**Príloha č. 5 ZMLUVY O DIELO A O POSKYTOVANÍ SLUŽIEB č. .../.../.../BVS**

**Zmluva o zabezpečení plnenia bezpečnostných opatrení**

**a notifikačných povinností**

podľa § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a príslušných vykonávacích predpisov, ako aj podľa ustanovenia § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „**Zmluva**“)

uzatvorená medzi týmito zmluvnými stranami:

|  |  |
| --- | --- |
| **Prevádzkovateľ základnej služby**: |  |
| Obchodné meno: | **Bratislavská vodárenská spoločnosť, a.s.** |
| Sídlo: | Prešovská 48, 826 46 Bratislava |
| IČO: | 35 850 370 |
| Bankové spojenie IBAN: | SK07 0200 0000 0000 0100 4062 |
| V zastúpení: | vyplní obstarávateľ |
| **Kontaktná osoba zodpovedná**  **za oblasť kybernetickej bezpečnosti:** |  |
| Funkcia: |  |
| Adresa pre doručovanie poštou: |  |
| Emailová adresa:  Telefónne číslo: |  |
| (ďalej len „**Prevádzkovateľ**“) |  |
| a |  |
| **Dodávateľ**: |  |
| Obchodné meno: | XXXX |
| Sídlo: |  |
| IČO: |  |
| Zapísaný: |  |
| IČ DPH: |  |
| Bankové spojenie IBAN: |  |
| V zastúpení: |  |
| **Kontaktná osoba zodpovedná**  **za oblasť kybernetickej bezpečnosti:** |  |
| Funkcia: |  |
| Adresa pre doručovanie poštou: |  |
| Emailová adresa: |  |
| Telefónne číslo: |  |
| (ďalej len „**Dodávateľ**“) |  |
| (Prevádzkovateľ a Dodávateľ ďalej spolu aj „**Zmluvné strany**“) | |

**Článok I**

**Úvodné ustanovenia**

* 1. Zmluvné strany potvrdzujú, že medzi sebou uzatvorili osobitnú zmluvu špecifikovanú v Prílohe č. 1 (ďalej len „**Hlavná zmluva**“).
  2. Pri plnení Hlavnej zmluvy vykonáva Dodávateľ činnosti, ktorých konkrétny rozsah je uvedený v Prílohe č. 1.
  3. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí, ktoré majú prístup k informáciám a údajom Prevádzkovateľa bez zbytočného odkladu, najneskôr však do 5 pracovných dní od účinnosti príslušnej zmeny. Zoznam pracovných rolí Dodávateľa, ktoré majú mať prístup k informáciám a údajom Prevádzkovateľa ku dňu uzatvorenia Zmluvy je uvedený v Prílohe č. 2.

**Článok II**

**Definície pojmov a výkladové pravidlá**

* 1. Na účely tejto Zmluvy sa pod pojmom:

1. „**kybernetická bezpečnosť**“ 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. „**kybernetický bezpečnostný incident**“ rozumie udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov,
3. „**dôvernosť**“ rozumie  záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
4. „**dostupnosť**“ rozumie záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované,
5. „**integrita**“ rozumie záruka, že bezchybnosť, úplnosť alebo správnosť údaja neboli narušené,
6. „**riziko**“ rozumie potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu,
7. „**hrozba**“ rozumie každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
8. „**riešenie kybernetického bezpečnostného incidentu**“ rozumie aktivita a postup zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie kybernetického bezpečnostného incidentu alebo na reakciu naň a zotavenie z neho,
9. „**bezpečnostné opatrenia**“ rozumejú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov, ktoré sú v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti a ktoré sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služby,
10. „**Úrad**“ rozumie Národný bezpečnostný úrad,
11. „**Ústredný orgán**“ rozumie Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky,
12. „**základná služba**“ rozumie „Správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov“,
13. „**analýza rizík**“ rozumie určenie pravdepodobnosti vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva,
14. „**Zákon**“ rozumie zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
15. „**vykonávacie predpisy**“ rozumejú všeobecné záväzné právne predpisy vydané na vykonanie Zákona, vrátane tých, ktoré nadobudnú účinnosť po nadobudnutí účinnosti tejto Zmluvy.
    1. Ak nie je výslovne uvedené inak,
16. pojmy a výrazy používané v tejto Zmluve, ktoré sú definované v Zákone a vo vykonávacích predpisoch, majú význam definovaný v týchto právnych predpisoch, pričom výklad ich obsahu musí byť v súlade s ich vymedzením v Smernici Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2),
17. alebo ak z obsahu nevyplýva niečo iné, jednotné číslo zahŕňa aj množné číslo a naopak,
18. akýkoľvek odkaz na akýkoľvek bod, písmeno alebo prílohu je odkazom na bod, písmeno alebo prílohu tejto Zmluvy.

**Článok III**

**Účel a predmet Zmluvy**

* 1. Predmetom tejto Zmluvy je úprava vzájomných práv a povinností Zmluvných strán s cieľom zabezpečiť plnenie bezpečnostných opatrení a notifikačných povinností pri výkone činností podľa Hlavnej zmluvy, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby (ďalej len „**Plnenie Hlavnej zmluvy**“).
  2. Účelom tejto Zmluvy je predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby pri Plnení Hlavnej zmluvy.

**Článok IV**

**Práva a povinnosti Zmluvných strán**

* 1. Dodávateľ vyhlasuje, že sa pred uzavretím tejto Zmluvy oboznámil s bezpečnostnými politikami uplatňovanými u Prevádzkovateľa a /alebo so špecifikovanými bezpečnostnými požiadavkami a opatreniami uvedenými v prílohe k tejto Zmluve a vyjadruje s nimi svoj súhlas a zaväzuje sa ich v celom rozsahu dodržiavať. Zoznam bezpečnostných politík a /alebo špecifikovaných bezpečnostných  požiadaviek podľa predchádzajúcej vety je uvedený v Prílohe č. 3. (ďalej len „**Bezpečnostné politiky**“).
  2. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti a musia zahŕňať minimálne (a) detekciu kybernetických bezpečnostných incidentov, (b) evidenciu kybernetických bezpečnostných incidentov, (c) postupy riešenia a riešenie kybernetických bezpečnostných incidentov, (d) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení, a (e) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania. Bezpečnostné opatrenia podľa predchádzajúcej vety musia byť prijaté najmä pre oblasti (1) správu zraniteľností a kybernetických hrozieb, (2) správu aktív a riadenie kybernetických hrozieb a rizík, (3) riadenie udalostí a kybernetických bezpečnostných incidentov, (4) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie, (5) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií, (6) kryptografické opatrenia a zásady používania kryptografie, (7) bezpečnosť a spôsobilosti ľudských zdrojov, (8) správu identít a prístupov, (9) bezpečnosť pri prevádzke sietí a informačných systémov, (10) ochranu proti škodlivému kódu a nežiaducemu obsahu, (11) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť, (12) monitorovanie, zaznamenávanie a hlásenie udalostí, (13) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení, (14) ochranu záznamov, súkromia a označovanie informácií, (15) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.
  3. Dodávateľ sa zaväzuje prijať a dodržiavať bezpečnostné opatrenia, ktorých minimálny rozsah a konkrétna špecifikácia sú uvedené v Prílohe č. 4 a s týmito bezpečnostnými opatreniami vyjadruje Dodávateľ svoj súhlas (ďalej len „**Bezpečnostné opatrenia**“).
  4. Vzhľadom na skutočnosť, že sa Bezpečnostné opatrenia u Prevádzkovateľa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu, je Prevádzkovateľ v závislosti na obsahu bezpečnostnej dokumentácie oprávnený jednostranne meniť obsah Bezpečnostných politík a rovnako upravovať rozsah a druhy Bezpečnostných opatrení, a to predovšetkým v prípade, ak sú dostupné prostriedky schopné zabezpečovať kybernetickú bezpečnosť účinnejšie než doposiaľ uplatňované. Zmena znenia Bezpečnostných opatrení bude Dodávateľovi oznámená emailom a zverejnením nového (aktuálneho) znenia na: *doplní úspešný uchádzač*, pričom zmeny budú záväzne uplynutím dní od doručenia oznámenia o zverejnení nového (aktuálneho) znenia kontaktnej osobe Dodávateľa (postačí oznámenie na email) spolu so znením, pokiaľ sa zmluvné strany nedohodnú inak.
  5. Prevádzkovateľ si vyhradzuje právo vykonávať v rámci vlastných alebo ním prevádzkovaných sietí a informačných systémov, ku ktorým má Dodávateľ prístup, kontroly bezpečnosti vykonávaných zásahov a prijímať opatrenia za účelom identifikácie zneužitia prístupu k týmto sieťam a informačným systémom.
  6. Dodávateľ sa zaväzuje, že po ukončení Hlavnej zmluvy Prevádzkovateľovi vráti, prevedie alebo podľa jeho pokynov aj zničí všetky informácie a dokumenty, ku ktorým počas trvania Hlavnej zmluvy získal prístup.
  7. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.
  8. Dodávateľ je povinný vypracovať a stanoviť postupy pre plnenie svojich povinností podľa tejto Zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi.
  9. Dodávateľ sa zaväzuje, že bez vykonaného preukázateľného oboznámenia s dokumentáciou podľa bodu 4.8. tohto článku, žiadnemu zo svojich zamestnancov ani inej osobe zapojenej do Plnenia Hlavnej zmluvy neumožní prístup k sieťam a k informačným systémom prevádzkovateľa základnej služby, ktoré prevádzkujú systémy základnej služby a pre prostriedky, ktoré podporujú základné služby.
  10. Bezpečnostné opatrenia a notifikačné povinnosti vyplývajúce z tejto Zmluvy sa Dodávateľ zaväzuje plniť počas celej doby Plnenia Hlavnej Zmluvy.
  11. V prípade, ak Plnenie Hlavnej zmluvy podlieha povinnej certifikácii v rámci systému certifikácie kybernetickej bezpečnosti, Dodávateľ týmto prehlasuje, že disponuje všetkými potrebnými povoleniami a potrebnými certifikátmi v zmysle príslušnej právnej úpravy a ich získanie je povinný preukázať Prevádzkovateľovi.

**Článok V**

**Kontrolné činnosti, audity a nápravné opatrenia**

* 1. Zmluvné strany potvrdzujú, že pred uzatvorením Zmluvy bola u Dodávateľa vykonaná analýza rizík kybernetickej bezpečnosti uskutočnená Prevádzkovateľom, vrátane overenia zverejnených politických rizík zo strany Úradu, so zameraním na odhalenie možných negatívnych dopadov a prijatie opatrení potrebných na zmiernenie negatívnych vplyvov v podmienkach Dodávateľa.
  2. Ak je to potrebné na zabezpečenie kybernetickej bezpečnosti pri Plnení Hlavnej zmluvy, je Prevádzkovateľ oprávnený vydávať Dodávateľovi zdokumentované pokyny. V takom prípade je Dodávateľ povinný postupovať podľa pokynov Prevádzkovateľa a pri Plnení Hlavnej zmluvy je týmito pokynmi viazaný. Dodávateľ je vždy povinný upozorniť Prevádzkovateľa, ak podľa jeho názoru záväzný pokyn Prevádzkovateľa porušuje Zákon, vykonávacie predpisy alebo je v rozpore so Zmluvou alebo Hlavnou zmluvou.
  3. Prevádzkovateľ je oprávnený kedykoľvek overovať či Dodávateľ dodržiava Zákon, vykonávacie predpisy a či koná v súlade so Zmluvu, a to spôsobom, aby takéto kontroly nezasahovali nad nevyhnutne nutnú mieru do činnosti Dodávateľa. Tieto kontroly je Prevádzkovateľ oprávnený vykonávať aj v priestoroch Dodávateľa nahliadaním do príslušnej dokumentácie a prístupom do sietí a informačných systémov prevádzkovaných Dodávateľom a využívaných na výkon činností pri Plnení Hlavnej zmluvy. Prevádzkovateľ je oprávnený výsledky takýchto kontrol zaznamenávať a dokumentovať. Prevádzkovateľ môže takéto kontroly vykonávať sám, alebo ich vykonaním poveriť ním určenú tretiu osobu. Náklady na kontrolu znáša každá Zmluvná strana samostatne.
  4. Prevádzkovateľ je oprávnený kedykoľvek požadovať od Dodávateľa preukázanie plnenia jeho povinností vrátane splnenia všetkých podmienok a požiadaviek podľa Zákona, vykonávacích predpisov a Zmluvy.
  5. Dodávateľ je najmä povinný:

1. na základe výzvy Prevádzkovateľa kedykoľvek v priebehu Plnenia Hlavnej zmluvy preukázať plnenie povinností vrátane splnenia všetkých podmienok a požiadaviek podľa Zákona, vykonávacích predpisov a Zmluvy,
2. v rámci vykonávania kontrol alebo auditov poskytovať Prevádzkovateľovi alebo ním poverenej tretej osobe potrebné informácie, podklady, a ďalšiu súčinnosť a náležite s ním spolupracovať,
3. poskytnúť riadne a včas všetky jemu dostupné informácie, podklady a požadovanú súčinnosť v prípade kontroly alebo auditu vykonávaného certifikovaným audítorom v oblasti kybernetickej bezpečnosti alebo Úradom a v celom rozsahu s nimi spolupracovať,
4. bez zbytočného odkladu, najneskôr však v lehote stanovenej Prevádzkovateľom, zjednať nápravu v prípade, ak Prevádzkovateľ zistí, že Dodávateľ porušuje alebo neplní svoje povinnosti vyplývajúce mu zo Zákona, vykonávacích predpisov a ďalších všeobecne záväzných právnych predpisov alebo nepostupuje v súlade so Zmluvou.
5. Dodávateľ je povinný informovať Prevádzkovateľa, ak je pravdepodobné, že uplatňované Bezpečnostné politiky alebo prijaté Bezpečnostné opatrenia nemusia byť z hľadiska požiadaviek Zákona alebo vykonávacích predpisov dostatočné.

**Čl. VI**

**Súčinnosť Dodávateľa pri plnení povinností Prevádzkovateľa**

* 1. Dodávateľ je povinný bezodkladne informovať Prevádzkovateľa o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení. Dodávateľ je povinný informovať o kybernetických bezpečnostných incidentoch a o všetkých skutočnostiach, ktoré majú vplyv na zabezpečenie kybernetickej bezpečnosti podľa predchádzajúcej vety elektronicky a zároveň telefonicky na kontakty pre komunikáciu o incidentoch uvedené v záhlaví tejto Zmluvy a kontaktnej osobe zodpovednej za oblasť kybernetickej bezpečnosti.

Správa musí obsahovať minimálne tieto informácie: (i) popis kybernetického bezpečnostného incidentu / všetkých skutočností ovplyvňujúcich kybernetickú bezpečnosť, (ii) typ kybernetického bezpečnostného incidentu, (iii) časové údaje o zistení a výskyte incidentu / skutočností ovplyvňujúcich kybernetickú bezpečnosť, (iv) dotknuté aktíva / služby, (v) informáciu o tom, či bol incident nahlásený úradu (áno - nie), (vi) spôsob odstránenia incidentu, (vii) popis navrhovaných opatrení na zabránenie opakovania incidentu.

* 1. Dodávateľ je povinný poskytnúť Prevádzkovateľovi všetky jemu dostupné informácie, podklady, a ako aj ďalšiu možnú súčinnosť, ktorá je potrebná za účelom plnenia povinnosti Prevádzkovateľa:

1. prijať bezpečnostnú dokumentáciu a udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu,
2. riešiť kybernetický bezpečnostný incident na základe rozhodnutia Úradu podľa príslušného ustanovenia Zákona, vykonať reaktívne opatrenie na základe rozhodnutia Úradu podľa príslušného ustanovenia Zákona alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa príslušného ustanovenia Zákona,
3. predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa príslušného ustanovenia Zákona,
4. bezodkladne hlásiť závažný kybernetický bezpečnostný incident (nahlásiť závažný kybernetický bezpečnostný incident podľa príslušného ustanovenia Zákona alebo odoslať neúplné hlásenie podľa príslušného ustanovenia Zákona),
5. spolupracovať s Úradom a Ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
6. v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
7. 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,
8. poskytnúť Úradu v prípade výkonu kontroly požadovanú súčinnosť,
9. prijať na základe výsledku kontroly opatrenia na odstránenie zistených nedostatkov a príčin ich vzniku a predložiť ich Úradu,
10. predložiť Úradu písomnú správu o splnení opatrení prijatých na odstránenie zistených nedostatkov,
11. preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia Prevádzkovateľa do registra prevádzkovateľov základnej služby,
12. preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa vykonávacích predpisov, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale,
13. predložiť Úradu záverečnú správu o výsledkoch auditu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu,
14. vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu,
15. a iné prípadné povinnosti ako vyplývajú zo Zákona a vykonávacích predpisov.
    1. V prípade, ak je poskytnutie informácií, podkladov alebo súčinnosti zo strany Dodávateľa pre splnenie povinnosti Prevádzkovateľa podľa bodu 6.2 písm. a) až o) nevyhnutné, je Dodávateľ povinný konať podľa pokynov, ktoré mu Prevádzkovateľ za tým účelom preukázateľne vydal.
    2. Informácie, podklady a ďalšie skutočnosti, ktorých hlásenie alebo predloženie je Prevádzkovateľom požadované na účely plnenia jeho povinností podľa bodu 6.2 písm. a) až o) bude Dodávateľ Prevádzkovateľovi poskytovať spôsobom a vo forme dohodnutej v bode 11.3.
    3. Dodávateľ je povinný:
16. bezodkladne hlásiť Prevádzkovateľovi každý kybernetický bezpečnostný incident a informovať ho o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
17. v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
18. neodkladne reagovať na informáciu o vzniknutom kybernetickom bezpečnostnom incidente a pri riešení kybernetického bezpečnostného incidentu prijať také opatrenia, aby sa minimalizovali negatívne dopady vzniknutého incidentu,
19. po nahlásení riešiť kybernetický bezpečnostný incident v súlade s pokynmi Prevádzkovateľa.

**Článok VII**

**Dôvernosť poskytnutých informácií**

* 1. Dodávateľ je povinný chrániť všetky informácie poskytnuté Prevádzkovateľom a zachovávať o nich mlčanlivosť. Povinnosť mlčanlivosti trvá aj po ukončení Hlavnej zmluvy.
  2. Povinnosť Dodávateľa zachovávať mlčanlivosť alebo dôvernosť informácií, ak bola založená na základe inej zmluvy uzavretej s Prevádzkovateľom alebo uložená osobitným predpisom, nie je týmto dotknutá a zostáva zachovaná.
  3. Dodávateľ nesmie informácie získané pri Plnení Hlavnej zmluvy použiť pre iné účely, než výslovne stanovuje Zmluva alebo Hlavná zmluva. Tieto informácie nie je oprávnený poskytnúť tretím stranám bez predchádzajúceho písomného súhlasu Prevádzkovateľa, s výnimkou prípadov, kedy je také poskytnutie informácií vyžadované všeobecne záväznými právnymi predpismi. V takom prípade sa Dodávateľ zaväzuje o tejto skutočnosti Prevádzkovateľa informovať, ak to nie je v rozpore s týmito právnymi predpismi alebo sa jedná o poskytnutie informácií schváleným Subdodávateľom, ak títo potrebujú mať k uvedeným informáciám prístup pre účely Plnenia Hlavnej zmluvy. Bez predchádzajúceho súhlasu Prevádzkovateľa si dodávateľ nesmie zhotovovať žiadne kópie alebo duplikáty informácií; to neplatí pre zálohovanie za účelom zabezpečenia Plnenia Hlavnej zmluvy.
  4. Dodávateľ je povinný zaviazať mlčanlivosťou všetky osoby zúčastnené na predmete Plnenia Hlavnej zmluvy tým, že zabezpečí, aby sa tieto osoby písomne zaviazali k zachovávaniu mlčanlivosti o skutočnostiach, o ktorých sa dozvedeli v súvislosti s plnením úloh podľa Hlavnej zmluvy alebo Zákona alebo vykonávacích predpisov a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť podľa predchádzajúcej vety trvá aj po skončení pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru. Tým nie sú dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

**Článok VIII**

**Subdodávatelia**

* 1. Ďalšieho dodávateľa, ktorý bude namiesto Dodávateľa úplne alebo čiastočne zabezpečovať Plnenie Hlavnej zmluvy (ďalej len „**Subdodávateľ**“), smie Dodávateľ zapojiť len s predchádzajúcim písomným súhlasom Prevádzkovateľa. Pri Plnení Hlavnej zmluvy Subdodávateľom má Dodávateľ voči Prevádzkovateľovi zodpovednosť, akoby Plnenie Hlavnej zmluvy vykonával sám.
  2. Prevádzkovateľ týmto súhlasí so zapojením Subdodávateľov uvedených v príslušnej prílohe Hlavnej Zmluvy, a to na vykonávanie činností pri Plnení Hlavnej Zmluvy namiesto Dodávateľa za podmienok v nej uvedených.
  3. Dodávateľ je povinný uložiť každému Subdodávateľovi rovnaké povinnosti ako má Dodávateľ podľa tejto Zmluvy a zároveň v celom rozsah zodpovedá za ich plnenie zo strany Subdodávateľa.
  4. Dodávateľ je povinný pred zapojením každého Subdodávateľa a následne v pravidelných intervaloch vykonávať kontroly u Subdodávateľov za účelom preverenia, či Subdodávateľ tieto povinnosti dodržiavajú a najmä, či dodržiava Bezpečnostné politiky a či postupuje v súlade s Bezpečnostnými opatreniami. Výsledky takých kontrol musia byť písomne zdokumentované a na požiadanie predložené Prevádzkovateľovi.
  5. Dodávateľ je povinný zaistiť v jeho zmluve so Subdodávateľom, že Prevádzkovateľ bude mať rovnaké práva kontroly nad Subdodávateľom, ako má Prevádzkovateľ nad samotným Dodávateľom bez toho, aby tým bola dotknutá zodpovednosť Dodávateľa za Subdodávateľa. Dodávateľ sa zaväzuje, že poskytne Prevádzkovateľovi na jeho žiadosť informácie o obsahu jeho zmluvy so Subdodávateľom, ktoré sú nevyhnutné na oboznámenie sa s povinnosťami Subdodávateľa vo vzťahu k zabezpečeniu kybernetickej bezpečnosti.

**Článok IX**

**TrvaniE Zmluvy**

* 1. Zmluva sa uzatvára na dobu trvania Hlavnej zmluvy. Zánik Hlavnej zmluvy spôsobuje zánik Zmluvy, a to s účinkom súčasného zrušenia oboch zmlúv. Ak však po ukončení Hlavnej zmluvy pretrvávajú určité práva a povinností Zmluvných strán súvisiace s poskytovaním Plnením Hlavnej zmluvy (ako napríklad nedokončené objednávky, záručný alebo pozáručný servis a pod.), Zmluva nezaniká a Zmluvné strany sú povinné postupovať a plniť všetky povinnosti podľa Zmluvy až do úplného ukončenia všetkých činností realizovaných na základe Hlavnej zmluvy.
  2. Zmluvné strany sa dohodli, že ktorákoľvek zmluvná strana môže od Zmluvy odstúpiť z dôvodu jej podstatného porušenia druhou Zmluvnou stranou. Odstúpením Zmluva zaniká dňom, keď je odstúpenie doručené druhej Zmluvnej strane. Zánik Hlavnej Zmluvy v dôsledku zániku Zmluvy nastane výlučne v prípade zrušenia Zmluvy odstúpením Prevádzkovateľa z dôvodov podľa bodu 9.3.
  3. Za podstatné porušenia tejto Zmluvy Dodávateľom sa považuje najmä: (i) nedodržiavanie Bezpečnostných politík, (ii) neprijatie alebo nedodržanie Bezpečnostných opatrení, (iii) neinformovanie Prevádzkovateľa o kybernetickom bezpečnostnom incidente alebo neposkytnutie súčinnosti pri jeho riešení, (iv) neoznámenie všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti Prevádzkovateľovi (v) neposkytnutie požadovanej informácie, podkladu alebo ďalšej možnej súčinnosti Prevádzkovateľovi na účely plnenia jeho zákonných povinností, (vi) nekonanie alebo konanie v rozpore s pokynom Prevádzkovateľa, (vii), marenie alebo sťaženie výkonu kontroly alebo auditu čiastočne alebo celkovo, (viii) porušenie povinnosti zachovávať mlčanlivosť alebo dôvernosť informácií, (ix) zapojenie vopred neschváleného Subdodávateľa v akomkoľvek rozsahu alebo (x) ak sa porušenia uvedeného v predchádzajúcich bodoch (i) až (ix) dopustí Subdodávateľ Dodávateľa.
  4. Zmluvné strany sa ďalej dohodli, že Prevádzkovateľ je oprávnený odstúpiť od Hlavnej zmluvy a tejto Zmluvy aj v prípade, ak štátny orgán v zmysle príslušných ustanovení Zákona vydá rozhodnutie, ktorým zakáže alebo obmedzí používanie produktu, procesu alebo služby a produkt, proces alebo služba uvedená(ý) v rozhodnutí je predmetom dodávky na základe Hlavnej zmluvy alebo ak sa zákaz alebo obmedzenie uvedené v rozhodnutí týka priamo používania Dodávateľa ako tretej strany; Prevádzkovateľ je v takom prípade oprávnený podľa vlastného uváženia odstúpiť od celého rozsahu alebo aj len časti Hlavnej zmluvy a kedykoľvek bez ohľadu na čas/lehotu uvedenú v rozhodnutí od kedy sa zákaz alebo obmedzenie má uplatniť.

**Článok X**

**Zodpovednosť a sankcie**

* 1. Bez ohľadu na akékoľvek iné dojednania medzi zmluvnými stranami, Dodávateľ zodpovedá v celom rozsahu za nesplnenie alebo porušenie ktorejkoľvek povinnosti vyplývajúcej z tejto Zmluvy, vrátane prípadu, ak sa tohto porušenia dopustil jeho Subdodávateľ. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie alebo porušenie jeho povinností vyplývajúcich z tejto Zmluvy ohrozuje kybernetickú bezpečnosť Prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, Dodávateľ zodpovedá v celom rozsahu za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto Zmluvy, Zákona alebo Vykonávacích predpisov a za dôsledky a škodu vzniknutú Prevádzkovateľovi alebo akejkoľvek tretej osobe v dôsledku kybernetických incidentov, ktoré by pri riadnom a včasnom plnení povinností podľa tejto Zmluvy nevznikli alebo by sa prejavili v menšej intenzite a rozsahu. Prevádzkovateľ má voči Dodávateľovi nárok na náhradu škody, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov Dodávateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka.
  2. Dodávateľ prehlasuje, že za účelom plnenia Hlavnej zmluvy s odbornou starostlivosťou vypracoval a implementoval koncepčné riadenie nepretržitej dostupnosti a prevádzky obchodných a procesných činností - *Biznis kontinuity manažment*, skutočnosť ktorú preukázal Objednávateľovi príslušnou dokumentáciou, najmä vypracovaným a riadne implementovaným Biznis continuity plánom a Plánom obnovy IT infraštruktúry (*Disaster Recovery Plan*) (ďalej len „**BCM**“ alebo aj ako „**BC Plány**“), pričom Dodávateľ sa zaväzuje, že:

1. bude BC Plány počas celej doby plnenia Predmetu Zmluvy riadne dodržiavať, pravidelne ich revidovať, testovať a vyhotovovať o týchto činnostiach príslušné záznamy;
2. umožní Objednávateľovi kedykoľvek na jeho požiadanie kontrolu vypracovaných BC Plánov a/alebo záznamov o revíziách týchto plánov a/alebo protokolov z testovania týchto plánov, a najmä poskytne Objednávateľovi pre účely výkonu kontroly podľa predchádzajúceho písm. a) tohto bodu Zmluvy všetku potrebnú súčinnosť a dokumentáciu pre účely preukázania splnenia povinnosti Dodávateľa podľa tohto bodu 10.2. Zmluvy.
   1. Ak Dodávateľ alebo jeho Subdodávateľ nesplní alebo poruší niektorú zo svojich povinností vyplývajúcich z tejto Zmluvy, osobitne, nie však výlučne povinnosť:
3. dodržiavať Bezpečnostné politiky podľa bodu 4.1,
4. prijať alebo dodržať Bezpečnostné opatrenia podľa bodu 4.3,
5. informovať Prevádzkovateľa o kybernetickom incidente podľa bodu 6.1,
6. chrániť informácie a zachovávať o nich mlčanlivosť podľa bodu 7.1, alebo
7. zapojiť Subdodávateľa len so súhlasom Prevádzkovateľa podľa bodu 8.1,

je povinný zaplatiť Prevádzkovateľovi zmluvnú pokutu výške       EUR (slovom       eur) za každé jednotlivé porušenie.

* 1. Ak Dodávateľ alebo jeho Subdodávateľ nesplní alebo poruší niektorú zo svojich povinností vyplývajúcich z tejto Zmluvy, osobitne, nie však výlučne povinnosť:

1. nakladať s informáciami po skončení Hlavnej zmluvy podľa bodu 4.6,
2. postupovať podľa pokynov prevádzkovateľa podľa bodu 5.2,
3. zjednať nápravu podľa bodu 5.5,
4. poskytnúť informácie, podklady a ďalšiu možnú súčinnosť za účelom plnenia povinnosti Prevádzkovateľa podľa bodu 6.2,
5. použiť informácie len na účely podľa Zmluvy alebo Hlavnej zmluvy podľa bodu 7.3,
6. zaviazať mlčanlivosťou osoby zúčastnené na plnení Hlavnej zmluvy podľa bodu 7.4,
7. poskytnúť súčinnosť pri výkone kontroly alebo auditu podľa bodu 5.5, alebo
8. poruší zákaz poskytnúť informácie tretím stranám bez súhlasu Prevádzkovateľa podľa bodu 7.3,

je povinný zaplatiť Prevádzkovateľovi zmluvnú pokutu výške       EUR (slovom       eur) za každé jednotlivé porušenie.

* 1. Ak Dodávateľ alebo jeho Subdodávateľ nesplní alebo poruší niektorú zo svojich povinností vyplývajúcich z tejto Zmluvy, osobitne, nie však výlučne povinnosť:

1. konať podľa pokynov Prevádzkovateľa podľa bodu 6.3,
2. uložiť Subdodávateľovi rovnaké povinnosti ako má Dodávateľ podľa Zmluvy podľa bodu 8.3,
3. vykonávať kontroly Subdodávateľa podľa bodu 8.4,
4. zaistiť rovnaké práva kontroly nad Subdodávateľom ako má Prevádzkovateľ nad Dodávateľom podľa bodu 8.5, alebo
5. opakovane nesplní povinnosť oznámiť zmenu v personálnom obsadení pracovných rolí podľa bod 1.3,

je povinný zaplatiť Prevádzkovateľovi zmluvnú pokutu výške       EUR (slovom       eur) za každé jednotlivé porušenie.

* 1. Ak ani napriek písomnej výzve Prevádzkovateľa v dodatočnej lehote určenej v tejto výzve Dodávateľ nenapraví porušenie alebo nesplnenie niektorej z jeho povinností

1. umožniť výkon kontroly podľa bodu 5.3,
2. poskytnúť informáciu o obsahu jeho zmluvy so Subdodávateľom podľa bodu 8.5, alebo
3. najneskôr do ukončenia Hlavnej zmluvy naložiť licenciami, právami alebo súhlasmi podľa bodu 11.1,

je povinný zaplatiť Prevádzkovateľovi zmluvnú pokutu výške       EUR (slovom       eur) za každé jednotlivé porušenie.

* 1. V prípade, ak Dodávateľ poruší ktorúkoľvek povinnosť súvisiacu s vypracovaním BC Plánov v zmysle špecifikácie podľa bodu 10.2. tejto Zmluvy, najmä ak

1. Dodávateľ nedodržiava, nereviduje alebo netestuje BC Plány a/alebo nepreukáže Objednávateľovi záznamy o týchto činnostiach vedené počas celej doby plnenia predmetu Hlavnej zmluvy; a/alebo
2. BC Plány Dodávateľa nie sú riadne implementované alebo vykazujú vážne nedostatky; a/alebo
3. Dodávateľ neposkytne Prevádzkovateľovi na základe jeho písomnej požiadavky súčinnosť pre účely výkonu kontroly plnenia povinností súvisiacich s BC Plánmi,

Prevádzkovateľ je oprávnený uplatniť si u Dodávateľa nárok na zaplatenie zmluvnej pokuty vo výške 5 000,- EUR (slovom: päťtisíc eur) za každý jednotlivý prípad porušenia ktorejkoľvek povinnosti Dodávateľa uvedenej v tomto bode Zmluvy, a to aj opakovane; právo Objednávateľa na odstúpenie od Hlavnej zmluvy tým nie je dotknuté.

* 1. Prevádzkovateľ je oprávnený, nie však povinný, požadovať od Dodávateľa úhradu zmluvnej pokuty po vzniku nároku na jej zaplatenie, a to buď v celej výške alebo len v určitej jej časti určenej podľa svojej vlastnej úvahy.
  2. Nárok na náhradu škody zostáva zachovaný popri nároku na zmluvnú pokutu a preto uplatnenie nároku na zmluvnú pokutu nemá vplyv na povinnosť Dodávateľa nahradiť Prevádzkovateľovi škodu vzniknutú nesplnením alebo porušením jeho povinností podľa tejto Zmluvy, a to v plnej výške vrátane sumy prevyšujúcej výšku uplatnenej zmluvnej pokuty.
  3. Za škodu sa za každých okolností bude považovať uloženie sankcie zo strany Úradu Prevádzkovateľovi z dôvodu nesplnenia alebo porušenia povinností vyplývajúcej zo Zákona, vykonávacieho predpisu alebo iného všeobecne záväzného právneho predpisu, ak toto porušenie je spôsobené konaním, resp. nekonaním Dodávateľa alebo jeho Subdodávateľa alebo uloženie inej finančnej povinnosti právoplatným rozhodnutím iného orgánu verejnej moci (napr. súdu) vo veci týkajúcej sa porušenia alebo nesplnenia povinnosti v oblasti zabezpečenia kybernetickej bezpečnosti Dodávateľa alebo jeho Subdodávateľa.

**Článok XI**

**Spoločné a záverečné ustanovenia**

* 1. Dodávateľ sa zaväzuje, že najneskôr ku dňu skončenia Hlavnej zmluvy udelí, poskytne, prevedie alebo postúpi všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na Prevádzkovateľa; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu a to po dobu päť rokov po ukončení Hlavnej zmluvy.
  2. Ak je Hlavnou zmluvou zmluva rámcová, vzťahujú sa ustanovenia tejto Zmluvy aj na všetky čiastkové zmluvy zavretej na základe Hlavnej zmluvy alebo objednávky k Hlavnej zmluve. Zmluvné strany potvrdzujú, že aj v období pred uzavretím tejto Zmluvy mali na zreteli povinnosti podľa Zákona a  vykonávacích predpisov (najmä plnenie notifikačných povinností a plnenie bezpečnostných opatrení) a tieto povinnosti v záujme zabezpečenia kybernetickej bezpečnosti plnili.
  3. Zmluvné strany sa dohodli, že ich vzájomná komunikácia pri plnení Zmluvy vrátane hlásenia všetkých informácií majúcich vplyv na Zmluvu vyžaduje písomnú formu, ktorú považujú za zachovanú aj v prípade elektronickej komunikácie prostredníctvom elektronickej pošty (e-mailu). Všetky informácie, údaje, oznámenia, hlásenia, pokyny, podklady a akékoľvek iné skutočnosti ktoré by mohli mať vplyv na plnenie Zmluvy, budú doručované v listinnej podobe poštou, kuriérom, osobne na adresu sídla danej Zmluvnej strany alebo jej príslušnej prevádzkarne alebo elektronickými prostriedkami na e-mailové adresy uvedené v záhlaví tejto Zmluvy Kontaktným osobám Zmluvných strán. Úkony zmluvných strán urobené v podobách uvedených podľa predchádzajúcej vety sa považujú za úkony vykonané v písomne zdokumentovanej forme.
  4. Pre prípad, že by sa ktorékoľvek ustanovenie tejto Zmluvy ukázalo byť neplatné, neúčinné, či nevykonateľné, Zmluvné strany sa dohodli, že ho bez zbytočného odkladu po zistení tejto skutočnosti nahradia ustanovením, ktoré bude najlepšie zodpovedať obsahu a účelu pôvodného ustanovenia.
  5. Zmluva je vyhotovená v troch rovnopisoch, každý s platnosťou originálu, pričom Dodávateľ dostane jedno vyhotovenie a Prevádzkovateľ dve vyhotovenia Zmluvy.
  6. Zmluvu možno meniť, s výnimkou ako je dohodnuté v bode 4.4 tejto Zmluvy, len formou písomného dodatku podpísaného oboma Zmluvnými stranami, ktorý sa musí uzatvoriť v listinnej podobe alebo elektronickej podobe. Riadne uzatvorený dodatok sa stáva neoddeliteľnou súčasťou Zmluvy.
  7. Zmluvné vzťahy vyplývajúce zo Zmluvy sa riadia slovenským právom. Na riešenie prípadných sporov zo Zmluvy sú príslušné slovenské súdy.
  8. Zmluva nadobúda platnosť a účinnosť jej podpisom obomi Zmluvnými stranami.
  9. Zmluvné strany vyhlasujú, že si Zmluvu pred jej podpísaním prečítali, jej obsahu porozu­meli a na znak toho, že obsah Zmluvy zodpovedá ich sku­točnej a slobodnej vôli, ju podpísali.
  10. Zmluva bude zaradená do evidencie všetkých uzatvorených zmlúv s treťou stranou, ktorá tvorí súčasť bezpečnostnej dokumentácie Prevádzkovateľa podľa § 9 ods. 5 Vyhlášky Národného bezpečnostného úradu č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
  11. Obsah nasledovných Príloh predstavuje neoddeliteľnú súčasť obsahu záväzkového vzťahu založeného Zmluvou:
* Príloha č. 1: Konkrétny rozsah činností Dodávateľa
* Príloha č. 2: Zoznam pracovných rolí Dodávateľa
* Príloha č. 3: Zoznam bezpečnostných politík a / alebo požiadaviek Prevádzkovateľa
* Príloha č. 4: Minimálny rozsah a špecifikácia bezpečnostných opatrení pre Dodávateľa
  1. V prípade rozporov medzi ustanoveniami tejto Zmluvy a Hlavnej zmluvy sa vo vzťahu ku kybernetickej bezpečnosti uplatnia prednostne ustanovenia tejto Zmluvy a v prípade rozporov medzi telom Zmluvy a jej prílohami majú prednosť ustanovenia tela Zmluvy pred jej prílohami.

V Bratislave, dňa \_\_\_\_\_\_\_\_\_\_ V \_\_\_\_\_\_\_\_\_\_\_\_\_\_ dňa \_\_\_\_\_\_\_\_\_\_

**Za Prevádzkovateľa: Za Dodávateľa:**

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Bratislavská vodárenská spoločnosť, a.s. | Názov spoločnosti |
| Meno, priezvisko, funkcia | Meno, priezvisko, funkcia |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Bratislavská vodárenská spoločnosť, a.s. | Názov spoločnosti |
| Meno, priezvisko, funkcia | Meno, priezvisko, funkcia |

Príloha č. 1 Zmluvy o bezpečnostných opatreniach a notifikačných povinnostiach - Konkrétny rozsah činností Dodávateľa

Ak je medzi zmluvnými stranami uzavretých viac Hlavných zmlúv, je pre každú takú zmluvu uzavretá separátna príloha č. 1, ktorá je odlišovaná iba využitím písmen abecedy.

**Hlavná zmluva**

ZMLUVA O DIELO A O POSKYTOVANÍ SLUŽIEB č. .../.../.../BVS zo dňa

**Rozsah primárnych činností Dodávateľa na základe Hlavnej zmluvy**

Analýza východiskového stavu IT prostredia Prevádzkovateľa a vypracovanie návrhu jeho budúceho riešenia, zabezpečenie migrácie vybratých služieb z existujúceho on-premise prostredia na cloudové riešenie Microsoft 365 vrátane modernizácie používateľského prostredia, zabezpečenia procesov súvisiacich s migráciou a integráciou vybraných dát s existujúcimi on-premise systémami, poskytovanie služieb SLA vo forme reaktívnej, proaktívnej a nadštandardnej podpory a ďalších služieb.

**Prevádzkovateľ**

**Bratislavská vodárenská spoločnosť, a.s.**, so sídlom Prešovská 48, 826 46 Bratislava, zapísaná v Obchodnom registri Mestského súdu Bratislava III oddiel: Sa, vložka č.: 3080/B

**Dodávateľ**

Identifikačné údajedoplní úspešný uchádzač, je spoločnosťou, ktorej predmetom podnikania je /predmetom činnosti je      .

Príloha č. 2 Zmluvy o bezpečnostných opatreniach a notifikačných povinnostiach - Zoznam pracovných rolí Dodávateľa

|  |  |  |
| --- | --- | --- |
| P.č. | Pracovná pozícia | Meno a priezvisko |
| 1. | doplní úspešný uchádzač | doplní úspešný uchádzač |
| 2. | doplní úspešný uchádzač | doplní úspešný uchádzač |
| 3. |  |  |

Príloha č. 3 Zmluvy o bezpečnostných opatreniach a notifikačných povinnostiach - Zoznam bezpečnostných politík a /alebo bezpečnostných požiadaviek Prevádzkovateľa

**Bratislavská vodárenská spoločnosť, a.s.**, so sídlom Prešovská 48, 826 46 Bratislava, zapísaná v Obchodnom registri Mestského súdu Bratislava III oddiel: Sa, vložka č.: 3080/B (ďalej aj „**PREVÁDZKOVATEĽ**“) ako prevádzkovateľ základnej služby prijala Bezpečnostnú stratégiu informačnej a kybernetickej bezpečnosti, ktorá obsahuje základné princípy a ciele, prostredníctvom ktorých PREVÁDZKOVATEĽ garantuje dostupnú a udržateľnú úroveň bezpečnosti pri plnení svojich úloh a určuje základný rámec, rozsah, bezpečnostné potreby a organizáciu bezpečnosti v rámci spoločnosti PREVÁDZKOVATEĽA.

Zoznam poskytnutých bezpečnostných politík:

|  |  |
| --- | --- |
| P.č. | Názov |
| 1. | Minimálny rozsah a špecifikácia bezpečnostných opatrení (Príloha č. 4 Zmluvy) |
| 2. | 08\_P2\_Stratégia informačnej bezpečnosti |
| 3. | 06\_P2\_Bezpečnostné politiky |
| 4. | 05\_P2\_Klasifikácia\_informácií\_v\_IS |
| 5. |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Príloha č. 4 Zmluvy o bezpečnostných opatreniach a notifikačných povinnostiach - Minimálny rozsah a špecifikácia bezpečnostných opatrení

Posúdenie prijatia a dodržiavania organizačných a technických bezpečnostných opatrení je vykonávané pred uzavretím Hlavnej zmluvy. Úroveň plnenia a dodržiavania relevantných bezpečnostných opatrení je posudzovaná, preskúmateľná a pravidelne prehodnocovaná.

Minimálny rozsah a špecifikácia bezpečnostných opatrení, ktoré je Dodávateľ povinný prijať, dodržiavať, a s ktorými bol riadne oboznámený sú bližšie uvedené v samostatnom dokumente **Minimálny rozsah a špecifikácia bezpečnostných opatrení pre Dodávateľa**.