Príloha č. 4

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:	**Národné centrum zdravotníckych informácií**
Sídlo:	Lazaretská 26, 811 09 Bratislava 1
IČO:	00165387
DIČ:	2020830119
IČ DPH:	nie je platca
v mene ktorého koná:	Mgr. Peter Lukáč, PhD., generálny riaditeľ
kontaktná osoba:	Mgr. Andrej Markovič
e-mail kontaktnej osoby:	andrej.markovic@nczisk.sk

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

a

Dodávateľom:

SKUPINA DODÁVATEĽOV v zložení:

Obchodné meno:	**Asseco Central Europe, a. s.**
Sídlo:	Galvaniho 19045/19, 821 04 Bratislava - mestská časť Ružinov
IČO:	35 760 419
v mene ktorého koná:	RNDr. Jozef Klein, predseda predstavenstva Ing. Branislav Tkáčik, člen predstavenstva
Obchodné meno:	**Asseco Central Europe, a. s.**
Sídlo:	Budějovická 778/3a, Michle, 140 00 Praha 4, ČR
IČO:	27 074 358
v mene ktorého koná:	RNDr. Jozef Klein, predseda predstavenstva Ing. Branislav Tkáčik, člen predstavenstva
Obchodné meno:	**Beset, spol. s r. o.**
Sídlo:	Jelenia 18, 811 05 Bratislava
IČO:	31 347 169
v mene ktorého koná:	RNDr. Viliam Čík, konateľ

(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 Zmluvu o poskytovaní podporných služieb – Underpinningcontract pre zabezpečenie prevádzky Informačného systému IS ESZ (ESZ a ESZ RF a RS) na základe dohodnutých cieľových úrovní podporných služieb – ServiceLevelTarget zo dňa 16.11.2017, v znení neskorších dodatkov (ďalej aj len ako „**dodávateľská zmluva**").

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 dodávateľskú zmluvu, 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.

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 dodávateľskú 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 sa mohli dotknúť Prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov Prevádzkovateľa

2. Pre účely tejto zmluvy sa za kybernetický incident považuje kybernetický bezpečnostný incident podľa zákona o kybernetickej bezpečnosti, ako aj bezpečnostná udalosť:
   a) ktorú zistí alebo o ktorej sa dozvie Dodávateľ,
   b) ktorá sa týka informačných systémov alebo sietí vo vzťahu ku ktorým Dodávateľ poskytuje výkon činností podľa dodávateľskej zmluvy,
   c) a ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k takému narušeniu kybernetickej bezpečnosti príp. integrity alebo dostupnosti služby Prevádzkovateľa, alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby Prevádzkovateľa alebo k zníženiu kvality poskytovanej služby Prevádzkovateľa.

Článok III.
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje dodržiavať Prevádzkovateľom vydané bezpečnostné smernice a štandardy, s ktorými bol Dodávateľ preukázateľne oboznámený (ďalej aj len ako „**bezpečnostná politika**") a bezpečnostné požiadavky uvedené v tejto zmluve.

2. Bezpečnostná politika Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, 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 politikou s dôrazom na zmeny v nej uvedené, pričom zmluvné strany následne potvrdia akceptáciu zmien bezpečnostnej politiky formou dodatku k tejto zmluve.

3. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa, ktoré tvoria **Prílohu č. 1** k tejto zmluve.

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 dodávateľskej zmluvy.

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 bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi v určenej lehote nie kratšej ako 5 pracovných dní.

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. 3** tejto zmluvy. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v Zozname osôb podľa tohto bodu bezodkladne na mailovú adresu kontaktnej osoby Prevádzkovateľa.

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

10. Dodávateľ môže zapojiť do poskytovania služieb na základe dodávateľskej zmluvy ďalšieho dodávateľa (subdodávateľ), ak mu to vyplýva z ustanovení dodávateľskej zmluvy počas doby jej platnosti a účinnosti.

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

12. Na výkon činností, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľskej zmluvy 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 dodávateľskej zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania dodávateľskej zmluvy.

Článok V.
Všeobecné bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

1. Dodávateľ je povinný v rámci prevencie pred kybernetickými incidentmi:
   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez siete a informačné systémy Dodávateľa nebolo možné ohroziť siete a informačné systémy Prevádzkovateľa,
   b) 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,
   c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
   d) sledovať hrozby, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,
   e) predchádzať vzniku kybernetických incidentov implementovaním najmä bezpečnostných opatrení v prostredí Dodávateľa,
   f) v prípade vzniku kybernetických incidentov v prostredí Dodávateľa, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
   g) 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,
   h) zasielať Prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a
   i) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Prevádzkovateľa.

Článok VI.
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý Dodávateľovi známy a so zmluvou 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. 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.

3. 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.

4. Dodávateľ pri riešení a reakcii na kybernetický incident postupuje v súlade so všeobecne záväznými právnymi predpismi, touto zmluvou, ako aj svojimi internými procedúrami a postupmi tak, aby bol kybernetický incident a jeho dôsledky odstránené v čo najkratšom možnom čase.

5. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.

6. Po vyriešení kybernetického incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote nie kratšej ako 5 pracovných dní povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „**ochranné opatrenie**") na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak bude navrhované ochranné opatrenie zjavne neúspešné, Dodávateľ sa zaväzuje spolupracovať s Prevádzkovateľom na návrhu nového ochranného opatrenia.

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

8. Dodávateľ je povinný informovať Prevádzkovateľa aj o akýchkoľvek iných Dodávateľovi známych a so zmluvou súvisiacich skutočnostiach, ktoré podľa názoru Dodávateľa môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti Prevádzkovateľa, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve.

Článok VII.
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením dodávateľskej zmluvy a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka 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.

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 dodávateľskej zmluvy, tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Prevádzkovateľa alebo osoby spriaznenej s Prevádzkovateľom alebo s ktorými sa pri plnení dodávateľskej zmluvy 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 dodávateľskej zmluvy (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.

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 12. dodávateľskej zmluvy. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

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 jeden (1) človekodeň vykonaný 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.

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

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 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.

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 dodávateľskú zmluvu 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 súčasne na e-mailovú adresu: csirt@nzcisk.sk.

6. Dodávateľ zodpovedá za porušenie záväzkov vyplývajúcich mu z tejto zmluvy a za škodu vzniknutú Prevádzkovateľovi v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu. Prevádzkovateľ má voči Dodávateľovi nárok na náhradu preukázanej škody, ktorá Prevádzkovateľovi vznikne v súvislosti s porušením uvedených záväzkov Dodávateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka. Zmluvné strany sa dohodli, že s prihliadnutím na ustanovenie § 379 zákona č. 513/1991 Z.z. Obchodný zákonník v znení neskorších predpisov a vzhľadom na všetky okolnosti súvisiace s predmetom tejto zmluvy, zmluvné strany konštatujú, že maximálna úhrnná predvídateľná škoda Prevádzkovateľa za akékoľvek škody, ktoré mu vzniknú na základe tejto zmluvy alebo v súvislosti s touto zmluvou, neprekročia sumu 250.000,- € (slovom: dvestopäťdesiattisíc eur). Uvedené predstavuje maximálny limit celkovej zodpovednosti Dodávateľa v zmysle zmluvných povinností Dodávateľa voči Prevádzkovateľovi podľa tejto zmluvy.

7. V prípade porušenia povinností alebo záväzkov uvedených v článku III. bod 1, článku III. bod 3, článku III. bod 6, článku VI. bod 1, v článku VIII, v článku IX. bod 10 a v článku IX. bod 11 Dodávateľom podľa tejto zmluvy, je Dodávateľ povinný Prevádzkovateľovi zaplatiť zmluvnú pokutu vo výške 1. 000,- EUR (slovom: jedentisíc eur) za každé jedno porušenie. V prípade porušenia povinností alebo záväzkov uvedených v článku III. bod 9 a v článku IV. bod 4 Dodávateľom podľa tejto zmluvy, je Dodávateľ povinný Prevádzkovateľovi zaplatiť zmluvnú pokutu vo výške 500,- EUR (slovom: päťsto eur) za každé jedno porušenie.

8. 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.

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.

10. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby podľa dodávateľskej zmluvy, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy, ak z dodávateľskej zmluvy nevyplýva dlhšia doba trvania dodávateľom udelených (poskytnutých) licencií, práv a/alebo súhlasov. Ustanovenia o autorských právach (licenciách) k výsledkom služieb Dodávateľa, ktoré sú obsiahnuté v dodávateľskej zmluve, nie sú týmto dotknuté.

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 dodávateľskej zmluvy.

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

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 za zrušenú momentom doručenia písomného odstúpenia od tejto zmluvy druhej zmluvnej strane.

4. V prípade porušenia povinností alebo záväzkov uvedených v tejto zmluve je Dodávateľ povinný tieto porušenia bezodkladne, najneskôr však do 30 dní odstrániť. V prípade, ak Dodávateľ v dodatočnej lehote porušenie neodstráni je Prevádzkovateľ oprávnený odstúpiť od tejto zmluvy. Prevádzkovateľ je oprávnený okamžite odstúpiť od tejto zmluvy v prípade, ak Dodávateľ poruší povinnosti alebo záväzky uvedené v článku III. bod 1, článku III. bod 3, článku III. bod 6, článku VI. bod 1 a v článku VIII. podľa tejto zmluvy.

5. Zmluvné strany sú oprávnené vypovedať túto zmluvu aj bez udania dôvodu s výpovednou lehotou 3 mesiace. 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 09. 06. 2023

Za Prevádzkovateľa:

[redacted]

Mgr. Peter Lukáč, PhD.
generálny riaditeľ
Národné centrum zdravotníckych informácií

V Bratislave dňa 08. JÚN 2023

Za Dodávateľa:

[redacted]

RNDr. Jozef Klein
predseda predstavenstva
Asseco Central Europe, a. s.,Bratislava

[redacted]

Ing. Branislav Tkáčik
člen predstavenstva
Asseco Central Europe, a. s.,
Bratislava

[redacted]

RNDr. Jozef Klein
predseda predstavenstva
Asseco Central Europe, a. s., Praha

Ing. Branislav Tkáčik
člen predstavenstva
Asseco Central Europe, a. s., Praha

RNDr. Viliam Čík
konateľ
Beset, spol. s r. o.

Príloha č. 1 Špecifikácia a rozsah bezpečnostných opatrení

1 BEZPEČNOSTNÉ OPATRENIA – TECHNICKÉ ZRANITEĽNOSTI SYSTÉMOV A ZARIADENÍ

1.1 Pre oblasť technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 9 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:

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

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

1.1.3 Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2 BEZPEČNOSTNÉ OPATRENIA – RIADENIE BEZPEČNOSTNÝCH SIETÍ A INFORMAČNÝCH SYSTÉMOV

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

2.1.1 Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Prevádzkovateľa, 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; servery so službami pre Prevádzkovateľa 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.

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

2.1.3 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.

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

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

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

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

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

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

2.1.10 Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.

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

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

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

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

2.1.15 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.

3 BEZPEČNOSTNÉ OPATRENIA – RIADENIE PRÍSTUPOV

3.1 Pre oblasť riadenia prístupov realizuje Dodávateľ opatrenia podľa § 12 Vyhlášky NBÚ č. 362/2018, Z.z., napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

3.1.1 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.

3.1.2 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.

3.1.3 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.

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

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

3.1.6 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).

3.1.7 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.

3.1.8 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 bezpečnostnej politiky.

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

4.1 Pre oblasť riešenia KBI realizuje Dodávateľ opatrenia podľa § 14 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:

4.1.1 Oboznámenie sa s postupmi Prevádzkovateľa pri riešení KBI a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú minimálne postupy hlásenia KBI voči Prevádzkovateľovi.

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

4.1.3 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.

4.1.4 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.

4.1.5 Riešenie zistených KBI a zníženie následkov zistených KBI podľa pokynov Prevádzkovateľa.

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

5 BEZPEČNOSTNÉ OPATRENIA – MONITOROVANIE, TESTOVANIE BEZPEČNOSTI A BEZPEČNOSTNÉ AUDITY

5.1 Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Dodávateľ opatrenia podľa § 15 Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu potrebnom pre poskytovanie služieb pre Prevádzkovateľa. Monitorovanie bezpečnosti sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu:

5.1.1 sieťových prvkov a serverov, ak sú súčasťou služieb pre Prevádzkovateľa,

5.1.2 služieb prístupných do externých sietí, ak sú súčasťou služieb pre 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.

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	Email
Mgr. Andrej Markovič	Manažér KB	Riadenie informačnej a kybernetickej bezpečnosti		andrej.markovic@nczisk.sk
Erik Kopáčik	SLA manažér	Osoba zodpovedná za SLA		erik.kopacik@nczisk.sk

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	Email
RNDr. Slavomír Vričan	Špecialista KB	Riadenie informačnej a kybernetickej bezpečnosti		slavomir.vrican@asseco-ce.com
Bc. Brigita Leginusová	SLA manažér	Osoba zodpovedná za SLA		brigita.leginusova@asseco-ce.com