Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. : O2.1-20230016

uzatvorená v zmysle § 269 ods. 2 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov a v súlade so znením § 19 a nasl. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
(ďalej len „Zmluva")

medzi

Názov:	Mesto Banská Bystrica
Sídlo:	Československej armády 26, 974 01 Banská Bystrica
IČO:	00313271
Konajúci:	MUDr. Ján Nosko, primátor mesta
Bankové spojenie:	ČSOB, a.s., Banská Bystrica
IBAN:	SK7775000000004016795432

(„Prevádzkovateľ základnej služby" alebo aj „PZS")

a

Obchodné meno:	Slovanet, a. s.
Sídlo:	Záhradnícka 151, 821 08 Bratislava
IČO:	35 954 612
Konajúci:	Ing. Peter Máčaj, predseda predstavenstva, Ing. Peter Tomášek, člen predstavenstva
Konanie menom spoločnosti:	V mene spoločnosti konajú a podpisujú vždy dvaja členovia predstavenstva spoločne. Za spoločnosť podpisujú tak, že k obchodnému menu spoločnosti pripoja svoje meno a svoj podpis.
Bankové spojenie:	
IBAN:	
Registrácia:	Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel: Sa, vložka č.: 3692/B.

(„Dodávateľ")

(spoločne ako „Zmluvné strany")

I. Úvodné ustanovenia

1. Mesto Banská Bystrica je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len " ZoKB").
2. Zmluvné strany uzatvárajú túto Zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na Zmluvu o poskytovaní verejných služieb č. VPN16050243901, uzatvorenú medzi Zmluvnými stranami dňa 31.08.2016, ktorá nadobudla účinnosť dňa 01.09.2016 (ďalej len „Prevádzková zmluva").
3. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie

požiadaviek podľa tejto Zmluvy v súvislosti s plneniami poskytovanými Dodávateľom na základe Prevádzkovej zmluvy.

4. Pre účely tejto Zmluvy sa Zmluvné strany dohodli, že pojmy uvedené v tejto Zmluve sa budú vykladať tak, ako ich stanovuje ZoKB a jeho vykonávacie predpisy (Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ďalej len „vyhláška NBÚ").
5. Zmluvné strany sa dohodli, že Dodávateľ sa zaväzuje plniť bezpečnostné opatrenia a notifikačné povinnosti podľa tejto Zmluvy iba vo vzťahu k plneniam poskytovaných Dodávateľom na základe a v rozsahu Prevádzkovej zmluvy a v rozsahu plnení vymedzených v tejto Zmluve. V prípade, ak činnosti prípadne povinnosti vyžadované touto Zmluvou cenovo prekročia bežný rámec starostlivosti garantovaný Dodávateľom na základe Prevádzkovej zmluvy, budú tieto realizované Dodávateľom až na základe Dodávateľom akceptovaných osobitných objednávok Prevádzkovateľa základnej služby v súlade s mechanizmami objednávania činností podľa Prevádzkovej zmluvy a v súlade s príslušnou ponukou vypracovanou Dodávateľom na základe žiadosti Prevádzkovateľa základnej služby v okamihu, keď bude zrejmé, že náklad realizácie požadovaných činností prípadne povinností presahuje bežný rámec starostlivosti garantovaný Prevádzkovou zmluvou.

II. Všeobecné požiadavky

1. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi základnej služby dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na tretie strany v zmysle § 19 ZoKB a vyhlášky NBÚ.
2. Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia Prevádzkovou zmluvou, ZoKB, vyhláškou NBÚ alebo inými právnymi predpismi vydanými v súlade so ZoKB.
3. Dodávateľ je povinný dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby, s ktorými ho Prevádzkovateľ základnej služby preukázateľne oboznámil. Dodávateľ vyhlasuje, že súhlasí s týmito bezpečnostnými politikami Prevádzkovateľa základnej služby. Dodávateľ berie na vedomie, že bezpečnostné politiky Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa základnej služby a aktuálnym hrozbám s ohľadom na Dodávateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby. Akákoľvek zmena týkajúca sa bezpečnostných politík Prevádzkovateľa základnej služby bude oznámená Dodávateľovi v zmysle článku VI. tejto Zmluvy.
4. Dodávateľ je povinný v súvislosti s poskytovaním služieb podľa Prevádzkovej zmluvy dodržiavať a prijímať bezpečnostné opatrenia v oblasti kybernetickej bezpečnosti a súhlasí s rozsahom a špecifikáciou bezpečnostných opatrení definovaných v čl. III tejto Zmluvy.
5. Dodávateľ je povinný dodržiavať a prijímať iba tie bezpečnostné opatrenia, ktoré je potrebné vykonať v súvislosti so službami poskytovanými Dodávateľom na základe Prevádzkovej zmluvy, zohľadňujúc charakter a rozsah poskytovaných služieb.
6. Dodávateľ je povinný dodržiavať a prijímať iba tie bezpečnostné opatrenia, ktoré sú relevantné pre informačné systémy a siete patriace Dodávateľovi, ktoré Dodávateľ priamo využíva pri poskytovaní služieb Prevádzkovateľovi základnej služby a iba tie bezpečnostné opatrenia, ktoré sú relevantné pre informačné systémy a siete Prevádzkovateľa základnej služby, a to v rozsahu činností-vyplývajúcich z predmetu Prevádzkovej zmluvy. Pre ostatné opatrenia je Dodávateľ povinný pri výkone svojich činností dodržiavať princípy, ktoré sú týmito popísanými opatreniami požadované.

III. Špecifikácia a rozsah bezpečnostných opatrení a činností

1. Rozsah činností, ktoré Dodávateľ vykonáva pre Prevádzkovateľa základnej služby je definovaný v Prevádzkovej zmluve a tejto Zmluve.
2. Dodávateľ bezodkladne poskytne Prevádzkovateľovi základnej služby najneskôr v deň podpisu tejto Zmluvy zoznam pracovných rolí, ktoré sú poverené na výkon činnosti v súvislosti s plnením tejto Zmluvy. Každú zmenu v personálnom obsadení pracovných rolí je Dodávateľ povinný Prevádzkovateľovi základnej služby vopred písomne oznámiť v zmysle článku VI. tejto Zmluvy.
3. Pre oblasť technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 9 vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov a sietí prostredníctvom opatrení definovaných v nasledovných bodoch:
   - Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí.
   - Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí.
   - Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.
4. Pre oblasť riadenia bezpečnosti sietí a informačných systémov, realizuje Dodávateľ opatrenia podľa § 10 vyhlášky NBÚ, prostredníctvom opatrení definovaných v nasledovných bodoch:
   - Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom.
   - Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
   - Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
   - Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete.
   - Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
   - Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
   - Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
   - Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.
   - Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
   - Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
   - Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.
   - Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.

- Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.
- Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do siete Prevádzkovateľa základnej služby.
- Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

5. Pre oblasť riadenia prístupov realizuje Dodávateľ opatrenia podľa § 12 vyhlášky NBÚ, prostredníctvom opatrení definovaných v nasledovných bodoch:
   - Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
   - Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb Prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
   - Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.
   - Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
   - Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
   - Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).
   - 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.
   - Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

6. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Dodávateľ opatrenia podľa § 14 vyhlášky NBÚ, najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na poskytovanie služieb Prevádzkovateľa základnej služby. To zahŕňa najmä prijatie opatrení definovaných v nasledovných bodoch:
   - Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Prevádzkovateľa základnej služby,

- Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
- Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetický bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.
- Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Prevádzkovateľa základnej služby.
- Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Prevádzkovateľom základnej služby.

7. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Dodávateľ opatrenia podľa § 15 vyhlášky NBÚ, najmä zaznamenáva činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú priamo využívané pri poskytovaní služieb Prevádzkovateľovi základnej služby.
8. Dodávateľ sa zaväzuje na plnenie tejto Zmluvy a bezpečnostných opatrení postupovať v súlade so schválenými normami upravujúcimi oblasť informačnej bezpečnosti a to najmä podľa STN ISO/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti) a vyhláškou NBÚ.

IV. Hlásenie kybernetických incidentov

1. Dodávateľ je povinný v súvislosti s poskytovaním služieb Prevádzkovateľovi základnej služby bezodkladne hlásiť a informovať Prevádzkovateľa základnej služby o každom svojom podozrení na kybernetický bezpečnostný incident (ďalej aj „incident") súvisiaci s poskytovaním služby Dodávateľom, ako aj o všetkých skutočnostiach majúcich negatívny vplyv na zabezpečovanie kybernetickej bezpečnosti prevádzkovanej základnej služby, a to prostredníctvom elektronickej pošty na kontaktnú adresu Prevádzkovateľa základnej služby uvedenú v čl. VI. tejto Zmluvy.
2. Hlásenie podozrenia o kybernetickom bezpečnostnom incidente musí obsahovať najmä informácie:
   a. o tom, kto hlási kybernetický bezpečnostný incident, a to:
      - identifikačné údaje a
      - kontaktné údaje,
   b. o kybernetickom bezpečnostnom incidente, a to:
      - časové údaje priebehu kybernetického bezpečnostného incidentu,
      - opis priebehu kybernetického bezpečnostného incidentu a
      - rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu,
   c. o službe zasiahnutej kybernetickým bezpečnostným incidentom, a to:
      - konkrétny popis všetkých zasiahnutých aktív a vplyv kybernetického bezpečnostného incidentu na poskytovanú službu,
   d. o riešení kybernetického bezpečnostného incidentu, a to:

- stav riešenia kybernetického bezpečnostného incidentu,
- vykonané nápravné opatrenia a
- popis následkov kybernetického bezpečnostného incidentu.

3. Pri riešení incidentov je Dodávateľ povinný spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získane z vlastnej činnosti podľa tejto Zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.
4. Dodávateľ je povinný v čase incidentu v rozsahu jeho oprávnení zabezpečiť dôkazy, ktoré budú slúžiť na objasnenie vzniku a riešenia kybernetického bezpečnostného incidentu.
5. Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu Dodávateľa o kybernetickom bezpečnostnom incidente, o ktorom sa dozvedel ako prvý a ktorý môže mať vplyv na plnenie tejto Zmluvy.

V. Mlčanlivosť a ochrana informácií

1. Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tejto Zmluvy dozvedel a ktoré nie sú verejne známe.
2. Dodávateľ je povinný písomne zaviazať všetky osoby, subdodávateľov a ich zamestnancov, ktoré sú zúčastnené na plnení tejto Zmluvy zachovávať mlčanlivosť v zmysle § 12 ods. 1 ZoKB.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje ZoKB.
4. Dodávateľ je povinný chrániť všetky informácie, ktoré mu boli poskytnuté Prevádzkovateľom základnej služby, a to pred ich neoprávneným vymazaním, zmenou alebo pred ich prezradením alebo poskytnutím neoprávnenej osobe.

VI. Pravidlá komunikácie a kontaktné osoby

1. Akákoľvek komunikácia a hlásenie informácii súvisiacich s plnením povinností vyplývajúcich zo ZoKB alebo majúcich vplyv na zabezpečenie kybernetickej bezpečnosti alebo plnenie tejto Zmluvy, musí byť realizovaná niektorou z nasledovných foriem: pošta, elektronická pošta, telefón alebo osobne, ak v tejto Zmluve nie je uvedené inak.
2. Zmluvné strany sa dohodli, že akékoľvek písomnosti týkajúce sa skončenia trvania tejto Zmluvy budú doručované len prostredníctvom pošty, osobne alebo kuriérnou službou, a to na adresu sídiel Zmluvných strán uvedených v tejto Zmluve, okrem prípadu ak odosielajúcej Zmluvnej strane adresát písomnosti oznámil novú adresu sídla. Súčasne sa Zmluvné strany dohodli, že tieto písomnosti si budú zasielať na vedomie aj elektronickou poštou na adresu uvedenú v kontaktných údajoch Zmluvných strán.
3. Zmluvné strany sa dohodli, že obsah komunikácie a hlásení informácií, ktoré boli realizované telefonicky alebo osobne si budú zmluvné strany bezodkladne zasielať aj elektronickou poštou na adresu uvedenú v kontaktných údajoch Zmluvných strán.
4. Zmluvné strany sa dohodli, že komunikácia vykonávaná elektronickou poštou sa bude riadiť nasledovnými pravidlami:
   a) elektronická pošta bude zasielaná pre oblasť hlásenia výhradne na adresy elektronickej pošty (e-mail) uvedené v tomto článku,
   b) elektronická pošta bude zasielaná v chránenej forme (napr. chránená heslom, chránená šifrovaním), v závislosti od dohody komunikujúcich strán a citlivosti informácií, ktoré sú obsahom komunikácie.
5. Kontaktné údaje Prevádzkovateľa základnej služby:
   1. Vedúci odboru informatizácie a digitalizácie, email: oit.ved@banskabystrica.sk, mobil: 0918 505 222
   2. Vedúci oddelenia prevádzky IT, email: oit-pit.ved@banskabystrica.sk, mobil: 0908 770 010

3. Manažér kybernetickej bezpečnosti, email:
   mobil:
6. Kontaktné údaje Dodávateľa:Ing.Jozef Priesol, PhD.,
   kybernetický incident.
7. Každú zmenu kontaktných údajov uvedených v tomto článku je jedna Zmluvná strana povinná bezodkladne oznámiť druhej Zmluvnej strane a to v preukázateľnej forme.

VII. Kontrolná činnosť a audit

1. Dodávateľ poskytne Prevádzkovateľovi základnej služby na jeho požiadanie informácie potrebné na preukázanie splnenia povinností vyplývajúcich z tejto Zmluvy, ZoKB a vyhlášky NBÚ s prihliadnutím na informácie dostupné Dodávateľovi.
2. Dodávateľ je povinný poskytnúť Prevádzkovateľovi základnej služby súčinnosť v rámci auditu prijatých bezpečnostných opatrení a kontroly zo strany Prevádzkovateľa základnej služby, Národnej jednotky CSIRT, vládnej jednotky CSIRT alebo subjektu, ktorého na vykonanie auditu poveril Prevádzkovateľ základnej služby.
3. Zmluvné strany sa dohodli, že Prevádzkovateľ základnej služby je oprávnený vykonať u Dodávateľa audit alebo kontrolu, zameranú na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy.
4. Prevádzkovateľ základnej služby je povinný informovať o termíne vykonania auditu alebo kontroly Dodávateľa oznámením zaslaným elektronickou poštou na kontakt uvedený v čl. VI. tejto zmluvy, a to minimálne 7 dní pred vykonaním auditu alebo kontroly. Dodávateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 dní odo dňa zaslania oznámenia. Pokiaľ Dodávateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.
5. Prípadné nedostatky zistené auditom a/alebo kontrolou je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 90 kalendárnych dní od zistenia toho ktorého nedostatku. O audite ako aj o kontrole bude spísaná zápisnica, ktorej obsah bude potvrdený podpisom Dodávateľa a osoby vykonávajúcej predmetnú činnosť, resp. povereným zamestnancom za tú ktorú stranu.
6. Prevádzkovateľ základnej služby môže audit alebo kontrolu realizovať sám alebo prostredníctvom tretej osoby; v prípade realizácie auditu alebo kontroly prostredníctvom tretej osoby, práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu alebo kontroly realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
7. Náklady, ktoré v súvislosti s auditom alebo kontrolou vzniknú osobe vykonávajúcej kontrolnú činnosť, znáša Prevádzkovateľ základnej služby. Dodávateľ poskytuje súčinnosť pri výkone auditu a kontroly bezodplatne, resp. prípadné náklady nad rámec štandardnej súčinnosti pri výkone auditu znáša Prevádzkovateľ základnej služby.

VIII. Zapojenie ďalšieho dodávateľa (Subdodávatelia)

1. Dodávateľ je povinný dodržiavať podmienky zapojenia ďalšieho dodávateľa (ďalej len „subdodávateľ") do poskytovania služieb tak, ako sú upravené v tejto Zmluve.
2. Dodávateľ informuje Prevádzkovateľa základnej služby o všetkých prvotných subdodávateľoch, ktorí sú zapojení do plnenia tejto Zmluvy a v súvislosti s ňou.
3. Dodávateľ je povinný vopred informovať Prevádzkovateľa základnej služby o zapojení nového subdodávateľa, a to prostredníctvom elektronickej pošty alebo písomne na kontakt Prevádzkovateľa základnej služby uvedený v čl. VI. tejto Zmluvy.
4. Dodávateľ nesmie poveriť nového subdodávateľa výkonom akýchkoľvek činností súvisiacich s plnením tejto Zmluvy bez predchádzajúceho informovania Prevádzkovateľa základnej služby.

5. Ak Dodávateľ zapojí do vykonávania činností spojených s poskytovaním služieb Prevádzkovateľovi základnej služby subdodávateľa, tomuto subdodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení a hlásenia kybernetických incidentov, ako sú ustanovené v tejto Zmluve.
6. Dodávateľ je povinný pri výbere subdodávateľa postupovať s odbornou starostlivosťou tak, aby bola zachovaná čo najvyššia kvalita poskytovaných činností a iných plnení podľa tejto Zmluvy, t. j. každý Dodávateľom navrhovaný subdodávateľ musí byť schopný vykonať činnosti a iné plnenia podľa tejto Zmluvy v minimálne rovnakej kvalite alebo kvalite lepšej ako Dodávateľ.
7. Zmluvné strany sa dohodli, že splnenie povinnosti informovania Prevádzkovateľa základnej služby o subdodávateľoch žiadnym spôsobom nezbavuje Dodávateľa povinností vyplývajúcich mu z tejto Zmluvy. Pre odstránenie pochybností zmluvné strany vyhlasujú, že Dodávateľ je povinný postupovať podľa tohto článku Zmluvy aj v prípade, ak v priebehu plnenia tejto Zmluvy a v súvislosti s ňou nepredložil Prevádzkovateľovi základnej služby žiadny zoznam subdodávateľov resp. tvrdil, že služby poskytne osobne a následne vznikla potreba poskytnúť služby subdodávateľom.
8. Dodávateľ zodpovedá za plnenie tejto Zmluvy prostredníctvom subdodávateľa tak, ako keby plnenie realizoval sám.

IX. Sankčné mechanizmy/Zodpovednosť za škodu

1. V prípade nedodržania akejkoľvek povinnosti alebo záväzkov Dodávateľa vyplývajúcich z tejto Zmluvy, ZoKB alebo vyhlášky NBÚ je Prevádzkovateľ základnej služby oprávnený Dodávateľa písomne vyzvať na nápravu porušovaných povinností. V prípade, ak k náprave nedôjde v Prevádzkovateľom základnej služby určenej primeranej lehote nie kratšej ako 30 dní, je Prevádzkovateľ základnej služby oprávnený uplatniť si u Dodávateľa nárok na zaplatenie zmluvnej pokuty vo výške 100 EUR S DPH (slovom jednosto) za každý, aj začatý deň omeškania s plnením predmetnej povinnosti alebo záväzku. Právo na uplatnenie predmetného nároku má Prevádzkovateľ bez ohľadu na to, či od Zmluvy odstúpi alebo nie. Zaplatením zmluvnej pokuty nie je dotknuté právo Prevádzkovateľa na náhradu škodu v plnej výške a to aj nad výšku zaplatenej zmluvnej pokuty.
2. V prípade ak porušením akejkoľvek povinnosti alebo záväzkov Dodávateľa vyplývajúcich z tejto Zmluvy, ZoKB alebo vyhlášky NBÚ vznikne Prevádzkovateľovi základnej služby finančná ujma, je Prevádzkovateľ základnej služby oprávnený uplatniť si u Dodávateľa nárok na jej úhradu vo výške vzniknutých finančných nákladov, ktoré by Prevádzkovateľovi základnej služby v prípade splnenia povinnosti alebo záväzku Dodávateľa nevznikli; ustanovenie odseku 3 tohto článku tým nie je dotknuté.
3. V prípade, ak porušením povinnosti alebo záväzku Dodávateľa vyplývajúceho z tejto Zmluvy, ZoKB alebo vyhlášky NBÚ vznikne Prevádzkovateľovi základnej služby škoda, je Dodávateľ povinný Prevádzkovateľovi základnej služby uhradiť len priamu škodu, vzniknutú v príčinnej súvislosti s porušením povinnosti alebo záväzku Dodávateľa; ustanovenie odseku 2 tohto článku tým nie je dotknuté.

X. Zánik Zmluvy

1. Zmluva môže zaniknúť:
   a) odstúpením,
   b) zánikom zmluvy uvedenej v článku I, ods. 2 tejto Zmluvy.
2. Prevádzkovateľ základnej služby je oprávnený odstúpiť od tejto Zmluvy v prípade, ak Dodávateľ opakovane (viac ako trikrát) poruší akúkoľvek povinnosť alebo záväzok plynúci mu z tejto Zmluvy a súčasne nevykoná nápravu v Prevádzkovateľom základnej služby stanovenej lehote podľa článku IX. ods. 1 Zmluvy.

3. Táto Zmluva tiež s ohľadom na článok XI. ods. 2 Zmluvy zaniká okamihom zániku Prevádzkovej zmluvy.

XI. Záverečné ustanovenia

1. Zmluva nadobúda platnosť dňom podpisu oboma Zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky. Táto Zmluva je povinne zverejňovanou zmluvou podľa § 5a 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 (ďalej len „zákon č. 211/2000 Z. z.").
2. Táto Zmluva sa uzatvára na dobu určitú, po dobu platnosti a účinnosti Prevádzkovej zmluvy. Plnenie povinností vyplývajúcich z tejto Zmluvy sa vyžaduje počas celej doby trvania Prevádzkovej zmluvy.
3. Po ukončení tejto Zmluvy je Dodávateľ povinný na základe rozhodnutia Prevádzkovateľa základnej služby vrátiť, previesť, alebo zničiť všetky informácie Prevádzkovateľa základnej služby, ku ktorým mal Dodávateľ prístup počas trvania tejto Zmluvy, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane Dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach Prevádzkovateľa základnej služby.
4. Po ukončení tejto Zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovaných služieb Prevádzkovateľom základnej služby. Tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu založeného touto Zmluvou najmenej po dobu 2 rokov.
5. Zmluvné strany vyhlasujú, že v čase uzavretia tejto Zmluvy im nie sú známe žiadne okolnosti, ktoré by bránili, alebo vylučovali uzavretie tejto Zmluvy, resp. ktoré by mohli byť vážnou prekážkou jej plnenia.
6. Zmluvné strany vyhlasujú, že si túto Zmluvu riadne prečítali, jej obsahu porozumeli a na znak súhlasu s jej obsahom pripájajú svoje vlastnoručné podpisy.
7. Ak ktorékoľvek ustanovenie tejto Zmluvy je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto Zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú bezodkladne rokovať o nahradení akéhokoľvek nezákonného, neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.
8. Zmluvné strany sa týmto zaväzujú, že vynaložia všetko úsilie, ktoré je od nich možné spravodlivo požadovať, aby došlo k urovnaniu všetkých sporov, rozporov alebo nárokov vzniknutých medzi nimi na základe tejto Zmluvy a v súvislosti s ňou zmierom. Ak Zmluvné strany nevyriešia akýkoľvek spor zmierom, bude takýto spor predložený na rozhodnutie príslušnému všeobecnému súdu v Slovenskej republike.
9. Vo všetkých ostatných otázkach, výslovne neupravených touto Zmluvou sa postupuje podľa ustanovení Obchodného zákonníka, ZoKB a Vyhlášky.

10. Táto Zmluva môže byť doplnená a zmenená len písomným dodatkom v listinnej forme podpísaným oboma Zmluvnými stranami.
11. Táto Zmluva je vyhotovená v 4 rovnopisoch, pričom každá zo Zmluvných strán dostane po 2 rovnopisoch.

V Banskej Bystrici dňa:

Za Prevádzkovateľ základnej služby:

MUDr. Ján Nosko
primátor mesta

V Bratislave dňa:

Za Dodávateľa:

Ing. Peter Máčaj
predseda predstavenstva

Ing. Peter Tomášek
člen predstavenstva