Príloha č. 5 k Zmluve

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená v súlade s povinnosťami prevádzkovateľa základnej služby podľa § 19 ods. 2 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**“)

(ďalej len „**zmluva**“)

medzi

Prevádzkovateľom základnej služby:
Generálne riaditeľstvo Zboru väzenskej a justičnej stráže
rozpočtová organizácia, zriadená zriaďovacou listinou Ministerstva spravodlivosti Slovenskej republiky v znení jej neskorších dodatkov

Sídlo:	Šagátova 1, 821 08 Bratislava
Korešpondenčná adresa:	Šagátova ul. č. 1, 813 04 Bratislava 1
IČO:	00 212 008
Štatutárny orgán:	plk. Mgr. JUDr. Ing. Ľubomír Kliština, generálny riaditeľ Zboru väzenskej a justičnej stráže (ďalej len „ generálny riaditeľ“)
Osoba oprávnená rokovať vo veciach zmluvných (zodpovedná osoba):	
Email:	
Telefón:	

(ďalej len „**Prevádzkovateľ**“)

a

Dodávateľ na výkon činností:

Obchodné meno:	**Vision IT Solutions, a. s.**
Zapísaný: v Obchodnom registri	Mestského súdu Bratislava III, Oddiel Sa, Vložka č. 5127/B
Sídlo:	Pribinova 25, 811 09 Bratislava
Korešpondenčná adresa:	Tower 115, Pribinova 25, 811 09 Bratislava
IČO:	36815799
Zastúpený:	
Osoba oprávnená rokovať vo veciach zmluvných (zodpovedná osoba):	
Email:	
Telefón:	

(ďalej ako „**Dodávateľ**“)
(„Prevádzkovateľ“ a „Dodávateľ“ spoločne ďalej len ako „**zmluvné strany**“)

Preambula

V zmysle zákona 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov § 19 ods. 2, vyhlášky národného bezpečnostného úradu 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení §9 a článku 6, bodu 6.1., písm. f) zmluvy GR ZVJS-07648/42-2024 (ďalej len „Hlavná zmluva“) sa uzatvára táto zmluva na aplikovanie bezpečnostných opatrení a oznamovania kybernetických bezpečnostných incidentov a ich zabezpečovanie aj na úrovni dodávateľských služieb predstavujú transpozíciu smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii, podľa ktorej (okrem iného) prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb by mali zaistiť bezpečnosť sietí a informačných systémov, ktoré používajú. Požiadavky týkajúce sa bezpečnosti a oznamovania by sa mali vzťahovať na relevantných prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb bez ohľadu na to, či údržbu svojich sietí a informačných systémov vykonávajú interne, alebo prostredníctvom externého dodávateľa.

Čl. I
Predmet zmluvy

Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na hlavnú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov Prevádzkovateľa (s ktorými priamo súvisí výkon činností dodávateľa na základe dodávateľskej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by mohli negatívne ovplyvniť siete a informačné systémy Prevádzkovateľa a minimalizovať dopad a vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby Prevádzkovateľa.

Čl. II.
Povaha a predmet zabezpečenia

Povaha zabezpečenia plnenia bezpečnostných opatrení a notifikačných povinnosti je daná hlavným zmluvným vzťahom, ktorý je upravený hlavnou zmluvou.

Čl. III
Obdobie trvania zmluvy

Dodávateľ zabezpečuje plnenie bezpečnostných opatrení a notifikačných povinností počas celého trvania platnosti a účinnosti Hlavnej zmluvy. Pre zamedzenie pochybností sa zmluvné strany výslovne dohodli, že zmluva zaniká dňom zániku Hlavnej zmluvy.

Čl. IV
Práva a povinnosti zmluvných strán

4.1. Dodávateľ sa zaväzuje dodržiavať Prevádzkovateľom vydanú bezpečnostnú stratégiu kybernetickej bezpečnosti v Zbore väzenskej a justičnej stráže, s ktorou bol dodávateľ preukázateľne oboznámený (ďalej aj ako „bezpečnostná smernica“) a ktorá tvorí prílohu č. 1 tejto zmluvy a bezpečnostné požiadavky uvedené v tejto zmluve.

4.2. Dodávateľ súhlasí s tým, že bezpečnostná smernica Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym bezpečnostným rizikám a hrozbám týkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na kvalitu, dostupnosť a bezpečnosť základnej služby Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou smernicou s dôrazom na zmeny v nej uvedené.

4.3. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v článku IV tejto zmluvy tak, aby boli naplnené ciele tejto zmluvy.

4.4. Bezpečnostné opatrenia Prevádzkovateľa sa môžu meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa , aktuálnej legislatíve a aktuálnym hrozbám týkajúcich sa prevádzky sietí a informačných systémov Prevádzkovateľa . Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanými bezpečnostnými opatreniami s dôrazom na zmeny v nich uvedené.

4.5. 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.

4.6. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom , najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

4.7. Dodávateľ je povinný stanoviť postupy plnenia 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 v určenej lehote, ktorá nesmie byť kratšia ako 5 pracovných dní.

4.8. Zoznam zamestnancov Dodávateľa, subdodávateľa a tretích osôb, ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa tejto zmluvy a ktorí budú mať prístup k informáciám Prevádzkovateľa (ďalej len „**zoznam osôb**“) tvorí prílohu č. 2 tejto zmluvy. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v zozname osôb podľa tohto bodu bezodkladne na emailovú adresu kontaktnej osoby Prevádzkovateľa .

4.9. Dodávateľ je povinný písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom na účely plnenia tejto zmluvy.

4.10. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Dodávateľa o hlásenom kybernetickom incidente. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

4.11. Na výkon činností, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľskej zmluvy a/alebo tejto zmluvy, môže Dodávateľ poveriť len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v prílohe č. 2 tejto zmluvy.

4.12. 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 Dodávateľovi podľa dodávateľskej zmluvy.

Čl. V
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

5.1. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v rámci prevencie pred kybernetickými incidentmi, ktoré by mohli mať nepriaznivý dopad na základnú službu Prevádzkovateľa, jeho informačné systémy a siete. Dodávateľ sa zaväzuje:

a) zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení dodávateľskej zmluvy alebo budú mať prístup k informáciám Prevádzkovateľa ,
b) sledovať výstrahy a varovania slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne, zasielať Prevádzkovateľovi 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 ,
d) predchádzať vzniku incidentov,
e) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa ,
f) chrániť informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa,
g) hlásiť všetky skutočnosti, informácie, zmeny, ktoré môžu mať vplyv na túto zmluvu. Uvedené Dodávateľ hlási formou elektronickej pošty do 2 kalendárnych 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 o kybernetickej bezpečnosti, a to najneskôr do 5 pracovných dní. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

5.2. Pre oblasť technických zraniteľností informačných systémov a zariadení Dodávateľ najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Prevádzkovateľovi , 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 zraniteľnostítechnických prostriedkov a ich častí,
c) využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

5.3. Pre oblasť riadenia bezpečnosti sietí a informačných systémov, ktoré Dodávateľ využíva pri poskytovaní služieb Prevádzkovateľovi , realizuje Dodávateľ opatrenia:

a) Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Prevádzkovateľa , 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 alebospôsobujúce 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 možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

5.4. Pre oblasť riadenia prístupov, ktoré Dodávateľ využíva pri poskytovaní služieb Prevádzkovateľovi , 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 prideľovania 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 , 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.
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.

5.5. 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:

a) Oboznámenie sa s postupmi Prevádzkovateľa pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči Prevádzkovateľovi.
b) Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívanéna poskytovanie služieb Prevádzkovateľovi.
c) Detegovanie incidentov, prostredníctvom nástroja na detekciu 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 incidentoch prostredníctvom nástroja na zber a

nepretržité vyhodnocovanie udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s incidentom; vyhodnocovanie udalostí na ich identifikáciu ako incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie udalostí pri nesprávne identifikovaných incidentoch.

e) Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Prevádzkovateľa.
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.
g) Dodávateľ je povinný bezodkladne hlásiť každý incident Prevádzkovateľovi spôsobom určeným Prevádzkovateľom, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov.
h) Dodávateľ je povinný na žiadosť Prevádzkovateľa 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.
j) Dodávateľ je povinný oznámiť Prevádzkovateľovi skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
k) Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie a implementovanie nápravného opatrenia.

5.6. Pre oblasť zaznamenávania udalostí a monitorovania sietí a informačných systémov realizuje Dodávateľ opatrenia podľa § 15 vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ktoré Dodávateľ využíva pri poskytovaní služieb Prevádzkovateľovi, 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.

5.7. Dodávateľ vyjadruje súhlas s dodržiavaním uvedených bezpečnostných opatrení.

Čl. VI
Mlčanlivosť

6.1. Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením dodávateľskej zmluvy a tejto zmluvy a ktoré nie sú verejne známe.

6.2. Povinnosť zachovávať mlčanlivosť podľa tohto článku zmluvy trvá aj po skončení tejto zmluvy.

6.3. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu alebo obchodného vzťahu.

6.4. Po ukončení tejto zmluvy je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. tieto podľa pokynu

Prevádzkovateľa zničiť.

Čl. VII
Kontaktné osoby na úseku kybernetickej bezpečnosti

7.1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s Prevádzkovateľom spôsobom určeným Prevádzkovateľom, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

7.2. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s dodávateľom:
- na úseku kybernetickej bezpečnosti:
- pre oblasť IT:

7.3. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti:

Čl. VIII
Spoločné ustanovenia

8.1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi.

8.2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať negatívny vplyv na základnú službu Prevádzkovateľa alebo ktoré by mohli narušiť kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

8.3. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy bezodkladne.

8.4. V prípade, ak Dodávateľ plní dodávateľskú 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 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 nového subdodávateľa bez predchádzajúceho výslovného písomného súhlasu Prevádzkovateľa . Novému dodávateľovi (subdodávateľovi) je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto zmluve. Zodpovednosť voči Prevádzkovateľovi nesie Dodávateľ, ak nový subdodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení alebo hláseniabezpečnostných incidentov.

8.5. Dodávateľ je povinný hlásiť Prevádzkovateľovi ďalšie informácie požadované Prevádzkovateľom na plnenie jeho povinnosti vyplývajúcich zo zákona o kybernetickej bezpečnosti, najmä:

a) informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované Prevádzkovateľom alebo Národným bezpečnostným úradom a ústredným orgánom

od Prevádzkovateľa za účelom splnenia povinnosti Prevádzkovateľa v zmysle ust. § 19 ods. 6 písm. c) zákona
o kybernetickej bezpečnosti,

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 v zmysle ust. § 19 ods. 6 písm. e) zákona o kybernetickej bezpečnosti 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 v zmysle ust. § 27 ods. 10 zákona o kybernetickej bezpečnosti.

Čl. IX
Audit kybernetickej bezpečnosti

9.1. Prevádzkovateľ 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.

9.2. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.

9.3. Prevádzkovateľ môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu realizuje Prevádzkovateľom poverená tretia osoba.

9.4. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

9.5. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, 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.

9.6. Prevádzkovateľ je povinný oznámiť Dodávateľovi svoj zámer realizovať u neho audit najmenej päť pracovných dní vopred.

9.7. Dodávateľ je povinný písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.

Čl. X

Sankcie

10.1 Ak Dodávateľ poruší svoje povinnosti vyplývajúce z článku IV bodu 4.1,4.3. až 4.7.,4. 9. a 4.10., článku V bodu 5.1. až 5.5., článku VIII bodu 8.1. tejto Zmluvy, má Prevádzkovateľ právo na zmluvnú pokutu vo výške 0,05 % z celkovej ceny plnenia za Hlavnú zmluvu bez DPH, a to za každé jednotlivé porušenie povinnosti Dodávateľom zvlášť.

10.2. Ak Prevádzkovateľ poruší svoju povinnosť vyplývajúcu z článku IV bodu 4.10., má Dodávateľ právo na zmluvnú pokutu vo výške 100,- € (slovom: sto eur) za každé jednotlivé porušenie tejto povinnosti.

10.3. Zaplatenie zmluvnej pokuty nemá vplyv na nárok zmluvných strán na náhradu škody, ktorá vznikla z nesplnenia povinnosti zabezpečenej zmluvnou pokutou.

10.4. Zaplatenie zmluvnej pokuty nezbavuje zmluvné strany splnenia si zmluvných povinností zabezpečených zmluvnou pokutou. Zmluvnú pokutu si zmluvné strany uhradia do 30 kalendárnych dní odo dňa jej písomného uplatnenia.

Čl. XI
Záverečné ustanovenia

11.1. Táto zmluva, ako aj práva a povinnosti zmluvných strán, ňou výslovne neupravené, sa riadia a vykladajú podľa príslušných všeobecne záväzných právnych predpisov, platných v Slovenskej republike. Právomoc rozhodovať spory z nej majú príslušné slovenské súdy.

11.2. Túto zmluvu možno doplniť alebo zmeniť len na základe písomnej dohody zmluvných strán, a to formou postupne číslovaných písomných dodatkov.

11.3. Zmluva je vyhotovená v štyroch rovnopisoch, pričom každá zo zmluvných strán dostane dve vyhotovenia.

11.4. Táto zmluva sa uzatvára na dobu určitú a platí počas celej doby účinnosti Hlavnej zmluvy. Zmluva nadobúda platnosť dňom jej podpisu a účinnosť dňom nasledujúcim po dni jej zverejnenia Prevádzkovateľom v Centrálnom registri zmlúv, vedenom Úradom vlády Slovenskej republiky.

11.5. Zmluva zaniká dňom ukončenia Hlavnej zmluvy. Zmluvu je možné tiež ukončiť písomnou dohodou zmluvných strán a odstúpením v zmysle v príslušných všeobecne záväzných právnych predpisov.

11.6. Zmluvné strany vyhlasujú, že si zmluvu riadne prečítali, že zmluva nebola dojednaná v tiesni a ani za inak jednostranne nevýhodných podmienok. Na znak súhlasu s jej obsahom ju vlastnoručne pospisujú.

11.7. Pokiaľ niektoré z ustanovení tejto zmluvy je neplatné alebo sa stane neskôr neplatným alebo neúčinným, nemá to vplyv na platnosť ostatných ustanovení tejto zmluvy. V prípade, ak nastane situácia podľa prvej vety tohto bodu, zmluvné strany sa zaväzujú, že ho nahradia ustanovením, ktoré najviac zodpovedá pôvodnej vôli zmluvných strán a účelu podľa tejto zmluvy.

11.8. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:

a) Príloha č. 1 k zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností – Bezpečnostná dokumentácia
b) Príloha č. 2 k zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností – Zoznam osôb a pracovných rolí dodávateľa

11.9. Táto zmluva je u Prevádzkovateľa evidovaná pod Hlavnou zmluvou s číslom: GR ZVJS-07648/42-2024.

V Bratislave, dňa.....

Za Prevádzkovateľa:

.....
plk. Mgr. JUDr. Ing. Ľubomír Kliština
generálny riaditeľ

V Bratislave, dňa.....

Za Dodávateľa:

.....
predseda predstavenstva

Príloha č. 1 k zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností – Bezpečnostná dokumentácia

a) Rozkaz generálneho riaditeľa 33/2023 o bezpečnostnej stratégií kybernetickej bezpečnosti v Zbore väzenskej a justičnej stráže v znení RGR č. 8/2024

Príloha č. 2 k zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností – Zoznam osôb a pracovných rolí dodávateľa

P.č.	Meno a Priezvisko	Pracovná rola
1.		VMware systémový inžinier NetApp systémový inžinier VEEAM systémový inžinier Microsoft systémový inžinier
2.		VMware systémový inžinier CheckPoint analytik
3.		VMware systémový inžinier VEEAM systémový inžinier
4.		NetApp systémový inžinier
5.		CheckPoint analytik
6.		Sophos analytik Projektový manažér
7.		Zabbix analytik
8.		Projektový manažér