

ZMLUVA

o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatvorená medzi

číslo zmluvy SSC č. 1268/1100/2022

Prevádzkovateľom základnej služby

Obchodné meno: **Slovenská správa ciest**
Sídlo: Miletičova 19, 826 19 Bratislava
Štatutárny orgán: Ing. Ivan Rybárik - generálny riaditeľ
IČO: 0000 33 28
DIČ: 2021067785
Bankové spojenie: Štátna pokladnica
Číslo účtu: IBAN: SK44 8180 0000 0070 0013 5433
Právna forma: Rozpočtová organizácia zriadená Ministerstvom dopravy, pôšt a telekomunikácií SR (právny nástupca je MDV SR) zriaďovacou listinou č. 5854/M-1995 zo dňa 07. 12. 1995 v znení neskorších zmien a doplnení

(ďalej len „prevádzkovateľ základnej služby“)

a

Dodávateľom základnej služby:

Obchodné meno: **AUTOCONT s.r.o.**
Sídlo: Krasovského 14, Bratislava – mestská časť Petržalka 851 01
Právna forma: spoločnosť s ručením obmedzeným
v zastúpení: Stanislav Šlesarik, poverený zástupca na základe plnej moci
IČO: 36 396 222
DIČ: 2020105428
IČ pre DPH: SK2020105428
Bankové spojenie: Slovenská sporiteľňa, a.s,
Číslo účtu: 5030808601/0900
IBAN: SK5309000000005030808601
Registrácia: Obchodný register Okresného súdu Bratislava I, oddiel: Sro, vložka číslo: 130357/B

(ďalej len „dodávateľ“)

(prevádzkovateľ základnej služby a dodávateľ spoločne ďalej len „zmluvné strany“)

Článok 1.

ÚVODNÉ USTANOVENIA

- 1.1. Slovenská správa ciest je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o kybernetickej bezpečnosti“).
- 1.2. Zmluvné strany uzatvárajú túto Zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na Zmluvu na poskytnutie služby číslo 633/1200/2022 uzatvorenú medzi Zmluvnými stranami dňa 9.6.2022 (ďalej len „Prevádzková zmluva“), ktoré definuje konkrétny rozsah činností dodávateľa.

- 1.3. Dodávateľ uzatvára s prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti (ďalej len „Zmluva“), ktorej predmet priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v zákone o kybernetickej bezpečnosti.
- 1.4. Prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom túto zmluvu podľa zákona o kybernetickej bezpečnosti.
- 1.5. Zmluva upravuje práva a povinnosti zmluvných strán a stanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by mohli negatívne ovplyvniť siete a informačné systémy prevádzkovateľa základnej služby, a minimalizovať dopad a vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby prevádzkovateľa.
- 1.6. Plnenie povinností podľa tejto zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania Prevádzkovej zmluvy.

Článok 2.

PREDMET ZMLUVY

- 2.1. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s uvedenými bezpečnostnými opatreniami.
- 2.2. Dodávateľ je povinný dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby, s ktorými ho prevádzkovateľ základnej služby písomne oboznámi. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami prevádzkovateľa základnej služby.
- 2.3. Dodávateľ súhlasí s tým, 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 bezpečnostným rizikám a hrozbám týkajúcich sa dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na kvalitu, dostupnosť a bezpečnosť základnej služby prevádzkovateľa.
- 2.4. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu tejto zmluvy.
- 2.5. Dodávateľ vyhlasuje, že má potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role, opatrenia a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie účelu tejto zmluvy.
- 2.6. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania Prevádzkovej zmluvy.
- 2.7. Odplata za plnenie povinností dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto zmluvy sú v

plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom základnej služby dodávateľovi podľa Prevádzkovej zmluvy.

Článok 3.

Povinnosť dodávateľa prijať a dodržiavať bezpečnostné opatrenia

- 3.1. Dodávateľ je povinný v rámci prevencie kybernetických incidentov, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa, a tým na činnosť prevádzkovateľa: :
- a) zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Prevádzkovej zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby,
 - b) sledovať výstrahy a varovania slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne, zasielať prevádzkovateľovi základnej služby včasné varovania pred incidentmi, ktoré by mohli negatívne ovplyvniť prevádzkovanie základnej služby prevádzkovateľa a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb alebo znižovanie kybernetických rizík,
 - c) monitorovať a vyhodnocovať také bezpečnostné riziká, ktoré by mohli mať nepriaznivý dopad na základnú službu prevádzkovateľa základnej služby,
 - d) predchádzať vzniku incidentov,
 - e) spolupracovať s prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.
 - f) chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.
 - g) hlásiť všetky skutočnosti, informácie, zmeny, ktoré môžu mať vplyv na túto zmluvu. Uvedené dodávateľ hlási formou elektronickej pošty do 2 dní od zistenia danej skutočnosti,
 - h) dodržiavať a prijať bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona, a to najneskôr do dvoch mesiacov od účinnosti zmluvy . Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.
- 3.2. Pre oblasť technických zraniteľností informačných systémov a zariadení dodávateľ najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, prostredníctvom nasledujúcich opatrení
- a) Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
 - b) Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
 - c) Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.
- 3.3. Pre oblasť riadenia bezpečnosti sietí a informačných systémov, ktoré dodávateľ využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, realizuje dodávateľ opatrenia:
- a) Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa

nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom.

- b) Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
- c) Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
- d) Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.
- e) Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
- f) Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
- g) Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
- h) Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.
- i) Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
- j) Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
- k) Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.
- l) Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.
- m) Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.
- n) Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.
- o) Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie novej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

3.4. Pre oblasť riadenia prístupov, ktoré dodávateľ využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, realizuje dodávateľ nasledovné opatrenia:

- a) Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob pridelovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
- b) Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabráňujú zneužitiu týchto údajov neoprávnenou osobou.
- c) Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám;

prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.

- d) Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
- e) Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
- f) Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).
- g) Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
- h) Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

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

- a) Oboznámenie sa s postupmi prevádzkovateľa základnej služby pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči prevádzkovateľovi základnej služby.
- b) Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb prevádzkovateľovi základnej služby.
- c) Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
- d) Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým 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.
- e) Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov prevádzkovateľa základnej služby.
- f) Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s prevádzkovateľom základnej služby.
- g) Dodávateľ je povinný bezodkladne hlásiť každý incident prevádzkovateľovi základnej služby spôsobom určeným prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov.

- h) Dodávateľ je povinný na žiadosť prevádzkovateľa základnej služby spolupracovať s Národným bezpečnostným úradom a na tento účel poskytnúť potrebnú súčinnosť a všetky informácie, ktoré by mohli byť dôležité pre riešenie incidentu.
- i) Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz o bezpečnostnom incidente tak, aby tento mohol byť použitý v trestnom konaní a poskytnúť ho prevádzkovateľovi základnej služby.
- j) Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby skutočnosť, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
- k) Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi základnej služby vykonanie a implementovanie nápravného opatrenia.

- 3.6. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje dodávateľ opatrenia podľa § 15 vyhlášky NBÚ č. 362/2018 Z.z., , ktoré dodávateľ využíva pri poskytovaní služieb prevádzkovateľovi základnej služby, najmä implementuje centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb prevádzkovateľovi základnej služby.
- 3.7. Dodávateľ je povinný doručiť prevádzkovateľovi základnej služby zoznam svojich zamestnancov a pracovných rolí dodávateľa, ktoré sa budú podieľať na plnení Prevádzkovej zmluvy a tejto zmluvy a budú mať prístup k informáciám prevádzkovateľa základnej služby a každú zmenu v personálnom obsadení je dodávateľ povinný prevádzkovateľovi základnej služby oznámiť (mailom, písomne).
- 3.8. Dodávateľ vyjadruje súhlas s dodržiavaním uvedených bezpečnostných opatrení.

Článok 4.

MLČANLIVOSŤ

- 4.1. Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením Prevádzkovej zmluvy a tejto zmluvy a ktoré nie sú verejne známe.
- 4.2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.
- 4.3. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávateľa a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu alebo obchodného vzťahu.
- 4.4. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. tieto podľa pokynu prevádzkovateľa základnej služby zničiť.

Článok 5.

KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

- 5.1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom základnej služby spôsobom určeným prevádzkovateľom základnej služby, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
- 5.2. Prevádzkovateľ základnej služby určuje nasledovnú kontaktnú osobu pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti: Marek Mička

- 5.3. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti: Blašková Zuzana, email: zuzana.blaskova@autocont.sk

Článok 6.

SPOLOČNÉ USTANOVENIA

- 6.1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy s odbornou starostlivosťou a v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi.
- 6.2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať negatívny vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by mohli narušiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
- 6.3. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy bezodkladne.
- 6.4. V prípade, ak dodávateľ poruší svoje povinnosti v zmysle tejto Zmluvy voči prevádzkovateľovi základnej služby, vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty a dodávateľ sa zaväzuje uhradiť zmluvnú pokutu vo výške 499 EUR za každé jedno porušenie zmluvnej povinnosti. Vznikom nároku na zaplatenie zmluvnej pokuty podľa tohoto bodu nie je dotknutý nárok Prevádzkovateľa základnej služby na náhradu škody vo výške presahujúcej zmluvnú pokutu
- 6.5. V prípade, ak dodávateľ plní Prevádzkovú zmluvu prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov. Dodávateľ je povinný vopred informovať prevádzkovateľa základnej služby o zapojení nového dodávateľa (teda subdodávateľa), a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom emailu na kontakt uvedený v záhlaví tejto zmluvy. Dodávateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb prevádzkovateľovi základnej služby nového subdodávateľa bez predchádzajúceho výslovného písomného súhlasu prevádzkovateľa základnej služby. Novému dodávateľovi (subdodávateľovi) je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto zmluve. Zodpovednosť voči prevádzkovateľovi základnej služby nesie dodávateľ, ak nový subdodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.
- 6.6. Dodávateľ je povinný hlásiť prevádzkovateľovi základnej služby ďalšie informácie požadované prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona, najmä
- a) informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované prevádzkovateľom základnej služby alebo Národným bezpečnostným úradom a ústredným orgánom od prevádzkovateľa základnej služby za účelom splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm. c) zákona,
 - b) informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
 - c) informácie potrebné na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods.6 písm. e) Zákona oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

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

- 6.7. Dodávateľ je povinný informovať Prevádzkovateľa základnej služby o všetkých bezpečnostných rizikách, ktoré identifikuje a navrhnúť vhodné technické, procesné, organizačné alebo fyzické objektové bezpečnostné opatrenia a odporúčania. Prevádzkovateľ základnej služby je povinný počas trvania platnosti tejto zmluvy organizovať pravidelné stretnutia s Dodávateľom, na ktorých budú dodávateľom identifikované bezpečnostné riziká a navrhované opatrenia konzultované s Prevádzkovateľom základnej služby a vzájomne odsúhlasené. Výsledok stretnutia bude formálne zapísaný, pričom v zázname bude určený vlastník rizika (jedna zo zmluvných strán) zodpovedná za zabezpečenie predmetného aktíva alebo procesu.
- 6.8. Po vykonaní SW a HW auditu u Prevádzkovateľa je dodávateľ povinný vydať odporúčania ohľadne zlepšenia/výmeny resp. doplnenia SW alebo HW, ktoré prevádzkovateľ môže zobrať na vedomie.
- 6.9. Prevádzkovateľ základnej služby určí systémy a zariadenia, ktoré spravuje tretia strana.

Článok 7.

AUDIT KYBERNETICKEJ BEZPEČNOSTI

- 7.1. Prevádzkovateľ základnej služby je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov tejto zmluvy.
- 7.2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
- 7.3. Prevádzkovateľ základnej služby môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti prevádzkovateľa základnej služby pri výkone auditu realizuje prevádzkovateľom základnej služby poverená tretia osoba.
- 7.4. Dodávateľ je povinný pri audite spolupracovať s prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
- 7.5. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi základnej služby súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy a platnej právnej úpravy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
- 7.6. Prevádzkovateľ základnej služby je povinný oznámiť dodávateľovi svoj zámer realizovať u neho audit najmenej päť pracovných dní vopred.
- 7.7. Dodávateľ je povinný písomne informovať prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom.

Článok 8.

ZÁVEREČNÉ USTANOVENIA

- 8.1. Táto zmluva sa uzatvára na dobu určitú do splnenia Prevádzkovej zmluvy alebo iného jej ukončenia. Prevádzkovateľ základnej služby je oprávnený od tejto zmluvy odstúpiť v prípadoch, ak dodávateľ porušuje svoje povinnosti vyplývajúce z tejto zmluvy.
- 8.2. 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 prevádzkovania základnej služby prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.
- 8.3. Táto zmluva sa spravuje zákonmi Slovenskej republiky. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka č. 513/1991 Zb. v znení neskorších predpisov a súvisiacimi predpismi.
- 8.4. Táto zmluva sa môže meniť alebo ukončiť iba dohodou zmluvných strán v písomnej forme.
- 8.5. Táto zmluva bola vyhotovená v štyroch rovnopisoch, po dvoch pre každú zmluvnú stranu.
- 8.6. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv.
- 8.7. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah tejto zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.

Za prevádzkovateľa základnej služby:

V mene dodávateľa:

V Bratislave, dňa

V Bratislave , dňa

Ing. Ivan Rybárik
generálny riaditeľ

Stanislav Šlesarik
poverený zástupca na základe plnej moci