmluvy.

5.3. Faktúra musí obsahovať náležitosti podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov. V prípade jej neúplnosti alebo nesprávnosti je Klient oprávnený ju vrátiť dodávateľovi na opravu alebo doplnenie; v takom prípade začne plynúť nová tridsať (30) dňová lehota splatnosti dňom doručenia novej alebo opravenej faktúry Klientovi. Súčasťou faktúry je Preberací protokol podľa bodu 4.3 zmluvy.

5.4. Zmluvné strany sa dohodli, že faktúry budú vyhotovené v elektronickej podobe (tzv. elektronická faktúra) vo formáte PDF/A a Klientovi budú doručované emailom na emailovú adresu efaktury@tavos.sk a zároveň aj na emailovú adresu uvedenú v bode 6.1 tejto zmluvy, pričom faktúry sa považujú za doručené Klientovi dňom nasledujúcim po dni ich odoslania..

5.5. Všetky peňažné plnenia podľa zmluvy sú splatné v EUR na bankový účet dodávateľa uvedený v záhlaví zmluvy.

5.6. V prípade uskutočnenia prác navyše, dopredu dohodnutých a odsúhlasených Klientom spolu s vyčíslenou zmenenou Cenou, ktorých potreba vyplynula z okolností, ktoré Klient nemohol pri vynaložení náležitej starostlivosti predvídať a takouto zmenou nedochádza k zmene charakteru zmluvy pristúpia zmluvné strany k uzatvoreniu písomného dodatku ku zmluve. Dodávateľ na potrebu uzatvorenia dodatku vopred Klienta upozorní, spolu s vyčíslením zmeny Ceny a jej odôvodnením. Pokiaľ nebude v dodatku dohodnuté inak, cena prác navyše bude určená na základe dodatočného času, ktorý Audítor kybernetickej bezpečnosti vynaloží z dôvodov podľa tohto bodu zmluvy a štandardných hodinových sadzieb bez DPH, ktoré sú uvedené v nasledujúcej tabuľke (tzv. osobodní, resp. *manday,* pričom jeden osobodeň predstavuje 8 pracovných hodín):

Audítor kybernetickej bezpečnosti	890,00 EUR/manday

5.7. V prípade omeškania Klienta s úhradou akéhokoľvek peňažného plnenia podľa tejto zmluvy je Dodávateľ oprávnený požadovať od Klienta úrok z omeškania vo výške 0,1 % z nezaplatenej sumy za každý aj začatý deň omeškania.

5.8. V prípade, že Dodávateľ nedodá finálnu verziu správy o audite v lehote stanovenej v článku 4.1 tejto zmluvy, a toto omeškanie nevzniklo z dôvodu konania klienta, je klient oprávnený požadovať zmluvnú pokutu vo výške 0,1 % z ceny za každý aj začatý deň omeškania. Povinnosť Dodávateľa platiť úroky z omeškania týmto nie je dotknutá.

5.9. Zmluvné pokuty sú splatné 30. (tridsiatym) dňom odo dňa, kedy malo dôjsť k nesplneniu povinnosti, na porušenie ktorej sa vzťahuje zmluvná pokuta. Ustanovenia tohto článku sa pre fakturáciu zmluvnej pokuty použijú primerane.

Článok č. 6. Komunikácia

6.1. Adresy, telefónne čísla a e-mailové adresy zmluvných strán na účely ich oznámení týkajúcich sa tejto zmluvy sú:

Za Dodávateľa: **CeMS s.r.o.**
Do pozornosti : Vedúci certifikačného orgánu
Tel: +421 903 515 662
E-mail: barborik@cems.sk

Za Klienta: **Trnavská vodárenská spoločnosť, a.s.**
Do pozornosti: Ing. Miroslav Sedlák – špecialista IT
Tel: 0911 047 072
E-mail: sedlak@tavos.sk

O zmene kontaktných údajov alebo kontaktných osôb je dotknutá zmluvná strana povinná druhú zmluvnú stranu informovať bez zbytočného odkladu, najneskôr však do dvoch (2) pracovných dní po vykonaní zmeny. Oznámenie musí byť zaslané písomne (napr. e-mailom) na kontaktnú adresu alebo e-mailovú adresu druhej zmluvnej strany uvedenú v ods. 6.1. Zmena kontaktných údajov si nevyžaduje uzatvorenie dodatku k zmluve.

6.2. S výnimkou otázok týkajúcich sa zániku tejto zmluvy, nárokov na náhradu škody alebo iného peňažného plnenia podľa tejto zmluvy, ktoré musia byť uplatnené písomne, sú zmluvné strany oprávnené komunikovať aj formou emailu a táto emailová komunikácia bude považovaná za riadne oznámenie podľa tejto zmluvy. Písomnosť sa považuje za doručenú za nasledovných podmienok:

(a) v prípade osobného doručovania odovzdaním písomnosti oprávnenej osobe za Klienta určenej v bode 6.1. tejto zmluvy alebo inej osobe oprávnenej prijímať písomnosti za túto zmluvnú stranu a podpisom takej osoby na doručenke a/alebo kópii doručovanej písomnosti, alebo odmietnutím prevzatia písomnosti takou osobou,

(b) v prípade poštového doručovania doručením na adresu zmluvnej strany a v prípade doporučenej zásielky odovzdaním písomnosti osobe oprávnenej prijímať písomnosti za túto zmluvnú stranu a podpisom takej osoby na doručenke, najneskôr však uplynutím siedmych (7) dní odo dňa uvedeného na podacom lístku, a to bez ohľadu na úspešnosť doručenia,

6.3. Klient si je vedomý, že v prípade emailovej komunikácie nemožno zaručiť úplnú bezpečnosť a bezchybnosť a že takéto informácie môžu byť zachytené, poškodené, môžu sa stratiť, zničiť, môžu byť doručené neskoro alebo neúplné, alebo môžu byť inak negatívne ovplyvnené.

Článok č. 7. Obmedzenie zodpovednosti

7.1. Dodávateľ zodpovedá len za skutočnú škodu spôsobenú porušením tejto zmluvy, a to v plnom rozsahu, nezodpovedá však za škody spôsobené porušením tejto zmluvy zo strany klienta či prípadných zákonných pochybení zo strany Klienta. Dodávateľ v plnom rozsahu zodpovedá aj za škodu spôsobenú konaním alebo opomenutím osôb, ktoré poveril výkonom auditu alebo zastupovaním pri externom audite.

7.2. Dodávateľ v súvislosti s plnením predmetu zmluvy nezodpovedá za žiadne nároky tretích strán voči Klientovi, okrem prípadu, keď nárok tretej stany vyplýva z porušenia jeho práv konaním dodávateľa.

7.3. Klient má zmluvný vzťah výlučne s dodávateľom. Klient nebude mať žiadne nároky voči iným osobám použitým pri plnení tejto zmluvy s výnimkou dodávateľa.

Článok č. 8. Autorské práva a duševné vlastníctvo

8.1. Dodávateľ je nositeľom všetkých práv duševného vlastníctva na všetko, čo vytvoril Audítor kybernetickej bezpečnosti pred alebo počas poskytovania Služieb, vrátane správ, písomného poradenstva, listov, odporúčaní alebo iných výstupov poskytovania Služieb Klientovi (ďalej ako „**Výstupy**"). Výstupy zostávajú vo vlastníctve dodávateľa. Momentom úhrady Ceny a ďalších zmluvou predpokladaných peňažných plnení udeľuje dodávateľ Klientovi výhradnú licenciu na použitie týchto Výstupov na dosiahnutie účelu tejto zmluvy a v súlade s ostatnými ustanoveniami zmluvy. Dodávateľ je oprávnený použiť Výstupy spôsobom, na ktorý licenciu udelil v súlade s bodom 8.3 zmluvy. Licencia sa udeľuje na obdobie trvania majetkových práv k Výstupom. Spôsoby používania Výstupov ako aj vecný a územný rozsah licencie sú obmedzené účelom, na ktorý boli Výstupy vypracované.

8.2. Pre vylúčenie akýchkoľvek pochybností platí, že licencia podľa bodu 8.1 sa vzťahuje na obsah a formu vyjadrenia Správy, nie však na metodiku a postupy, ktorými bola Správa vytvorená. Zmluvné strany sa dohodli, že Dodávateľ je oprávnený Výstupy naďalej použiť, a to v súlade so všeobecne záväznými právnymi predpismi alebo na základe rozhodnutia orgánu verejnej moci.

8.3. Ustanovenia tohto článku sa nevzťahujú na správy a iné dokumenty, ktoré je klient povinný poskytnúť Národnému bezpečnostnému úradu (NBÚ) podľa Zákona o kybernetickej bezpečnosti a/alebo Zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám. Klient má právo použiť, zverejniť a poskytnúť tieto dokumenty, pokiaľ je to v súlade s platnou legislatívou, pričom sa na tieto výstupy licenčné podmienky nevzťahujú.

Článok č. 9. Ochrana osobných údajov a ochrana dôverných skutočností

9.1. Zmluvné strany vyhlasujú, že majú zavedenú štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Zmluvné strany spracúvajú osobné údaje v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „**Nariadenie**"), ako aj zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon OOÚ**").

9.2. V súlade s Nariadením a Zákonom OOÚ, Klient a dodávateľ sú v postavení samostatných prevádzkovateľov. Dodávateľ pri vykonávaní auditu spracúva osobné údaje vo vlastnom mene a pre účely auditu, a nie v mene Klienta.

9.3. Klient aj dodávateľ sú povinní dôsledne chrániť všetky spracúvané osobné údaje, s ktorými prídu do styku pri plnení predmetu tejto zmluvy. Klient aj dodávateľ sú povinní prijať primerané technické a organizačné opatrenia tak, aby spracúvanie osobných údajov spĺňalo požiadavky Nariadenia resp. Zákona OOÚ a aby bola zabezpečená ochrana práv dotknutých osôb podľa Nariadenia a Zákona OOÚ. Zároveň sú povinní plniť ďalšie povinnosti uložené príslušnými právnymi predpismi v oblasti ochrany osobných údajov a ochrany informácií.

9.4. Klient potvrdzuje, že všetky osobné údaje poskytnuté dodávateľovi boli získané zákonným spôsobom, pri zachovaní všetkých základných zásad spracúvania osobných údajov.

9.5. Audítor kybernetickej bezpečnosti je povinný vo vzťahu ku všetkým mu poskytnutým informáciám a údajom zachovávať mlčanlivosť podľa § 12 Zákona.

9.6. Všetky informácie, ktoré si zmluvné strany pre splnenie predmetu zmluvy navzájom poskytli počas predzmluvných rokovaní, sa považujú za dôverné a poskytnúť tieto informácie tretej osobe môže zmluvná strana len po predchádzajúcom písomnom súhlase druhej zmluvnej strany. Uvedené informácie sa zaväzuje chrániť ako vlastné, využívať ich len v súvislosti s plnením predmetu zmluvy, nezneužívať a nesprístupniť ich tretím osobám. Dôverné informácie nemôžu byť sprístupnené tretej osobe bez výslovného predchádzajúceho písomného súhlasu druhej zmluvnej strany, ak zmluva neustanovuje inak alebo ak zo zmluvy nevyplýva inak. Za dôverné informácie sa na účely zmluvy pokladajú aj všetky informácie, údaje alebo iné skutočnosti, o ktorých sa zmluvná strana dozvedela na základe a/alebo v spojení so zmluvou (ďalej len „**Dôverné informácie**").

9.7. Pre potreby tohto článku sa za Dôverné informácie okrem iného považujú informácie, ktoré súvisia s činnosťou zmluvnej strany, ktoré druhá zmluvná strana priamo alebo nepriamo získa, v písomnej, ústnej, elektronickej alebo inej forme, a to bez ohľadu na to, či sú alebo nie sú označené ako tajné alebo dôverné.

9.8. Každá zmluvná strana súhlasí, že vyvinie rovnaký stupeň starostlivosti a diskrétnosti, aby zabránila zverejneniu Dôverných informácií druhej zmluvnej strany, ktoré získa alebo získala na základe tejto zmluvy vo vzťahu k druhej zmluvnej strane alebo jej zástupcom alebo akejkoľvek tretej strane, ak povinnosť poskytnutia takejto informácie Klientom nevyplýva z právneho predpisu Slovenskej republiky.

9.9. Povinnosť ochrany osobných údajov a mlčanlivosti o dôverných informáciách nie je časovo obmedzená a platí aj po skončení trvania zmluvy, okrem prípadov, kedy poskytnutie, sprístupnenie alebo zverejnenie údajov ustanovuje zákon alebo rozhodnutie súdu.

Článok č. 10. Trvanie a ukončenie zmluvy

10.1. Táto zmluva nadobúda platnosť dňom jej podpísania oboma zmluvnými stranami. Táto Zmluva je povinne zverejňovanou Zmluvou podľa 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. Zmluvné strany sa dohodli, že zmluva nadobúda účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv.

10.2. Platnosť zmluvy sa skončí podľa toho, ktorý prípad nastane skôr:

(a) riadnym splnením predmetu zmluvy podľa ods. 3.3; alebo
(b) zmluvné strany uzatvoria písomnú dohodu o ukončení platnosti zmluvy; alebo
(c) odstúpením od zmluvy po tom, ako jedna zmluvná strana prevezme písomné oznámenie druhej zmluvnej strany o odstúpení od zmluvy, v ktorom sa uvádza, že druhá zmluvná strana porušila podstatným spôsobom povinnosti jej vyplývajúce zo zmluvy (ďalej len „**porušujúca zmluvná strana**") za predpokladu, že porušujúca zmluvná strana bola na

porušovanie povinností vopred písomne upozornená a napriek tomu nevykonala nápravu v primeranej lehote (ktorá nesmie byť kratšia ako 15 dní) od doručenia písomného upozornenia.

10.3. Dodávateľ je okrem dôvodov podľa bodu 10.2 písm. c) zmluvy oprávnený od zmluvy odstúpiť na základe písomného oznámenia doručeného Klientovi aj v prípade, ak zistí, že sa objavila závažná prekážka vo výkone auditu pred dňom alebo počas výkonu auditu kybernetickej bezpečnosti (okrem iného vrátane takej zmeny v príslušnej legislatíve alebo v dôsledku takého rozhodnutia štátneho orgánu alebo inej príslušnej profesijnej organizácie alebo takých náležitostiach žiadosti o audit kybernetickej bezpečnosti), na základe ktorých by plnenie ktorejkoľvek časti zmluvy zo strany dodávateľa bolo zmenené, sťažené, protiprávne alebo inak nezákonné alebo v rozpore s pravidlami nezávislosti alebo pravidlami profesijnej etiky.

Predčasné ukončenie zmluvy nemá vplyv na povinnosť Klienta uhradiť dodávateľovi Cenu za Služby, ktoré podľa zmluvy riadne poskytol do dňa účinnosti ukončenia platnosti zmluvy. Zmluvné strany sa dohodli, že cena podľa prechádzajúcej vety sa vypočíta ako súčin dohodnutej jednotkovej ceny za MD (Man-Day), ktorá je definovaná v bode 5.2 zmluvy, a skutočného počtu MD/pracovných dní, ktoré dodávateľ vynaložil na poskytovanie služieb do ukončenia zmluvy.

Článok č. 11. Záverečné ustanovenia

11.1. Zmluvné strany vyhlasujú, že získali všetky potrebné povolenia a oprávnenia na uzavretie tejto zmluvy a na jej plnenie.

11.2. Táto zmluva sa vyhotovuje v piatich (3) rovnopisoch v slovenskom jazyku, pričom dva(2) rovnopisy obdrží Klient a jeden (1) rovnopis Dodávateľ.

11.3. Akékoľvek zmeny a/alebo doplnenia zmluvy sa môžu vykonať iba na základe dohody obidvoch zmluvných strán, a to vo forme písomných a očíslovaných dodatkov k zmluve podpísaných oprávnenými zástupcami oboch zmluvných strán.

11.4. V prípade, že akékoľvek ustanovenie zmluvy je alebo sa stane neplatným, neúčinným alebo nevykonateľným, nie je tým dotknutá platnosť, účinnosť, alebo vykonateľnosť ostatných ustanovení zmluvy, pokiaľ to nevylučuje v zmysle všeobecne záväzných právnych predpisov samotná povaha takého ustanovenia. Zmluvné strany sa zaväzujú bez zbytočného odkladu po tom, ako zistia, že niektoré z ustanovení zmluvy je neplatné, neúčinné alebo nevykonateľné, nahradiť dotknuté ustanovenie ustanovením novým, ktorého obsah bude v čo najväčšej miere zodpovedať vôli zmluvných strán v čase uzatvorenia zmluvy.

11.5. Zmluvné strany vyhlasujú, že túto zmluvu uzatvorili slobodne, vážne a bez omylu, nebola uzatvorená v tiesni ani za nápadne nevýhodných podmienok, že si zmluvu prečítali a jej obsahu porozumeli, a na znak súhlasu s jej obsahom ju podpisujú.

11.6. Zoznam príloh – neoddeliteľnou súčasťou tejto zmluvy sú:

a) Príloha č. 1 – Vzor žiadosti o výkon auditu kybernetickej bezpečnosti

Dodávateľ:	**Klient:**
V ..... dňa	V Trnave dňa .....
CeMS, s.r.o.	**Trnavská vodárenská spoločnosť, a.s.**
Ing. Denis Barborík	Ing. Vladimír Púčik
konateľ	predseda predstavenstva
	Ivan ŠišKA
	podpredseda predstavenstva

Príloha č. 1 – Vzor žiadosti o vykonanie auditu kybernetickej bezpečnosti

Spoločnosť, IČO	
Zodpovedný zamestnanec (meno, email, tel. číslo)	

Č.	Otázka	Odpoveď
1	Ste prevádzkovateľom prvku kritickej infraštruktúry[1]?	
2	Ste prevádzkovateľom základnej služby („PZS“)?	
2.1	Ak áno, aké základné služby prevádzkujete?[2]	
3	Počet užívateľov Siete a Informačného Systému[3] s väzbou na základné služby? (ďalej len IS) *Príklad:* *1500 interných* *3000 externých*	
4	Počet IS pre jednotlivé základné služby?	
5	Počet zamestnancov zúčastňujúcich na prevádzke IS s väzbou na základnú službu?	
6	Štruktúra správy IS s väzbou na základnú službu *Centralizovaná verzus distribuovaná*	
7	Počet externých pracovísk, kde je prevádzkovaný samostatný IS s väzbou na základnú službu, iný ako na ostatných pracoviskách?	
8	Máte s tretími stranami uzavreté akékoľvek zmluvy na výkon činností, ktoré priamo súvisia s prevádzkou IS s väzbou na základné služby (*ak áno, počet a typ služieb*)? *Príklad:* *1 x dodávateľ podpory užívateľských staníc* *1 x dodávateľ IS zariadení* *1 x dodávateľ laboratórnych zariadení*	
9	Počet zamestnancov tretích strán zúčastňujúcich na prevádzke IS s väzbou na základnú službu?	
10	Máte vypracovanú bezpečnostnú dokumentáciu týkajúcu sa Vašich IS ?	
11	Máte určenú rolu manažéra kybernetickej bezpečnosti?	
12	Vykonali ste kategorizáciu IS podľa požiadaviek Zákona?	
12.1	Ak áno, sú IS zaradené do:	
12.2	I. kategórie	
12.3	II. kategórie	
12.4	III. kategórie	

13	Máte záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti podľa § 29 Zákona.	
14	Vyskytol sa závažný kybernetický bezpečnostný incident za posledné 2 roky?	
15	Porušili ste povinnosti ZoKB, prípadne bola udelená pokuta? *(ak áno, aké)*	
16	Ste držiteľom certifikátu podľa technickej normy (napr. ISO 27001) a certifikovaná oblasť zahŕňa IS s väzbou na základnú službu? *(uveďte aj podľa akej normy)*	
17	Máte potvrdenie o priemyselnej bezpečnosti? *(ak áno, uveďte číslo)*	
18	Počet lokalít, v ktorých sa vykonávajú aktivity na zabezpečenie prevádzky Základnej služby?	
19	Ďalšie informácie	

1 § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre

2 Každý informačný systém, ktorý je asociovaný k základnej službe, je potenciálnym cieľom kybernetického útoku. Preto je dôležité identifikovať všetky tieto systémy, aby sa mohli zahrnúť do auditu a posúdiť ich bezpečnosť.

V závislosti od dôležitosti a citlivosti údajov, ktoré sú v informačných systémoch uložené, sa systémy kategorizujú.

Príklad
Ak prevádzkovateľ základnej služby poskytuje napríklad online bankovníctvo, medzi asociované informačné systémy môžu patriť:

- Systém pre správu účtov klientov
- Systém pre spracovanie transakcií
- Systém pre autentifikáciu klientov
- Webová stránka banky
- Mobilná aplikácia banky

3 § 3 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

Každý, kto využíva služby, ktoré štát určil ako kľúčové pre fungovanie spoločnosti a štátu. Tieto služby sú nevyhnutné pre zabezpečenie základných potrieb obyvateľstva, fungovanie ekonomiky a štátu.
Príklady používateľov základných služieb

- **Bežný občan**:*
  - Klient banky, ktorý využíva online bankovníctvo.
  - Pacient, ktorý sa objednáva k lekárovi cez internet.
  - Cestujúci, ktorý si kupuje lístok na vlak online.
- **Podnikateľ**:*
  - Firma, ktorá využíva cloudové služby pre svoje podnikanie.
  - Spoločnosť, ktorá využíva telekomunikačné služby pre komunikáciu so zákazníkmi.