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:	.....
zapísaným:	.....
v mene ktorého koná:	.....
kontaktná osoba:	.....
e-mail kontaktnej osoby:	.....
hlásenie incidentov – email:	... mkb@nczisk.sk.....

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

a

Dodávateľom:

Obchodné meno:	.....
Sídlo:	.....
IČO:	.....
DIČ:	.....
IČ DPH:	.....
zapísaným:	.....
v mene ktorého koná:	.....
kontaktná osoba:	.....
e-mail kontaktnej osoby:	.....
hlásenie incidentov – email:	.....

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

Článok II.
Úvodné ustanovenia a vyhlásenia

1. Prevádzkovateľ je podľa § 3 písm. l) 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. k) zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona

o kybernetickej bezpečnosti dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby.

2. 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**“) zmluvné strany uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**zmluva**“).

3. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na Zmluvu o poskytovaní podporných služieb pre zabezpečenie prevádzky informačných systémov ESZ a ESZ RFaRS zo dňa ..... (ďalej aj len ako „**dodávateľská zmluva**“), na základe ktorej Dodávateľ bude poskytovať Prevádzkovateľovi výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby.

Článok III.
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 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 IV.
Práva a povinnosti zmluvných strán

1. Poskytovateľ sa zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa, Prevádzkovateľom vydané bezpečnostné smernice a štandardy, ktorými bol Dodávateľ preukázateľne oboznámený, formou elektronickej pošty alebo zápisom (ďalej aj len ako „**bezpečnostná politika**“), a požiadavky na bezpečnosť definované zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon o KB**“), zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon o ITVS**“), vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (ďalej len „**Vyhláška o BOITVS**“), vyhláškou Úradu

podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v platnom znení (ďalej len „**Vyhláška o štandardoch pre ITVS**“) ako aj ostatnými všeobecne záväznými právnymi predpismi platnými v čase plnenia tejto zmluvy a bezpečnostné požiadavky uvedené v tejto zmluve. Platnú bezpečnostnú politiku Prevádzkovateľ poskytne Prevádzkovateľ Dodávateľovi po nadobudnutí účinnosti tejto zmluvy.

2. Dodávateľ súhlasí s tým, že 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 Dodávateľ následne preukázateľne potvrdí akceptáciu zmien bezpečnostnej politiky.

3. Dodávateľ sa zaväzuje prijímať a dodržiavať najmenej bezpečnostné opatrenia Prevádzkovateľa, ktoré tvoria **Prílohu č. 1** k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami Prevádzkovateľa.

4. Dodávateľ súhlasí s tým, že 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. Dodávateľ sa zaväzuje dodržiavať takto zmenené alebo doplnené bezpečnostné opatrenia Prevádzkovateľa od okamihu, v ktorom ho s nimi Prevádzkovateľ preukázateľne oboznámi.

5. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú v súlade s bezpečnostnou politikou Prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v Prílohe č. 1 tejto zmluvy. Dodávateľ vyhlasuje, že s bezpečnostnými opatreniami súhlasí.

6. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti počas celej doby trvania tejto zmluvy, pokiaľ zo všeobecne záväzných právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľskej zmluvy.

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

8. 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.

9. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy v oblastiach podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa § 9, § 10, § 12 § 14 a § 15 vyhlášky a v rozsahu špecifikovanom v bezpečnostnej politike Prevádzkovateľa.

10. 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.

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

12. 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. V prípade zapojenia subdodávateľa, musí dodávateľ garantovať dodržiavanie bezpečnostných opatrení vyplývajúcich z tejto zmluvy aj subdodávateľom.

13. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

14. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek kladených na Prevádzkovateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve.

15. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany“ v zmysle zákona o kybernetickej bezpečnosti.

16. Ostatný konkrétny rozsah činnosti Dodávateľa je stanovený dodávateľskou zmluvou.

Článok V.
Okolnosti plnenia zmluvy

1. Výklad pojmov používaných v tejto zmluve sa nesmie dostať do rozporu s významom, ktorý im je priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

2. 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 zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.

3. 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.

4. Dodávateľ nemá nárok na žiadnu odplatu ani náhradu výdavkov za plnenie záväzkov podľa tejto zmluvy.

Článok VI.
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 zasiahnuť 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,
d. preukázateľne Vykonávať poučenia o povinnostiach v oblasti kybernetickej bezpečnosti pre oprávnené osoby a pracovníkov Dodávateľa, ktorí budú vykonávať pre Prevádzkovateľa činnosti súvisiace s plnením tejto Zmluvy a o tomto poučení musí Poskytovateľ vytvoriť záznam, ktorý bude podpísaný poučenou osobou a osobou, ktorá poučenie vykonala, pričom za riadne poučenie zodpovedá Dodávateľ,
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 VII.
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident Prevádzkovateľovi spôsobom určeným Prevádzkovateľom, ktorý je uvedený v **Prílohe č. 2.** 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, 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 oznámiť Prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.
6. Dodávateľ je povinný v čase kybernetického incidentu, ktorý mal dopad na Prevádzkovateľa, zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho Prevádzkovateľovi.
7. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.

8. Po vyriešení kybernetického incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote 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 je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom na návrhu nového ochranného opatrenia.
9. Po schválení ochranného opatrenia Prevádzkovateľom je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť Prevádzkovateľovi.
10. Dodávateľ je povinný informovať Prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti.

Článok VIII.
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy na výkon činností 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 dodávateľskej zmluvy, tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Prevádzkovateľa alebo osoby spriaznenej s Prevádzkovateľom alebo s ktorými sa 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 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. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

Článok IX.
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.

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.

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

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 voľný 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 tretiu osobu 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. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

11. 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**"), s ktorými boli v súlade s týmto bodom, 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 Objednávateľom 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 X.
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, bezpečnostnými štandardmi, znalostnými štandardmi v oblasti kybernetickej bezpečnosti, operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenie kybernetických incidentov.

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 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.

6. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie alebo porušenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť Prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, Dodávateľ zodpovedá v celom rozsahu za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky a za dôsledky a škodu vzniknutú Prevádzkovateľovi alebo akejkoľvek tretej osobe 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 preukázateľnej škody, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením uvedených

záväzkov Dodávateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka.

7. V prípade porušenia povinnosti alebo záväzku Dodávateľa vyplývajúceho mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky, je Dodávateľ povinný Prevádzkovateľovi základnej zaplatiť zmluvnú pokutu vo výške 15 000,- EUR; nárok Prevádzkovateľa na náhradu škody v plnej výške, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením povinností Dodávateľa, tým nie sú dotknuté.

8. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

9. 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.

10. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom; tento záväzok trvá po dobu najmenej 5 rokov po ukončení tejto zmluvy. Ustanovenia o autorských právach (licenciách) k výsledkom služieb Dodávateľa, ktoré sú obsiahnuté v dodávateľskej zmluve, nie sú týmto dotknuté.

Článok XI.
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 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 je možné vykonať 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 akúkoľvek povinnosť alebo záväzok plynúci mu z tejto zmluvy.

5. Prevádzkovateľ je oprávnený 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 doručená výpoveď Dodávateľovi.

6. Platným ukončením zmluvy podľa tohto článku zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy okrem povinností zachovávať, ktoré sú účinné po dobu desiatich rokov od ukončenia tejto zmluvy a okrem práv a povinností, z ktorých povahy je zrejmé, že majú trvať aj po zániku zmluvy.

7. 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.

8. 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.

9. 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.

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

11. 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.

12. 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

13. Táto zmluva sa vyhotovuje v 2 rovnopisoch, po 1 pre každú zmluvnú stranu.

14. 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

Požiadavky na bezpečnostné opatrenia

Bezpečnostné opatrenia dodávateľa sú rozdelené do nasledovných dvanástich oblastí:

1) **Fyzická bezpečnosť** - opatrenia fyzickej bezpečnosti popisujú bezpečnostné opatrenia, ktoré sú navrhnuté tak, aby zabránili neautorizovanému prístupu do budov, k zariadeniam a pod. a chránili osoby a zariadenia proti napadnutiu, zničeniu alebo inej ujme (napríklad špionáž, krádež, alebo teroristický útok). Najmä sa jedná o nasledujúce oblasti a k nim prislúchajúce opatrenia:
    a) Procesné a personálne riadenie fyzickej bezpečnosti;
    b) Bezpečnostná klasifikácia a zónovanie budov a lokalít z hľadiska bezpečnosti a prístupov;
    c) Mechanická a elektronická ochrana lokalít;
    d) Monitoring prístupu do lokalít;
    e) Ochrana aktív a majetku proti požiaru a prírodným katastrofickým javom

2) **Ochrana údajov** – opatrenia ochrany údajov zavádzajú klasifikáciu údajov spoločnosti, ďalej tiež definujú a popisujú pravidlá a povinnosti zamestnancov a dodávateľov pri nakladaní so služobnými informáciami a tiež zavádzajú kontrolné mechanizmy, ktoré umožnia zamedziť zneužitiu klasifikovaných údajov. Najmä sa jedná o nasledujúce oblasti a k nim prislúchajúce opatrenia:
    a) Procesné a personálne riadenie ochrany údajov;
    b) Proces klasifikácie a označovania osobných údajov;
    c) Implementácia technických opatrení na ochranu údajov.

3) **Riadenie identít a prístupov** – opatrenia ochrany riadenia identít a prístupov popisujú bezpečnostné opatrenia s cieľom zabezpečiť jednotnú a efektívnu metodiku riadenia fyzických a logických prístupov identít a zamedziť neautorizovaným prístupom k zariadeniam a informáciám. Najmä sa jedná o nasledujúce oblasti a k nim prislúchajúce opatrenia:
    a) Procesné a personálne riadenie identít a prístupov;
    b) Oddelenie povinností (segregation of duties);
    c) Procesné riadenie prístupových práv k IS a službám;
    d) Riadenie prístupov privilegovaných účtov;
    e) Vzdialený prístup a minimálne požiadavky na bezpečnosť koncových bodov.

4) **Riadenie rizík aktív** – opatrenia riadenia rizík súvisiacich s aktívami definujú mechanizmus identifikácie, vyhodnotenia a stanovenia priorít rizík za účelom minimalizácie, monitorovania a riadenia pravdepodobností a dosahov negatívnych udalostí na aktíva a procesy organizácie. Pre riadenie rizík sa jedná najmä o nasledujúce oblasti a k nim prislúchajúce opatrenia:
    a) Procesné a personálne zabezpečenie riadenia rizík aktív;
    b) Zavedenie zoznamu rizík;
    c) Proces pravidelného prehodnocovania rizík;
    d) Plán implementácie opatrení pre minimalizáciu rizík.

5) **Riadenie informačných bezpečnostných incidentov** – opatrenia riadenia bezpečnostných incidentov popisujú opatrenia s cieľom zabezpečiť jednotný a účinný

spôsob riadenia bezpečnostných incidentov, vrátane evidencie o bezpečnostných incidentoch a príčinách. Riadenie bezpečnostných incidentov v IS obsahuje najmä tieto oblasti a k nim prislúchajúce opatrenia:

a) Procesné riadenie informačných bezpečnostných incidentov;
b) Klasifikácia incidentov;
c) Zavedenie a prevádzka Security Operation Center;
d) Proces poučenia z riešených incidentov.

6) **Sieťová bezpečnosť** – opatrenia sieťovej bezpečnosti popisujú bezpečnostné opatrenia prijaté na prevenciu a kontrolu neoprávneného prístupu, zneužitia, modifikácie počítačových sietí a sieťovo prístupných zdrojov a služieb. Zabezpečenie siete zahŕňa tiež opatrenia na riadenie autorizovaných prístupov k údajom v sieti. Jedná sa najmä o nasledujúce oblasti a k nim prislúchajúce opatrenia:
   a) Procesné riadenie vnútorných a telekomunikačných sietí;
   b) Bezpečnosť webových serverov, poskytovaných a publikovaných služieb;
   c) Zónovanie a monitoring sietí;
   d) Aktívna ochrana proti sieťovým útokom a útokom na všetkých vrstvách ISO/OSI modelu

7) **Prevádzková bezpečnosť** – opatrenia prevádzkovej bezpečnosti popisujú bezpečnostné opatrenia, ktoré sú navrhnuté tak, aby procesy organizácie, prevádzka aktív a operácie s údajmi boli efektívne z hľadiska využívania zdrojov a z hľadiska plnenia požiadaviek organizácie. V tejto súvislosti sa jedná najmä o nasledujúce oblasti a k nim prislúchajúce opatrenia:
   a) Procesné riadenie prevádzkovej bezpečnosti;
   b) Politika oddelenia vývojových, testovacích a produkčných prostredí;
   c) Opatrenia proti škodlivému kódu a ochrana proti útokom zabezpečujúcim odopretie služby;
   d) Kontrola implementácie a prevádzky autorizovaného softvéru;
   e) Auditné záznamy a ich analýza;
   f) Záloha a obnova;
   g) Monitorovanie prevádzky;
   h) Kontrola a správa zraniteľností.

8) **Bezpečnosť vo vývoji, obstarávaní alebo údržbe** – opatrenia bezpečnosti vo vývoji IS a aplikácií popisujú a zavádzajú také bezpečnostné opatrenia, aby zabezpečili adekvátnu ochranu aplikácii a údajov v nich, za účelom ochrany aktív, procesov a organizácie celom cykle životnosti daného IS alebo aplikácie. Bezpečný vývoj, akvizícia, dodávka alebo údržba musí zohľadňovať najmä nasledujúce oblasti a k nim prislúchajúce opatrenia:
   a) Procesné riadenie bezpečnosti vo vývoji, akvizícii, dodávke alebo údržbe;
   b) Analýza a riadenie rizík citlivých projektov;
   c) Riadenie rizík a a proces schvaľovania zvyškových rizík;
   d) Proces implementácie bezpečnostných opatrení v projektoch;
   e) Implementácia bezpečných a bezpečnostných postupov prie vývoj;
   f) Technické overovanie pred spustením produkčnej prevádzky;
   g) Bezpečnostné štandardy a najlepšie praktiky.

9) **Ochrana osobných údajov** – opatrenia ochrany osobných údajov popisujú pravidlá a povinnosti zamestnancov a dodávateľov pri nakladaní s osobnými údajmi a tiež

stanovujú kontrolné mechanizmy, ktoré zabraňujú zneužitiu osobných údajov. Jedná sa najmä o nasledujúce oblasti a k nim prislúchajúce opatrenia:

a) Procesné a personálne zabezpečenie riadenia ochrany osobných údajov v zmysle platnej legislatívy;
b) Proces evidencie a klasifikácie osobných údajov;
c) Proces posudzovania a riešenia rizík súvisiacich s osobnými údajmi a vykonávanie DPIA v súlade s nariadením GDPR.

10) **Riadenie kontinuity činností a riadenie krízových situácií** – opatrenia biznis kontinuity a krízového riadenia definujú riadený proces, podporovaný vedením organizácie, ktorý identifikuje potenciálne dopady a straty. Cieľom je vytvoriť také postupy a prostredie, ktoré umožní zaistiť nepretržitú kontinuitu a efektívnu obnovu kľúčových procesov a činností organizácie, na vopred stanovenej úrovni, v prípade ich narušenia alebo straty. V súvislosti s riadením kontinuity procesov a krízového riadenia sa jedná najmä o nasledujúce oblasti a k nim prislúchajúce opatrenia:
    a) Procesné riadenie nepretržitej dostupnosti a prevádzky obchodných a procesných činností organizácie;
    b) Proces analýzy dopadov na činnosti organizácie (BIA);
    c) Proces tvorby a revízie plánov zabezpečenia kontinuity procesov a činností organizácie a krízového riadenia;
    d) Proces testovania a revízie plánov zabezpečenia kontinuity činností organizácie a krízového riadenia.

11) **Obnova prevádzky/ Disaster recovery** – opatrenia v oblasti obnovy prevádzky definujú zásady a postupy, ktoré umožnia prevádzkovať životne dôležitú technologickú infraštruktúru a systémy aj po vzniku prírodných alebo človekom vyvolaných krízových udalostí. Jedná sa najmä o nasledujúce oblasti a k nim prislúchajúce opatrenia:
    a) Procesné a organizačné riadenie obnovy prevádzky;
    b) Proces analýzy dopadov na činnosti organizácie (BIA);
    c) Proces tvorby a revízie plánov pre obnovu prevádzky;
    d) Proces testovania plánov pre obnovu prevádzky.

12) **Riadenie zhody** – opatrenia riadenia zhody (compliance) popisujú bezpečnostné opatrenia, ktoré sú navrhnuté tak, aby nedošlo k porušeniu právnych, normatívnych alebo zmluvných záväzkov týkajúcich sa informačnej bezpečnosti a všetkých bezpečnostných požiadaviek. Najmä sa jedná o program auditu a jeho naviazanie na akčné plány.

Príloha č. 2

Spôsob hlásenia bezpečnostného incidentu

1) Hlásenie incidentov a následná komunikácia prebieha medzi jednotlivými stranami zasielaním na kontaktné elektronické adresy uvedené 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.

Príloha č. 3

Zoznam osôb a pracovných rolí Dodávateľa