Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov medzi

Prevádzkovateľom základnej služby:

Názov:	Úrad verejného zdravotníctva Slovenskej republiky
Sídlo:	Trnavská cesta 52, 826 45 Bratislava, Slovenská republika
IČO:	00607223
DIČ:	2020878090
IČ DPH:	nie je platca DPH
V mene ktorého koná:	MUDr. Tatiana Červeňová, MPH., MHA. - hlavný hygienik SR
Kontaktná osoba:	Ing. Jana Grňo Mikulášiová – manažér kybernetickej bezpečnosti
E-mail kontaktnej osoby:	

(ďalej aj len ako „**Prevádzkovateľ**“)

a

Dodávateľom:

Obchodné meno:	Asseco Central Europe, a.s.
Sídlo:	Galvaniho 19045/19, 821 04 Bratislava – mestská časť Ružinov
IČO:	35 760 419
Zapísané v:	Obchodný register Mestského súdu Bratislava III, Oddiel: Sa, Vložka číslo: 2024/B
DIČ:	2020254159
IČ DPH:	SK7020000691
V mene ktorého koná:	Ing. Michal Navrátil - prokurista
Kontaktná osoba:	Miroslav Kepencay
E-mail kontaktnej osoby:	

(ďalej všetci spoločne aj len ako „**Dodávateľ**“)

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

Článok I.
Úvodné ustanovenia a vyhlásenia

1. Prevádzkovateľ ako objednávateľ uzavrel s Dodávateľom ako poskytovateľom dňa 29.05.2024 Zmluvu o podpore prevádzky, údržbe a rozvoji informačného systému, predmetom ktorej je podpora prevádzky, údržba a rozvoj **Integrovaného informačného systému úradov verejného zdravotníctva** (ďalej len „**IS ÚVZ**“) pre zabezpečenie prevádzky Informačného systému IS UVZ na základe dohodnutých cieľových úrovní podporných služieb zo dňa 29.05.2024, v znení neskorších dodatkov (ďalej aj len ako „**SLA**“).

2. Prevádzkovateľ je podľa § 3 písm. m) 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**“) prevádzkovateľom základnej služby podľa § 3 písm. l) zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom

služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

3. Za účelom plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a § 8 vyhlášky 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 OBO**"), zmluvné strany uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**zmluva**"); pri uzatvorení zmluvy sa vykonáva analýza dodávateľských rizík prevádzkovateľom.

4. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na SLA, na základe ktorej Dodávateľ bude poskytovať Prevádzkovateľovi služby (činnosti), ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby. Vzhľadom na skutočnosť, že Prevádzkovateľ si Paušálne služby podľa SLA objednáva vždy len na určité časové obdobie, sa zmluvné strany dohodli, že Dodávateľ bude plniť záväzky a povinnosti vyplývajúce z tejto zmluvy len počas obdobia a za obdobie, v ktorom bude mať Prevádzkovateľ objednanú aspoň jednu Paušálnu službu podľa SLA.

Článok II.
Predmet zmluvy

1. 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 SLA, a to s cieľom zabezpečiť informačnú a kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov Prevádzkovateľa (s ktorými priamo súvisí výkon činností Dodávateľa na základe SLA) počas trvania SLA, predchádzať informačným a kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť Prevádzkovateľa a minimalizovať vplyv informačných kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov Prevádzkovateľa, zabezpečiť kontinuitu prevádzkovania služieb, sietí a informačných systémov, zabezpečenie potrebného monitorovania a merania, výkon auditu a kontroly ako aj implementovať ostatné bezpečnostné opatrenia (špecifikované v prílohe č. 1 tejto zmluvy), ktoré sú nevyhnutné na splnenie požiadaviek zákona o kybernetickej bezpečnosti a súvisiacich vyhlášok (napríklad vyhláška OBO, atď.).

2. Pre účely tejto zmluvy sa za kybernetický incident považuje kybernetický bezpečnostný incident podľa zákona o kybernetickej bezpečnosti, ako aj akákoľvek bezpečnostná udalosť:
   a) bez ohľadu na zdroj informácií o kybernetickom bezpečnostnom incidente (t. j. bez ohľadu na to, či ju zistí Dodávateľ, alebo Prevádzkovateľ),
   b) ktorá sa týka informačných systémov alebo sietí, vo vzťahu ku ktorým Dodávateľ poskytuje výkon činností podľa SLA,
   c) ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k narušeniu kybernetickej bezpečnosti, prípadne dôvernosti, integrity alebo dostupnosti služby Prevádzkovateľa, alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby Prevádzkovateľa alebo k zníženiu kvality poskytovanej služby Prevádzkovateľa, a
   d) bezpečnostné incidenty, ktoré sú definované v SLA kap. 1 ods. 1.1 písm. b) s ohľadom na ustanovenia uvedené v kap. 5 SLA.

Článok III.
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje dodržiavať Prevádzkovateľom vydané bezpečnostné smernice a štandardy, s ktorými bol Dodávateľ preukázateľne oboznámený ku dňu podpisu tejto zmluvy (ďalej aj len ako „**bezpečnostná dokumentácia**") a bezpečnostné požiadavky uvedené v tejto zmluve. Akékoľvek činnosti alebo zmeny vyvolané zmenou bezpečnostnej dokumentácie alebo nevyhnutné v dôsledku zmeny bezpečnostnej dokumentácie po uzavretí tejto zmluvy Dodávateľ vykoná a zapracuje na základe

osobitnej dohody s Prevádzkovateľom pričom na tieto činnosti sa použijú zdroje Prevádzkovateľa (Objednávateľa v zmysle SLA) podľa bodu A5 *Zmeny Systému v rámci Paušálnych služieb* Prílohy č. 1 SLA, prípadne si ich Prevádzkovateľ osobitne objedná ako Objednávkové služby podľa SLA.

2. Bezpečnostná dokumentácia Prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnej legislatíve, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcich sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou dokumentáciou s dôrazom na zmeny v nej uvedené, pričom zmluvné strany následne potvrdia akceptáciu zmien bezpečnostnej dokumentácie.

3. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa, ktoré tvoria **Prílohu č. 1** k tejto zmluve a ktoré sú obsiahnuté v bezpečnostnej dokumentácii Prevádzkovateľa. Dodávateľ sa zaväzuje zdokumentovať oboznámenie svojich zamestnancov, ktorí poskytujú služby spojené s definovaným predmetom zmluvy a zaväzuje sa realizovať pravidelné školenia o pravidlách uvedených v Prílohe č. 1 tejto zmluvy a bezpečnostnej dokumentácii Prevádzkovateľa (minimálne jedenkrát ročne), Dodávateľ zabezpečí k bezpečnostnej dokumentácii riadený prístup a zaviaže osoby, ktoré budú mať prístup k bezpečnostnej dokumentácii Prevádzkovateľa mlčanlivosťou, pričom povinnosť mlčanlivosti trvá aj po skončení pracovného pomeru alebo obdobného pracovného vzťahu fyzických osôb. Splnenie povinnosti v zmysle tohto bodu je Poskytovateľ povinný na výzvu Objednávateľa kedykoľvek hodnoverne preukázať. Ostatné ustanovenia týkajúce sa ochrany dôverných informácií a osobných údajov sú uvedené v Zmluve o podpore prevádzky, údržbe a rozvoji informačného systému, predmetom ktorej je podpora prevádzky, údržba a rozvoj IS ÚVZ, vrátane definovania sankcií.

4. Bezpečnostné opatrenia Prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanými bezpečnostnými opatreniami s dôrazom na zmeny v nich uvedené, pričom zmluvné strany následne potvrdia akceptáciu zmien bezpečnostných opatrení formou dodatku k tejto zmluve.

5. Dodávateľ je povinný plniť bezpečnostné opatrenia a notifikačné povinnosti v oblasti kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve počas celej doby trvania tejto zmluvy, pokiaľ zo zmluvy nevyplývajú povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo SLA.

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

7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v internej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu.

8. Internú dokumentáciu, ktorá súvisí s poskytovaním služieb, definovaných v predmete tejto zmluvy je povinný Dodávateľ predložiť na posúdenie Prevádzkovateľovi. Dodávateľ je povinný zohľadniť pripomienky Prevádzkovateľa k dokumentácii, ktoré smerujú k zabezpečeniu poskytovania základnej služby Prevádzkovateľa. Dodávateľ je na požiadanie povinný predložiť dokumentáciu Prevádzkovateľovi v určenej lehote nie kratšej ako [5] pracovných dní.

9. Dodávateľ je povinný bezodkladne písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom na účely plnenia tejto zmluvy na e-mailovú adresu .

10. Dodávateľ môže zapojiť do poskytovania služieb na základe SLA ďalšieho dodávateľa (subdodávateľ), ak mu to vyplýva z ustanovení SLA počas doby jej platnosti a účinnosti. Túto skutočnosť je povinný oznámiť pred zapojením subdodávateľa do poskytovania služieb spolu s identifikáciou konkrétnych osôb na e-mailovú adresu . Prevádzkovateľ si vyhradzuje právo odsúhlasiť osoby, ktoré budú zapojené do poskytovania základných služieb. Dodávateľ nesmie zapojiť do realizácie prác súvisiacich s výkonom činností definovaných v SLA a tejto zmluvy osoby, ktoré nie sú odsúhlasené Prevádzkovateľom pričom na tieto osoby sa použije ods. 9 tohto článku. Zmluvné strany sa dohodli, že subdodávatelia uvedení v SLA a v jej prílohách sa považujú za oznámených Prevádzkovateľovi a odsúhlasených Prevádzkovateľom podľa tejto Zmluvy. Povinnosť Dodávateľa odsúhlasiť zoznam zamestnancov odsúhlasených subdodávateľov, ako aj zmeny v tomto zozname zostáva nedotknutá. Prevádzkovateľ berie na vedomie a súhlasí, že v prípade ak odmietne udeliť súhlas niektorému dodatočnému subdodávateľovi na plnenie SLA, alebo zamestnancovi subdodávateľa, môže dôjsť k omeškaniu s poskytovaním služieb podľa SLA, za ktoré v takom prípade nezodpovedá Dodávateľ a preto voči Dodávateľovi nemôžu byť z tohto dôvodu uplatnené žiadne sankcie podľa SLA alebo tejto zmluvy.
11. Dodávateľ je povinný oznámiť zoznam zamestnancov Manažérovi kybernetickej bezpečnosti Prevádzkovateľa, ktorý sa do 5 pracovných dní k návrhu vyjadrí. Ak Dodávateľ nebude mať doručené do 5 dní od oznámenia zamietavé stanovisko k návrhu, bol návrh schválený.
12. 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. 3 tejto zmluvy. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v Zozname osôb podľa tohto bodu bezodkladne na e-mailovú adresu . Prevádzkovateľ berie na vedomie a súhlasí, že v prípade ak odmietne udeliť súhlas niektorému dodatočnému zamestnancovi Dodávateľa alebo subdodávateľa na plnenie SLA, môže dôjsť k omeškaniu s poskytovaním služieb podľa SLA, za ktoré v takom prípade nezodpovedá Dodávateľ a preto voči Dodávateľovi nemôžu byť z tohto dôvodu uplatnené žiadne sankcie podľa SLA alebo tejto zmluvy.
13. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Dodávateľa o hlásenom kybernetickom incidente. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.
14. Dodávateľ je povinný bezodkladne informovať Prevádzkovateľa o podozrení na výskyt bezpečnostného incidentu, alebo o bezpečnostnom incidente, ktorý by mohol mať vplyv, alebo súvis s poskytovanými službami.
15. Na výkon činností, ktoré vyplývajú z podstaty služieb poskytovaných na základe SLA a/alebo tejto zmluvy môže poveriť Dodávateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v Prílohe č. 3.

Článok IV.
Okolnosti plnenia zmluvy

1. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou záväzkov podľa tejto zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek tejto zmluvy.

2. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Prevádzkovateľa podľa SLA. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania SLA.

Článok V.
Všeobecné bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

1. Dodávateľ je povinný v rámci prevencie pred kybernetickými incidentmi:
   a) dodržiavať všetky bezpečnostné opatrenia definované v bezpečnostnej dokumentácii Prevádzkovateľa,
   b) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez siete a informačné systémy Dodávateľa nebolo možné ohroziť siete a informačné systémy Prevádzkovateľa,
   c) preukázateľne vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy na výkon činností a tejto zmluvy alebo budú mať prístup k dátam alebo informáciám Prevádzkovateľa,
   d) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
   e) sledovať hrozby, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,
   f) predchádzať vzniku kybernetických incidentov implementovaním najmä bezpečnostných opatrení v prostredí Dodávateľa,
   g) v prípade vzniku kybernetických incidentov v prostredí Dodávateľa, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
   h) prijímať od Prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,
   i) zasielať Prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a
   j) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Prevádzkovateľa,
   k) realizovať testovanie kontinuity činností a implementovať zistenia, vyplývajúce z výsledkov takýchto testov v dohodnutom rozsahu tejto zmluvy a SLA ,
   l) poskytovať služby osobami, ktoré majú potrebné kompetencie, znalosti a schopnosti,
   m) poskytnúť súčinnosť pri výkone auditu podľa požiadaviek zákona o kybernetickej bezpečnosti a ISO 27001:2022.

Článok VI.
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý Dodávateľovi známy a s SLA a prevádzkou IS UVZ súvisiaci kybernetický incident Prevádzkovateľovi spôsobom určeným Prevádzkovateľom, ktorý je uvedený v **Prílohe č. 2,** vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

2. Dodávateľ je povinný o celom procese riešenia bezpečnostného incidentu informovať priebežne určených zamestnancov Prevádzkovateľa.

3. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou

incidentov (ďalej len „**Reakčné opatrenia**“), a to ako na výzvu Prevádzkovateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie. Dodávateľ musí zabezpečiť všetky dôkazy súvisiace s incidentom tak, aby mohla prebehnúť analýza a vyšetrovanie bezpečnostného incidentu.

4. Dodávateľ pri reakciách na incidenty spolupracuje s Prevádzkovateľom, Národným bezpečnostným úradom a inými príslušnými orgánmi a za týmto účelom im poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami, ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.

5. Dodávateľ pri riešení a reakcii na kybernetický incident postupuje v súlade so všeobecne záväznými právnymi predpismi, touto zmluvou, ako aj svojou internou dokumentáciou tak, aby bol kybernetický incident a jeho dôsledky odstránené v čo najkratšom možnom čase.

6. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie analýzy príčiny vzniku bezpečnostného incidentu a opatrení na riešenie kybernetického incidentu a ich výsledok.

7. Po vyriešení kybernetického incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote nie kratšej ako 5 dní povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „**ochranné opatrenie**“) na schválenie.

8. Po schválení ochranného opatrenia Prevádzkovateľom je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť Prevádzkovateľovi.

9. Dodávateľ je povinný informovať Prevádzkovateľa aj o akýchkoľvek iných Dodávateľovi známych a so SLA súvisiacich skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti Prevádzkovateľa, a to zaslaním e-mailu na e-mailovú adresu .

Článok VII.
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením SLA a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa, alebo ktoré boli Prevádzkovateľom klasifikované ako interné, chránené a prísne chránené.

2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.

3. Dodávateľ je povinný chrániť všetky informácie ku ktorým má prístup na základe SLA, tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Prevádzkovateľa alebo osoby spriaznenej s Prevádzkovateľom alebo s ktorými sa pri plnení SLA a tejto zmluvy oboznámil v dôsledku vlastnej činnosti s tým, že všetci dotknutí zamestnanci Dodávateľa, jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých Dodávateľ poskytuje služby podľa SLA (ďalej len „**tretia osoba**“) sú povinní zaviazať sa k zachovávaniu mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

4. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho dotknutí zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba, a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

5. Dodávateľ je povinný zabezpečiť, aby sa každá osoba uvedená v Zozname osôb zaviazala zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti. Tento záväzok mlčanlivosti je

Dodávateľ povinný preukázať Prevádzkovateľovi u každej z týchto osôb. Pre účely tejto zmluvy postačuje záväzok mlčanlivosti zamestnancov vyplývajúci zo Zákonníka práce, interných predpisov Dodávateľa alebo príslušnej pracovnej zmluvy alebo dohody o prácach vykonávaných mimo pracovného pomeru. Fyzické osoby uvedené v Zozname osôb, ktoré nie sú zamestnancami budú mať povinnosť mlčanlivosti dohodnutú písomne.

6. Ak táto zmluva neustanovuje inak a nevylučuje to všeobecne záväzný právny predpis, zmluvné strany sa pri ochrane dôverných informácií a zachovávaní mlčanlivosti spravujú ustanoveniami článku 13. SLA. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa SLA alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

Článok VIII.
Sankcie

1. V prípade porušenia povinnosti mlčanlivosti a porušenia ostatných ustanovení tejto zmluvy je Dodávateľ povinný uhradiť Poskytovateľovi sankcie (zmluvné pokuty), ktoré sú stanovené a definované v SLA, čl. 21, pokiaľ v tejto zmluve nie je stanovená osobitná sankcia (zmluvná pokuta). Pre vylúčenie pochybností platí, že sankcie ani náhrada škody nebudú voči Dodávateľovi uplatnené duplicitne podľa SLA a tejto zmluvy.

Článok VIII.
Audit kybernetickej bezpečnosti

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. Výdavky Prevádzkovateľa spojené s vykonaním auditu znáša Prevádzkovateľ. Náklady Dodávateľa vzniknuté v rámci auditu/kontrolu podľa tohto článku Zmluvy znáša Dodávateľ, avšak len náklady za jeden audit za kalendárny rok v rozsahu práce troch (3) človekodní vykonaných zamestnancom Dodávateľa. V prípade, ak bude Prevádzkovateľ požadovať vykonanie auditu nad rámec tohto rozsahu alebo kontrolu viac ako jedenkrát (1) do roka, Prevádzkovateľ sa zaväzuje v plnom rozsahu znášať a nahradiť Dodávateľovi všetky náklady s tým spojené, v opačnom prípade je Dodávateľ oprávnený odoprieť Prevádzkovateľovi vykonanie auditu nad rámec dohodnutého rozsahu.

2. Dodávateľ sa zaväzuje, že Prevádzkovateľovi umožní kedykoľvek vykonať audit, ktorým si Prevádzkovateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností v oblasti kybernetickej bezpečnosti a tiež bude zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.

3. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní, ak sa zmluvné strany nedohodnú inak. V prípade neodstránenia zistených nedostatkov v stanovenom termíne je Dodávateľ povinný uhradiť Prevádzkovateľovi zmluvnú pokutu vo výške 300,- € za každý deň omeškania, pričom sa použije obmedzenie výšky zmluvnej pokuty podľa bodu 21.4 SLA.

4. Prevádzkovateľ môže audit u Dodávateľa realizovať sám alebo prostredníctvom písomne poverenej tretej osoby, v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu realizuje Prevádzkovateľom písomne poverená tretia osoba.

5. Dodávateľ je pri audite povinný spolupracovať s Prevádzkovateľom a sprístupniť priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku

kybernetickej bezpečnosti podľa tejto zmluvy a SLA, umožniť osobám určených Prevádzkovateľom vstup do svojich priestorov a zabezpečiť im dokumentáciu a technické vybavenie potrebné na plnenie úloh podľa tejto zmluvy a SLA.

6. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa a ďalším osobám, ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

7. 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 a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a/alebo tretích osôb o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie. Preukázanie skutočností uvedených v predchádzajúcej vete môže Dodávateľ realizovať napr. prostredníctvom predloženia relevantných certifikátov, poučení, prezenčných listín a inej dokumentácie.

8. Prevádzkovateľ je povinný oznámiť Dodávateľovi najmenej 10 pracovných dní vopred svoj zámer vykonať u Dodávateľa audit.

9. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje zodpovednosti Dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.

10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Prevádzkovateľ a osoby ním určené pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „**BOZP**") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „**PO**"), pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne bezodkladne informovať osoby určené Prevádzkovateľom o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

11. Dodávateľ je povinný poskytnúť podporu pri realizácii auditu kybernetickej bezpečnosti podľa zákona o kybernetickej bezpečnosti, ktorý bude realizovaný na základných službách Prevádzkovateľa certifikovaným audítor kybernetickej bezpečnosti ako aj podporu v prípade výkonu kontroly zo strany Národného bezpečnostného úradu najviac v rozsahu troch (3) človekodní za jeden kalendárny rok vykonaných zamestnancom Dodávateľa.

Článok IX.
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy.

2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania a riešenia kybernetických incidentov a dokumentovania školení svojich zamestnancov a ďalších osôb, ktoré sa

budú v mene Dodávateľa podieľať na plnení tejto zmluvy) a na žiadosť Prevádzkovateľa mu predložiť túto dokumentáciu.

4. V prípade, ak Dodávateľ plní SLA prostredníctvom svojich subdodávateľov, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subdodávateľov.

5. Všetky informácie, ktoré majú vplyv na plnenie tejto zmluvy sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na e-mailové adresy kontaktných osôb uvedené v záhlaví tejto zmluvy a na e-mailovú adresu .

6. Zodpovednosť za škodu vzniknutú Prevádzkovateľovi sa riadi článkom 19 SLA.

7. Po ukončení tejto zmluvy je Dodávateľ povinný podľa pokynu Prevádzkovateľa vrátiť alebo previesť na Prevádzkovateľa všetky údaje a informácie, ku ktorým mal počas trvania tejto zmluvy prístup, ako aj údaje a informácie získané v súvislosti s plnením tejto zmluvy, resp. tieto údaje a informácie zničiť, 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.

8. Dodávateľ je povinný najneskôr ku dňu ukončenia zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby. Tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu v trvaní päť rokov po ukončení zmluvného vzťahu. Ak Dodávateľ splní požiadavky čl. 12 SLA považuje sa tento bod za splnený. V prípade akéhokoľvek nesplnenia čl. 12 SLA je Dodávateľ povinný postupovať v súlade s požiadavkami definovanými v tomto bode zmluvy.

9. Dodávateľ bezodkladne po ukončení tejto zmluvy, najneskôr však do troch (3) dní, predloží Prevádzkovateľovi sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča dát, ktoré priamo alebo nepriamo súvisia s povinnosťami Dodávateľa vyplývajúcimi z tejto zmluvy, a ktoré sa týkajú Prevádzkovateľa. Prevádzkovateľ na základe sumarizácie podľa predchádzajúcej vety písomne informuje Dodávateľa o tom, ktoré podklady a informácie má Dodávateľ vrátiť Prevádzkovateľovi, previesť na Prevádzkovateľa a ktoré má zničiť. Dodávateľ je povinný splniť si povinnosť podľa predchádzajúcej vety najneskôr do piatich (5) dní odo dňa, kedy Prevádzkovateľ informoval Dodávateľa o spôsobe naloženia s týmito podkladmi a informáciami.

Článok X.
Záverečné ustanovenia

1. Táto 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, nie však skôr ako dňom nadobudnutia účinnosti SLA.

2. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania platnosti a účinnosti SLA.

3. Každá zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade uvedenom vo všeobecne záväznom právnom predpise alebo tejto zmluve. Odstúpenie od tejto zmluvy musí byť vykonané v písomnej forme, pričom odstúpenie od zmluvy musí byť riadne doručené druhej zmluvnej strane. V prípade platného odstúpenia od tejto zmluvy sa zmluva považuje na zrušenú momentom doručenia písomného odstúpenia od tejto zmluvy druhej zmluvnej strane.

4. Prevádzkovateľ je oprávnený odstúpiť od tejto zmluvy v prípade, ak Dodávateľ poruší povinnosť alebo záväzok podľa tejto zmluvy.

5. Zmluvné strany sú oprávnené vypovedať túto zmluvu aj bez udania dôvodu s výpovednou lehotou 6 mesiacov. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane .

6. Ukončením tejto zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy okrem práv a povinností, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do skončenia tejto zmluvy.

7. Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto zmluvy medzi Prevádzkovateľom a Dodávateľom je zákonnou povinnosťou Prevádzkovateľa.

8. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

9. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd Slovenskej republiky.

10. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve, ak táto zmluva neustanovuje inak.

11. Kontaktné osoby zmluvných strán a ich kontaktné údaje môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu alebo kontaktné údaje druhej zmluvnej strane v písomnej forme, pričom nie je potrebné uzatvoriť dodatok k zmluve.

12. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu neplatných alebo nevykonateľných ustanovení.

13. Neoddeliteľnou súčasťou tejto zmluvy je:
    Príloha č. 1 – Požiadavky na bezpečnostné opatrenia
    Príloha č. 2 – Spôsob hlásenia bezpečnostného incidentu
    Príloha č. 3 – Zoznam osôb a pracovných rolí Dodávateľa

14. Táto zmluva sa vyhotovuje v 4 rovnopisoch, po 2 pre každú zmluvnú stranu.

15. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave dňa .....

Za Prevádzkovateľa:

.....

V ..... dňa .....

Za Dodávateľa:

.....

Príloha č. 1 Špecifikácia a rozsah bezpečnostných opatrení

1 BEZPEČNOSTNÉ OPATRENIA – KLASIFIKÁCIA INFORMÁCIÍ A KATEGORIZÁCIA SIETÍ A INFORMAČNÝCH SYSTÉMOV

1.1 Pre oblasť klasifikácie informácií a kategorizácie sietí a informačných realizuje Dodávateľ opatrenia podľa § 4 Vyhlášky NBÚ č. 362/2018 Z.z., najmä prevádzkou systémov a sietí:

1.1.1 v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa;

1.1.2 identifikovaním a oznamovaním rozporu medzi definovanými pravidlami v bezpečnostnej dokumentácii Prevádzkovateľa a nastaveniami systémov a sietí,

1.1.3 navrhovaním spôsobov riešenia zistených rozporov,

1.1.4 dodržiavaním schválenej klasifikačnej schémy Prevádzkovateľa a správnym označovaním informačných aktív Prevádzkovateľa.

2 BEZPEČNOSTNÉ OPATRENIA – ORGANIZÁCIA KYBERNETICKEJ BEZPEČNOSTI

2.1 Pre oblasť organizácie kybernetickej bezpečnosti realizuje Dodávateľ opatrenia podľa § 5 Vyhlášky NBÚ č. 362/2018 Z.z., najmä prevádzkou systémov a sietí:

2.1.1 v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa,

2.1.2 prideľovaním najnižších privilégií pre zamestnancov Dodávateľa, identifikáciou, dokumentovaním a kontrolou činností, realizovaných zamestnancami Dodávateľa

2.1.3 prideľovaním úloh oprávneným osobám, t. j. tým, ktoré boli schválené Prevádzkovateľom a ktoré majú pridelené príslušné roly.

3 BEZPEČNOSTNÉ OPATRENIA – RIADENIE RIZÍK

3.1 Pre oblasť riadenia rizík realizuje Dodávateľ opatrenia podľa § 6 Vyhlášky NBÚ č. 362/2018 Z.z., najmä prevádzkou systémov a sietí:

3.1.1 v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa;

3.1.2 identifikáciou, oznamovaním a riadením rizík súvisiacich s prevádzkou systémov a sietí manažérovi kybernetickej bezpečnosti Prevádzkovateľa,

3.1.3 odstraňovaním identifikovaných rizík v definovaných termínoch,

3.1.4 participáciou na spracovaní a pravidelnej aktualizácii analýzy rizík a analýzy dopadov, ako aj ostatných analýz potrebných pre identifikáciu rizík spojených s prevádzkou a údržbou systémov a sietí

4 BEZPEČNOSTNÉ OPATRENIA – PERSONÁLNA BEZPEČNOSŤ

4.1 Pre oblasť personálnej bezpečnosti realizuje Dodávateľ opatrenia podľa § 7 Vyhlášky NBÚ č. 362/2018 Z.z., najmä prevádzkou systémov a sietí:

4.1.1 v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa;

4.1.2 udržiavaním vysokej úrovne bezpečnostného povedomia u zamestnancov Dodávateľa,

4.1.3 preverovaním vedomostí, znalostí, kompetencií ako aj dôveryhodnosti zamestnancov, ktorí budú participovať na službách poskytovaných Prevádzkovateľovi,

4.1.4 definovaním interných pravidiel, ktoré budú v súlade s požiadavkami bezpečnostnej dokumentácie Prevádzkovateľa.

5 BEZPEČNOSTNÉ OPATRENIA – RIADENIE PRÍSTUPOV

5.1 Pre oblasť riadenia prístupov realizuje Dodávateľ opatrenia podľa § 8 Vyhlášky NBÚ č. 362/2018, Z.z., napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.1.4 Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.

5.1.5 Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.

5.1.6 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).

5.1.7 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.

5.1.8 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 smernice Riadenie prístupov do IS a aplikácií ÚVZ SR

5.1.9 A plnením opatrení a povinností vyplývajúcich zo smernice Riadenie prístupov do IS a aplikácií ÚVZ SR.

6 BEZPEČNOSTNÉ OPATRENIA – VZŤAH S TRETÍMI STRANAMI

6.1 Pre oblasť riadenia KB a informačnej bezpečnosti vo vzťahoch s tretími stranami realizuje Dodávateľ opatrenia podľa § 9 Vyhlášky NBÚ č. 362/2018 Z.z., najmä::

6.1.1 identifikuje tretie strany, a oznamuje ich participáciu na poskytovaní služieb Prevádzkovateľovi;

6.1.2 prenáša povinnosti a zodpovednosti definované touto zmluvou na tretie strany (subdodávateľov)

6.1.3 v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa.

7 BEZPEČNOSTNÉ OPATRENIA – RIADENIE BEZPEČNOSTNÝCH SIETÍ A INFORMAČNÝCH SYSTÉMOV

7.1 Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje Dodávateľ opatrenia podľa §10 a §13 Vyhlášky NBÚ č. 362/2018, Z.z., napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

7.1.1 definovaním interných dokumentov pre riadenie zmien, riadenia kapacít Dodávateľa

7.1.2 realizáciou činností v súlade s definovanými a odsúhlasenými postupmi pre riadenie zmien a riadenie kapacít,

7.1.3 Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Dodávateľa, ktoré využíva pri poskytovaní služieb pre Prevádzkovateľa, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov.

7.1.4 Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.

7.1.5 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.

7.1.6 Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.

7.1.7 Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.

7.1.8 Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.

7.1.9 Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.

7.1.10 Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.

7.1.11 Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.

7.1.12 Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.

7.1.13 Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.

7.1.14 Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.

7.1.15 Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.

7.1.16 Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.

7.1.17 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.

7.1.18 Vyhodnocovanie informácií získaných z implementovaných nástrojov na monitoring systémov a sietí a pravidelné informovanie Prevádzkovateľa o zisteniach súvisiacich s poskytovanými službami.

7.1.19 Poskytovanie služieb v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa.

8 BEZPEČNOSTNÉ OPATRENIA – TECHNICKÉ ZRANITEĽNOSTI SYSTÉMOV A ZARIADENÍ

8.1 Pre oblasť technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 11 Vyhlášky NBÚ č. 362/2018 Z.z., najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Prevádzkovateľovi a ktoré toto poskytovanie služieb Prevádzkovateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledujúcich bodoch alebo opatrení s porovnateľným účinkom:

8.1.1 zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou služieb pre Prevádzkovateľa;

8.1.2 zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, ak sú súčasťou služieb pre Prevádzkovateľa;

8.1.3 využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

8.1.4 nahlasovanie a výkon činností súvisiacich s riešením a odstraňovaním technických zraniteľností musí byť realizované v súlade so smernicou Riadenie zraniteľností.

9 BEZPEČNOSTNÉ OPATRENIA – OCHRANA PROTI ŠKODLIVÉMU KÓDU

9.1 Pre oblasť ochrany proti škodlivému kódu realizuje Dodávateľ opatrenia podľa § 12 Vyhlášky NBÚ č. 362/2018 Z.z., najmä:

9.1.1 poskytovanie služieb v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa,

9.1.2 nasadenie systému na ochranu proti škodlivému kódu v prostredí Dodávateľa z dôvodu ochrany siete a systémov Prevádzkovateľa.

10 BEZPEČNOSTNÉ OPATRENIA – MONITOROVANIE, TESTOVANIE BEZPEČNOSTI A BEZPEČNOSTNÉ AUDITY

10.1 Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Dodávateľ opatrenia podľa § 15 Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu poskytnutia súčinnosti pri výkone auditov kybernetickej bezpečnosti Prevádzkovateľa .

10.2 Monitorovanie bezpečnosti sietí a informačných systémov Dodávateľ uskutočňuje vo svojom prostredí napríklad implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov, pričom má zabezpečený bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním a vyhodnocovaním bezpečnosti prevádzky týchto sietí a informačných systémov a to najmenej v takom rozsahu, aby nebolo ohrozené ani ovplyvnené poskytovanie základnej služby Prevádzkovateľa. V prípade zistenia ohrozenia, alebo identifikácie podozrenia na ohrozenie je Dodávateľ povinný postupovať podľa pravidiel definovaných pre nahlasovanie kybernetických bezpečnostných incidentov.

10.3 Oblasť monitorovania, testovania bezpečnosti je tiež upravená v SLA, Príloha č. 1 Špecifikácia obsahu a rozsahu Paušálnych služieb a špecifikácia spôsobu plnenia, časť B Služby profylaktiky a vykonávanie prevádzkového monitoringu a prevádzky Systému.

11 BEZPEČNOSTNÉ OPATRENIA – FYZICKÁ BEZPEČNOSŤ

11.1 Pre oblasť fyzickej bezpečnosti realizuje Dodávateľ opatrenia podľa § 15 Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu potrebnom pre poskytovanie služieb pre Prevádzkovateľa a to dodržiavaním pravidiel uvedených v bezpečnostnej dokumentácii Prevádzkovateľa, najmä smernice riadenie fyzickej bezpečnosti.

12 BEZPEČNOSTNÉ OPATRENIA – RIEŠENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV (ĎALEJ LEN „KBI“)

12.1 Pre oblasť riešenia KBI realizuje Dodávateľ opatrenia podľa § 17 Vyhlášky NBÚ č. 362/2018, Z.z., najmä deteguje a rieši KBI, ktoré môžu mať dopad na poskytovanie služieb Prevádzkovateľovi. To zahŕňa napríklad prijatie opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

12.1.1 Oboznámenie a realizácia činností v súlade s postupmi Prevádzkovateľa (najmä Smernicou o riadení bezpečnostných incidentov) pri riešení KBI a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú minimálne postupy hlásenia KBI voči Prevádzkovateľovi a sú v súlade s bezpečnostnou dokumentáciou Prevádzkovateľa.

12.1.2 Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Prevádzkovateľovi.

12.1.3 Detegovanie KBI, prostredníctvom nástroja na detekciu KBI, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.

12.1.4 Zber a vyhodnocovanie relevantných informácií o KBI prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o KBI; vyhľadávanie a zoskupovanie záznamov súvisiacich s KBI; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako KBI; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných KBI.

12.1.5 Riešenie zistených KBI a zníženie následkov zistených KBI podľa pokynov Prevádzkovateľa, analýza príčin vzniku KBI.

12.1.6 Vyhodnocovanie spôsobov riešenia KBI po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI v súčinnosti s Prevádzkovateľom.

13 BEZPEČNOSTNÉ OPATRENIA – KRYPTOGRAFICKÉ OPATENIA

13.1 Pre oblasť nasadených kryptografických opatrení Dodávateľ implementuje v IS ÚVZ požadované a potrebné opatrenia a zabezpečí prevádzku implementovaných opatrení podľa § 17a Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu potrebnom pre poskytovanie služieb pre Prevádzkovateľa a to zabezpečením dôvernosti, integrity a hodnovernosti údajov v rámci sietí a informačných systémov, bezpečným nakladaním s kryptografickými kľúčmi a certifikátmi, nastavením procesu na riadenie kľúčov a certifikátov v súlade s predmetnou vyhláškou a umožnenie kontroly a auditu správy kryptografických kľúčov a certifikátov súvisiacich s poskytovanými službami.

14 BEZPEČNOSTNÉ OPATRENIA – KONTINUITA PREVÁDZKY

14.1.1 Pre oblasť zabezpečenia kontinuity prevádzky realizuje Dodávateľ opatrenia podľa § 17b Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu potrebnom pre poskytovanie služieb pre Prevádzkovateľa v súlade s touto zmluvou a SLA a to:

a) dodržiavaním pravidiel uvedených v bezpečnostnej dokumentácii Prevádzkovateľa, najmä smernice riadenie kontinuity procesov a činností,

b) Participáciou na realizácii pravidelných testov kontinuity činností,

c) Realizáciou opatrení, ktoré vyplynuli z realizovaných testov kontinuity činností.

d) Aktualizácia plánov obnovy a plánov kontinuity činností v častiach, ktoré sa týkajú prevádzky systémov a sietí s ohľadom na realizované zmeny,

e) Zabezpečením zdrojov potrebných na realizáciu testovania tak, že v žiadnom prípade nebude ohrozená kontinuita služieb Prevádzkovateľa.

Príloha č. 2 Spôsob hlásenia bezpečnostného incidentu

1) Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v záhlaví tejto zmluvy a zároveň musí byť v komunikácii zahrnutý:
   a) Manažér kybernetickej bezpečnosti Prevádzkovateľa.
   b) Vedúci sekcie IT Prevádzkovateľa.

   a musí byť zároveň nahlásená v súlade so smernicou o riadení bezpečnostných incidentov na .

2) Pri nahlasovaní incidentu je potrebné uviesť, že sa jedná o bezpečnostný incident v zmysle tejto zmluvy a tiež kontaktnú osobu, s ktorou je možné komunikovať za účelom získania dodatočných informácií súvisiacich s procesom analýzy a riešenia bezpečnostného incidentu.

3) Samotný spôsob a forma hlásenia bezpečnostné incidentu sa bude riadiť platným predpisom Prevádzkovateľa – „Riadenie bezpečnostných incidentov“.

Príloha č. 3 Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa

Prevádzkovateľ:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou služby**	**Telefónny kontakt**	**E-mail**

Dodávateľ:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou služby**	**Telefónny kontakt**	**E-mail**
