Číslo zmluvy objednávateľa:

Číslo zmluvy poskytovateľa:

DODATOK č. 1 k SERVISNEJ ZMLUVE

(„Zmluva o poskytovaní služieb pre prevádzku a údržbu informačných systémov Mesta Prešov“) zo dňa 14.11.2018 (ďalej len ako „Dodatok“)

I. ZMLUVNÉ STRANY

Objednávateľ:	**obchodné meno:**	**Mesto Prešov**
	sídlo:	**Hlavná 73, 080 01 Prešov**
	Zastúpený: **Oprávnení k podpisu zmluvy:**	Ing. František Oľha, primátor mesta
	Osoba oprávnená na jednanie v technických veciach:	Ing. Ľubomír Hleba, oddelenie IT
	e-mail:	it@presov.sk
	IČO:	00327646
	DIČ:	2021225679
	IČ DPH:	
	bankové spojenie:	UniCredit Bank
	IBAN:	SK05 1111 0000 0066 1991 1008
	SWIFT(BIC):	
	zápis v registri:	
	(ďalej v texte len „objednávateľ“)	

Poskytovateľ:	**obchodné meno:**	**CORA GEO, s. r. o.**
	sídlo:	**A. Kmeťa 5397/23, 036 01 Martin**
	právna forma:	Spoločnosť s ručením obmedzeným
	prevádzka:	Štefánikova 15, 058 01 Poprad
	Štatutárny zástupca :	Ing. Jozef Habiňák, konateľ spoločnosti
	Zástupcovia vo veciach technických a zmluvných:	Ing. Pavel Kollár, account manažér
	email:	obchod@corageo.sk
	IČO:	31 612 989
	DIČ:	2020433888
	IČ DPH:	SK2020433888
	bankové spojenie:	Tatra banka, a.s.
	IBAN:	SK67 1100 0000 0029 4808 5378
	SWIFT(BIC):	TATRSKBX
	zápis v registri:	Zapísaná v Obchodnom registri Okresného súdu Žilina, Oddiel: Sro, Vložka č. 2134/L
	(ďalej v texte len „poskytovateľ“)	

objednávateľ a poskytovateľ ďalej len ako „zmluvné strany“

II. ÚVODNÉ USTANOVENIA

1. Zmluvné strany uzatvorili dňa 14.11.2018 SERVISNÚ ZMLUVU („**Zmluva o poskytovaní služieb pre prevádzku a údržbu informačných systémov Mesta Prešov**“) ďalej na účely tohto Dodatku len ako „**Servisná zmluva**“.
2. Objednávateľ je podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej na účely tohto Dodatku len ako „**Zákon**“) prevádzkovateľom základnej služby. Servisná zmluva je podľa § 19 Zákona zmluvou na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre objednávateľa ako prevádzkovateľa základnej služby.
3. Účelom tohto Dodatku je zabezpečiť splnenie Zákonom ustanovenej povinnosti objednávateľa ako prevádzkovateľa základnej služby mať uzatvorenú zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona s poskytovateľom ako treťou stranou tak ako ju definuje Zákon počas celej doby platnosti Servisnej zmluvy, ktoré priamo súvisia so zabezpečením prevádzky a využívaním informačných systémov poskytovateľa (Informačný systém samosprávy, geografický informačný systém a riešenie pre podporu eGovernmentu ďalej spolu na účely tohto Dodatku len „**Informačné systémy CG**“) pre objednávateľa ako prevádzkovateľa základnej služby.
4. Zmluvné strany vyhlasujú, že práva a povinnosti vyplývajúce zmluvným stranám z tohto Dodatku sa vzťahujú výlučne k základnej službe poskytovanej objednávateľom ako prevádzkovateľom základnej služby a to výlučne vo vzťahu k tým aplikačným informačným systémom, ktoré dodal poskytovateľ pre objednávateľa ako poskytovateľa základnej služby a teda pre poskytovateľom dodané Informačné systémy CG, vo vzťahu ku ktorým poskytovateľ poskytuje prevádzkovateľovi základnej služby servis a podporu v súlade so Servisnou zmluvou a súčasne výlučne vo vzťahu k informačným systémom poskytovateľa prostredníctvom, ktorých poskytovateľ poskytuje objednávateľovi ako prevádzkovateľovi základnej služby servis a podporu pre Informačné systémy CG a to za podmienok a spôsobom bližšie špecifikovaným v tomto Dodatku.

III. PREDMET DODATKU

1. Predmetom tohto Dodatku je dohoda zmluvných strán o doplnení Servisnej zmluvy o náležitosti špecifikované v § 8 ods. 2 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej na účely tohto Dodatku len „**Vyhláška**“) v nadväznosti na bezpečnostné opatrenia najmenej v rozsahu podľa § 8 ods. 3 Vyhlášky a to za účelom, aby Servisná zmluva plnila účinnosťou tohto Dodatku súčasne obsah zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa § 19 ods. 2 Zákona.
2. Uzatvorením tohto Dodatku sa čl. X. Záverečné ustanovenia Servisnej zmluvy dopĺňa a to v bode ustanovenia X.7 ktoré bude znieť nasledovne:

X.7 Neoddeliteľnou súčasťou tejto Servisnej zmluvy sú nasledovné prílohy:
Príloha č. 1 Zoznam modulov pre UPDATE, všetky v rozsahu multilicencia
Príloha č. 2 Rozsah planenia a detailná cenová kalkulácia pre rok 2019
Príloha č. 3 Cenník služieb pre rok 2019
Príloha č. 4 Technická špecifikácia pre rok 2019
Príloha č. 5 Údaje o subdodávateľoch
Príloha č. 6 Bezpečnostné opatrenia a iné povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášku Národného bezpečnostného úradu č. 362/2018 Z. z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

3. Uzatvorením tohto Dodatku sa Servisná zmluva dopĺňa o novú prílohu č. 6 s označením Bezpečnostné opatrenia a iné povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášku Národného bezpečnostného úradu č. 362/2018 Z.z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ktorá znie nasledovne:

Príloha č. 6 - Bezpečnostné opatrenia a iné povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášku Národného bezpečnostného úradu č. 362/2018 Z. z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Príloha č. 6“)

Pojmy aplikované v tejto Prílohe č. 6 sú pojmami tak ako sú definované v § 3 na účely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

1. Povinnosť poskytovateľa dodržiavať bezpečnostnú politiku objednávateľa ako prevádzkovateľa základnej služby a povinnosť poskytovateľa dodržiavať a prijať bezpečnostné opatrenia.

1.1 Poskytovateľ sa zaväzuje dodržiavať platné bezpečnostné politiky objednávateľa ako prevádzkovateľa základnej služby, ktoré sú normatívne upravené v dokumentoch objednávateľa ako prevádzkovateľa základnej služby a to od momentu kedy bude s nimi poskytovateľ riadne oboznámený. Riadnym oboznámením sa s obsahom bezpečnostných politík podľa predchádzajúcej vety sa rozumie protokolárne odovzdanie dokumentov, ktoré má poskytovateľ dodržiavať a s ktorými sa poskytovateľ oboznámi pred podpisom tohto Dodatku.
1.2 Poskytovateľ vyhlasuje, že sa s bezpečnostnou politikou objednávateľa ako prevádzkovateľa základnej služby oboznámil a vyjadruje súhlas s bezpečnostnou politikou prevádzkovateľa základnej služby. Bezpečnostná politika objednávateľa ako prevádzkovateľa základnej služby je uvedená v Doložke č. 1 k tejto Prílohe č. 6, ktorú

poskytovateľ protokolárne prevzal od objednávateľa ako prevádzkovateľa základnej služby pred podpisom tohto Dodatku.

1.3 Poskytovateľ sa zaväzuje dodržiavať a prijať bezpečnostné opatrenia vo vzťahu k dodaným Informačným systémom CG, vo vzťahu ku ktorým poskytovateľ poskytuje prevádzkovateľovi základnej služby Ročnú podporu v súlade s ustanoveniami Servisnej zmluvy a súčasne výlučne vo vzťahu k informačným systémom poskytovateľa, prostredníctvom ktorých poskytovateľ poskytuje objednávateľovi ako prevádzkovateľovi základnej služby Ročnú podporu pre Informačné systémy CG a to pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) Zákona. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie objednávateľa, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

1.4 Zmluvné strany sa dohodli, že objednávateľ ako prevádzkovateľ základnej služby prehlasuje, že Informačné systémy CG prevádzkuje a spravuje prevádzkovateľ základnej služby samostatne na vlastných sieťach (serveroch) bez toho, aby k nim mal poskytovateľ osobitný prístup. Pre vylúčenie pochybností sa ustanovenia tejto Prílohy č. 6 a tejto Servisnej zmluvy vzťahujú len po dobu (v čase) realizácie služby Ročná podpora prostredníctvom vzdialenej správy zo strany poskytovateľa a vo vzťahu k samotnej funkčnosti dodaných Informačných systémov CG, prostredníctvom ktorej sú realizované služby podľa čl. II. Servisnej zmluvy bod II.7, II.9 a II.10.

2. Špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma poskytovateľ a vyjadrenie súhlasu s nimi:

2.1 **Bezpečnostné opatrenia pre oblasť riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s poskytovateľom ako treťou stranou:**
Poskytovateľ identifikuje technické zraniteľností informačných systémov a zariadení vo vzťahu k poskytovanej Ročnej podpore najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb objednávateľovi ako prevádzkovateľovi základnej služby prostredníctvom nasledujúcich opatrení, ak sú relevantné:

a. zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
b. zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
c. využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2.2 **Bezpečnostné opatrenia pre oblasť riadenia bezpečnosti sietí a informačných systémov vo vzťahu k poskytovanej Ročnej podpore:**
Poskytovateľ realizuje nasledovné opatrenia, ak sú relevantné:

a. Riadenie bezpečného prístupu medzi informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu informačných systémov, ktoré sú zabezpečené segmentáciou informačných systémov.
b. Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
c. Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.

d. Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
e. Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
f. Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
g. Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
h. Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.

2.3 **Bezpečnostné opatrenia pre oblasť ochrany proti škodlivému kódu a pre oblasť riadenia prístupov vo vzťahu k poskytovanej Ročnej podpore realizuje poskytovateľ** nasledovné opatrenia:
a. Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci Informačných systémov CG, ktoré sú nevyhnutné na plnenie zverených úloh používateľa.
b. Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
c. Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej (i) vypracovanie zásad riadenia prístupu k informáciám; (ii) riadenia prístupu používateľov; (iii) zodpovednosti používateľov; (iv) riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; (v) prístupu k aplikáciám; (vi) monitorovania prístupu a používania informačného systému a (vii) riadenia vzdialeného prístupu.
d. Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
e. Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
f. 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.
g. 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.

2.4 Bezpečnostné opatrenia pre oblasť akvizície, vývoja a údržby informačných sietí a informačných systémov a pre oblasť riešenia kybernetických bezpečnostných incidentov vo vzťahu k zabezpečeniu služieb Ročnej podpory a počas povoleného času prístupu do siete objednávateľa ako prevádzkovateľa základnej služby realizuje poskytovateľ nasledovné opatrenia: Poskytovateľ najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať priamy dopad na výkon činnosti pre objednávateľa ako prevádzkovateľa základnej služby, ak sú relevantné:
a. Oboznámenie sa s postupmi prevádzkovateľa základnej služby pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne

postupy hlásenia kybernetických bezpečnostných incidentov voči prevádzkovateľovi základnej služby.

2.5 Bezpečnostné opatrenia pre oblasť zaznamenávania udalostí a monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje poskytovateľ: opatrenia podľa § 15 Vyhlášky najmä implementuje centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb objednávateľa ako prevádzkovateľa základnej služby.

2.6 Špecifikácia a rozsah bezpečnostných opatrení vymedzených v tomto článku Prílohy č. 6 je dohodnutý zmluvnými stranami len rámcovo. Zmluvné strany sa zaväzujú dodatočne doplniť konkrétne bezpečnostné opatrenia, ktoré bude musieť tá-ktorá zmluvná strana plniť, podľa záverov, ktoré vyplývajú z Analýzy rizík zo strany prevádzkovateľa základnej služby, ktoré bude musieť tá-ktorá zmluvná strana plniť a ktoré budú uvedené v Doložke č. 2 k tejto Prílohe č. 6 k Servisnej zmluve. V Doložke č. 2 k tejto Prílohe č. 6 k Servisnej zmluve budú popri konkrétnych bezpečnostných opatreniach v zmysle zákona č. 69/2018 Z. z. identifikované aj osoby zodpovedné za plnenie konkrétnych bezpečnostných opatrení.

2.7 Zmluvné strany si prostredníctvom technických zástupcov dohodnú a protokolárne potvrdia presné technické špecifikácie konkrétnych bezpečnostných opatrení, ktoré vyplývajú z interných bezpečnostných opatrení objednávateľa ako prevádzkovateľa základnej služby a to na základe zrealizovanej Analýzy rizík zo strany prevádzkovateľa základnej služby, ktoré budú uvedené v Doložke č. 2 k Prílohe č. 6 k Servisnej zmluve po podpise tohto Dodatku. Do protokolárneho potvrdenia obidvoma zmluvnými stranami Doložky č. 2 k Prílohe č. 6 k Servisnej zmluve nie je poskytovateľ v omeškaní s plnením opatrení špecifikovaných v tomto článku. Bezpečnostné opatrenia v súlade s týmto článkom prijíma samotný poskytovateľ v primeranom rozsahu podľa vlastného rozhodnutia, tak aby bol naplnený účel zákona č. 69/2018 Z. z.. Objednávateľ ako prevádzkovateľ základnej služby do bezpečnostných opatrení poskytovateľa nijako nezasahuje.

2.8 Objednávateľ ako prevádzkovateľ základnej služby berie na vedomie, že aplikácií bezpečnostných opatrení bude aplikovaná len na Informačné systémy CG dodané poskytovateľom a na tie časti siete, na ktoré má poskytovateľ reálny dosah.

3. Rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu objednávateľom ako prevádzkovateľom základnej služby u poskytovateľa

3.1 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený vykonávať kontrolnú činnosť a audit u poskytovateľa, a to v rozsahu a za účelom kontroly plnenia povinnosti poskytovateľa v zmysle Zákona a tohto dodatku.

3.2 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený vykonať kontrolnú činnosť a/alebo audit u poskytovateľa prostredníctvom poverenej osoby, ktorej identifikačné údaje je objednávateľ ako prevádzkovateľ základnej služby povinný poskytovateľovi vopred oznámiť (ďalej len „Poverená osoba“). Poverená osoba sa v čase realizácie kontrolnej činnosti a/alebo auditu u poskytovateľa musí preukázať písomným poverením vystaveným objednávateľom ako prevádzkovateľom základnej služby na jeho vykonanie. Zmluvné strany sa dohodli, že náklady na realizáciu kontrolnej činnosti a/alebo auditu u poskytovateľa tak na strane objednávateľa ako

prevádzkovateľa základnej služby ako aj na strane poskytovateľa znáša v celom rozsahu objednávateľ ako prevádzkovateľ základnej služby.

3.3 Prevádzkovateľ základnej služby je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu pravidelne raz za kalendárny rok; a to v prípade preukázaného podozrenia z porušenia tejto prílohy alebo Zákona; v prípade nedodržania bezpečnostných opatrení a v prípade žiadosti dozorného orgánu podľa Zákona.

3.4 Prevádzkovateľ základnej služby informuje o termíne vykonania auditu alebo kontroly poskytovateľa oznámením zaslaným e-mailom uvedeným v záhlaví tohto Dodatku, a to minimálne 7 pracovných dní pred vykonaním auditu alebo kontroly. Poskytovateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 pracovných dní odo dňa zaslania oznámenia. Pokiaľ poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.

3.5 Prevádzkovateľ základnej služby je oprávnený vykonávať audit u poskytovateľa nasledovne, pričom zmluvné strany majú pri výkone kontrolných činností a auditu nasledovné práva a povinnosti:

a. Prevádzkovateľ základnej služby je oprávnený vykonať u poskytovateľa audit zameraný na overenie plnenia povinností poskytovateľa podľa tejto prílohy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia poskytovateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u poskytovateľa pre plnenie cieľov tejto Servisnej zmluvy.
b. Prípadné nedostatky zistené auditom je poskytovateľ povinný odstrániť bez zbytočného odkladu.
c. Prevádzkovateľ základnej služby môže audit u poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v prípade ak objednávateľ realizuje audit prostredníctvom tretej osoby, tak je táto tretia osoba pred začatím realizácie auditu povinná uzatvoriť s poskytovateľom dohodu o mlčanlivosti tzv. NDA, následne práva a povinnosti objednávateľa ako prevádzkovateľa základnej služby pri výkone auditu realizuje objednávateľom ako prevádzkovateľom základnej služby poverená tretia osoba.
d. Poskytovateľ je povinný pri audite spolupracovať s objednávateľom ako prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto prílohy vo vzťahu k dodaným Informačným systémom CG a výkonu Ročnej podpory. Objednávateľ ako prevádzkovateľ základnej služby je povinný minimálne 7 pracovných dní pred samotným auditom zaslať poskytovateľovi predmet auditu s menovitým zoznam tém a oblastí v rozsahu ním dodaným Informačných systémov CG, ktorých sa audit bude týkať.
e. Objednávateľ ako prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom poskytovateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto prílohy za prítomnosti osoby poverenej poskytovateľom, na ktorú sa sťahuje bod c) tohto článku.
f. V rámci auditu je poskytovateľ povinný preukázať objednávateľovi ako prevádzkovateľovi základnej služby súlad jeho postupov s touto prílohou, najmä

preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto prílohy, záväzok a poučenie svojich zamestnancov, o povinnosti mlčanlivosti podľa tejto prílohy a aktuálnosť svojej bezpečnostnej dokumentácie.

g. Ak poskytovateľ, napriek splneniu podmienky podľa pís. c) a d) tohto článku objednávateľom ako prevádzkovateľom základnej služby, neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto prílohy, to neplatí ak možnosť realizácie auditu oznámil poskytovateľ objednávateľovi ako prevádzkovateľovi základnej služby v náhradnom termíne a tento termín prevádzkovateľ základnej služby odmietol akceptovať.
h. Prevádzkovateľ základnej služby, resp. ním poverená tretia osoba je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.
i. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny poskytovateľa týkajúce sa uvedených priestorov na úseku BOZP a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO“), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal poskytovateľ 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 poskytovateľa.

3.6 Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť prevádzkovateľovi základnej služby na účely kontroly a auditu v zmysle ust. § 28 a 29 Zákona.

3.7 Poskytovateľ je povinný v lehote určenej prevádzkovateľom základnej služby, avšak najneskôr v lehote 90 dní odo dňa ich oznámenia prijať opatrenia na nápravu nedostatkov zistených auditom u prevádzkovateľa základnej služby a poskytnúť potrebnú súčinnosť prevádzkovateľovi základnej služby na ich odstránenie.

4. Vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre objednávateľa ako prevádzkovateľa základnej služby namiesto poskytovateľa

4.1 Poskytovateľ je povinný dodržiavať podmienky zapojenia nového dodávateľa do poskytovania služieb tak, ako sú upravené v tejto prílohe.

4.2 Poskytovateľ je povinný vopred informovať objednávateľa ako prevádzkovateľa základnej služby o zapojení nového dodávateľa, a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom e-mailu na kontakt uvedený v záhlaví tohto Dodatku.

4.3 Poskytovateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb objednávateľa ako prevádzkovateľovi základnej služby nového dodávateľa bez predchádzajúceho výslovného písomného súhlasu objednávateľa ako prevádzkovateľa základnej služby.

4.4 Ak poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb objednávateľovi ako prevádzkovateľovi základnej služby nového dodávateľa, tomuto novému dodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto prílohe. Zodpovednosť voči objednávateľovi ako prevádzkovateľovi základnej služby nesie poskytovateľ, ak nový dodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

5. Povinnosti poskytovateľa informovať objednávateľa ako prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti:

5.1 Objednávateľ ako prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu poskytovateľa o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie tohto Dodatku stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

5.2 Poskytovateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident týkajúci sa predmetu tohto Dodatku v zmysle Zákona a informovať objednávateľa ako prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.

5.3 V prípade, ak počas vykonávania Ročnej podpory poskytovateľ zaznamená kybernetický bezpečnostný incident je povinný bezodkladne informovať objednávateľa ako prevádzkovateľa základnej služby podľa bodu 5.2 tohto článku tejto Prílohy č. 6 hlásením kybernetického bezpečnostného incidentu prostredníctvom zaslania hlásenia na e-mailovú adresu uvedenú v záhlaví tohto Dodatku v rozsahu nasledovných informácií:

a. <u>informácie o tom, kto hlási kybernetický bezpečnostný incident</u>:
   - identifikačné údaje poskytovateľa,
   - funkcia a pracovné zaradenie osoby poskytovateľa, ktorá hlási kybernetický bezpečnostný incident,
   - identifikačné údaje ďalších organizácií dotknutých kybernetickým bezpečnostným incidentom,

b. <u>informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu, ak sú dostupné a známe</u>:
   - kategória kybernetického bezpečnostného incidentu (bezpečnostný incident I. stupňa, bezpečnostný incident II. stupňa, bezpečnostný incident III. stupňa),
   - typ závažného kybernetického bezpečnostného incidentu
   - nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
   - škodlivý kód (vírus, malvér, ransomvér),
   - získavanie informácií (skenovanie siete, odpočúvanie, sociálne inžinierstvo),
   - pokus o prienik do systému,

- podozrenie na úspešný prienik do systému vrátane APT,
- nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby),
- neoprávnený prístup k informáciám, únik informácií, poškodenie informácií,
- podvod (neautorizované využitie prostriedkov, porušenia autorských práv),
- zraniteľnosť (ich existencia),
- iné,

– časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu

- čas začiatku incidentu (ak je známy), čas a spôsob zistenia incidentu, informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,

– detailný opis priebehu závažného kybernetického bezpečnostného incidentu a jeho prvotná príčina,
– popis rozsahu škôd,
– odhad závažnosti dopadu závažného kybernetického bezpečnostného incidentu na užívateľov základnej služby,

c. <u>informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom</u>:

– prvotne zasiahnuté aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby),
– informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity služby alebo činnosti, a či je zariadenie v čase podávania hlásenia v prevádzke,

d. <u>informácie o riešení závažného kybernetického bezpečnostného incidentu</u>:

– stav riešenia závažného kybernetického bezpečnostného incidentu,
– informácia o vykonaní nápravných opatrení smerujúcich k riešeniu hláseného závažného kybernetického bezpečnostného incidentu,
– opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,
– popis možných negatívnych dopadov, opatrení a možných dôsledkov závažného kybernetického bezpečnostného incidentu,
– výsledok opatrení,
– dátum a čas realizácie opatrení.

5.4 Poskytovateľ je povinný na vyžiadanie nahlásiť objednávateľovi ako prevádzkovateľovi základnej služby ďalšie informácie požadované objednávateľom na plnenie jeho povinnosti vyplývajúcich zo Zákona, najmä je povinný poskytnúť objednávateľovi ako prevádzkovateľovi základnej služby:

a. informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované prevádzkovateľom základnej služby alebo Národným bezpečnostným úradom a ústredným orgánom od prevádzkovateľa základnej služby za účelom splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm. c) Zákona,
b. informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
c. informácie potrebné na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods.6 písm. e) Zákona oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

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

5.5 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený požadovať od poskytovateľa vykonanie reaktívneho opatrenia a poskytovateľ je povinný vykonať reaktívne opatrenie v prípadoch, kedy bola objednávateľovi ako prevádzkovateľovi základnej služby uložená povinnosť vykonať reaktívne opatrenie Národným bezpečnostným úradom v zmysle Zákona vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany poskytovateľa a vo vzťahu k informačným systémom poskytovateľa prostredníctvom, ktorých poskytovateľ poskytuje prevádzkovateľovi základnej služby Ročnú podporu pre Informačné systémy CG.

5.6 Poskytovateľ je povinný bezodkladne objednávateľovi ako prevádzkovateľovi základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok a poskytnúť prevádzkovateľovi základnej služby všetku potrebnú súčinnosť pri splnení povinnosti objednávateľa ako prevádzkovateľa základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok pred Národným bezpečnostným úradom vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany poskytovateľa a vo vzťahu k informačným systémom poskytovateľa prostredníctvom, ktorých poskytovateľ poskytuje prevádzkovateľovi základnej služby Ročnú podporu pre Informačné systémy CG.

5.7 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený požadovať od poskytovateľa návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu, a to najmä v prípadoch, kedy Národný bezpečnostný úrad požaduje od prevádzkovateľa základnej služby návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany poskytovateľa a vo vzťahu k informačným systémom poskytovateľa prostredníctvom, ktorých poskytovateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy CG (ďalej aj len „ochranné opatrenie“). Ochranné opatrenie sú prijímané na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

5.8 Poskytovateľ je povinný bezodkladne objednávateľovi ako prevádzkovateľovi základnej služby predložiť navrhované ochranné opatrenie na schválenie.

5.9 V prípade, ak poskytovateľ nenavrhne ochranné opatrenie v lehote určenej objednávateľom ako prevádzkovateľom základnej služby alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je poskytovateľ povinný poskytnúť všetku potrebné súčinnosť objednávateľovi, ktorý je povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

5.10 Bez ohľadu na ustanovenia Prílohy č. 6, povinnosti poskytovateľa majú len podporný charakter, táto Príloha č. 6 nezbavuje objednávateľa ako prevádzkovateľa základnej služby plniť povinnosti v zmysle Zákona, okrem iného § 19 ods. 6 a § 24 Zákona.

6. Ostatné dojednania súvisiace s povinnosťami zmluvných strán vyplývajúcich zo Zákona a Vyhlášky

6.1 Zmluvné strany sa dohodli, že hlásenia ďalších informácií požadovaných objednávateľom ako prevádzkovateľom základnej služby na plnenie jeho povinností

vyplývajúcich zo Zákona sa uskutoční nasledovne: zadaním požiadavky prostredníctvom stránky www.helpdesk.corageo.sk

6.2 Zmluvné strany sa dohodli, že hlásenia všetkých/akýchkoľvek informácií majúcich vplyv na Servisnú zmluvu sa uskutoční nasledovne: zadaním požiadavky prostredníctvom stránky www.helpdesk.corageo.sk

6.3 Poskytovateľ sa zaväzuje, že po ukončení zmluvného vzťahu vráti, prevedie alebo zničí všetky informácie, ku ktorým mal prístup počas trvania zmluvného vzťahu s objednávateľom ako prevádzkovateľovi základnej služby.

6.4 Poskytovateľ prehlasuje, že Zákonom ustanovenú povinnosť po ukončení Servisnej zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné práva na používanie softvéru licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby špecifikovanú v tejto Servisnej zmluve na objednávateľa ako prevádzkovateľa základnej služby bola splnená a to samotným dodaním Informačných systémov CG.

6.5 Poskytovateľ prehlasuje, že sa zaväzuje chrániť všetky informácie poskytnuté objednávateľom ako prevádzkovateľom základnej služby.

6.6 V prípade zavineného porušenia povinnosti poskytovateľa, vyplývajúcej mu z Prílohy č. 6 tohto Dodatku, je objednávateľ ako prevádzkovateľ základnej služby oprávnený požadovať od poskytovateľa zaplatenie zmluvnej pokuty vo výške 500,- EUR (slovom: päťsto eur) za každé jednotlivé (aj opakované) preukázateľné zdokladované zavinené porušenie tejto zmluvnej povinnosti poskytovateľa vyplývajúce z Prílohy č. 6 tohto Dodatku. Zmluvné strany sa dohodli, že súčet zmluvných pokút podľa predchádzajúcej vety za kalendárny rok neprevýši sumu zodpovedajúcu 10% ceny skutočne zaplatenej (uhradenej) ceny služieb poskytovateľa podľa Servisnej zmluvy v danom roku.. Objednávateľ nie je oprávnený požadovať náhradu škody spôsobenej porušením povinnosti, na ktorú sa vzťahuje zmluvná pokuta. Objednávateľ nie je oprávnený domáhať sa náhrady škody presahujúcej zmluvnú pokutu. V prípade ak Objednávateľ neuplatní zmluvnú pokutu podľa tohto článku má nárok voči poskytovateľovi na náhradu skutočnej škody (nie ušlého zisku), ako aj nárok na náhradu pokút, poplatkov alebo iných peňažných sankcií uložených orgánmi verejnej moci poskytovateľovi v prípade ak bude preukázané zavinené porušenie povinností poskytovateľa a to najviac do sumy zodpovedajúcej 10% ceny skutočne zaplatenej (uhradenej) ceny služieb poskytovateľa podľa Servisnej zmluvy.

6.7 Zmluvné strany sa dohodli, že celkové finančné záväzky, ktoré bude Poskytovateľ znášať v súvislosti so všetkými nárokmi vznesenými Objednávateľom v súvislosti s týmto Dodatkom, nepresiahnu hodnotu skutočných priamych škôd, ktoré vzniknú Objednávateľovi, maximálne však do výšky 10% ceny skutočne zaplatenej (uhradenej) ceny služieb Poskytovateľa podľa Servisnej zmluvy pre jeden kalendárny rok poskytovania služieb, ktoré sú predmetom nároku, a to bez ohľadu na právny základ nároku (v prípade opakovaných platieb do výšky platieb za 12 mesiacov).

IV. SPOLOČNÉ A ZÁVEREČNÉ USTANOVENIA

1. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony a znenie tohto Dodatku si prečítali, rozumejú jeho obsahu, ich zmluvná voľnosť nebola obmedzená, a že ho uzatvorili na základe ich slobodnej a vážnej vôle, nie v tiesni ani za nápadne

nevýhodných podmienok a na znak súhlasu s jeho ustanoveniami pripájajú svoje vlastnoručné podpisy, ako vyjadrenie ich slobodnej a vážnej vôle.

2. Ostatné ustanovenia Servisnej zmluvy, ktoré neboli menené, zrušené alebo doplnené týmto Dodatkom ostávajú v platnosti v celom rozsahu. Pojmy definované v Servisnej zmluve majú ten istý význam aj v tomto Dodatku.
3. Tento Dodatok nadobúda platnosť dňom jeho podpísania zmluvnými stranami a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR podľa § 47a ods. 1 Občianskeho zákonníka v nadväznosti na § 5a ods. 1 a 4 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií).
4. Dodatok je neoddeliteľnou súčasťou Servisnej zmluvy.
5. Tento Dodatok bol vyhotovený v 4 rovnopisoch, z ktorých po dvoch rovnopisoch obdrží každá zo zmluvných strán.

Prešov, Dátum:	Poprad, Dátum:
Objednávateľ: Ing. František Oľha primátor Mesto Prešov	Poskytovateľ: Ing. Jozef Habiňák konateľ CORA GEO, s. r. o.