Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená v zmysle zákona č. 513/1991 Z.z. Obchodný zákonník a zákona č.69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení medzi zmluvnými stranami:

Objednávateľ:

Obchodné meno:	**Slovenská pošta, a.s.**
Sídlo:	Partizánska cesta 9, 975 99 Banská Bystrica
V mene spoločnosti:	**Ing. Martin Ľupták, PhD., predseda predstavenstva**
	Ing. Ľubomír Mindek, podpredseda predstavenstva
IČO:	36 631 124
DIČ:	2021879959
IČ DPH:	SK2021879959

Spoločnosť zapísaná v OR Okresného súdu Banská Bystrica, oddiel: Sa, vložka č. 803/S
(ďalej aj ako „prevádzkovateľ základnej služby“ alebo Objednávateľ)

Poskytovateľ:

Obchodné meno:	**EMM, spol. s r.o.**
Sídlo:	Sekurisova 16, 841 02 Bratislava
V mene spoločnosti:	**Ing. Jozef Chebeň, konateľ**
IČO:	17 316 260
DIČ:	2020316529
IČ DPH:	SK2020316529

Spoločnosť zapísaná v OR Okresného súdu Bratislava I, Oddiel: Sro, vložka č. 686/B:
(ďalej aj ako „Poskytovateľ“)

*(ďalej spolu ako aj **„zmluvné strany“**)*

Článok I.
Preambula

1. Na základe Zmluvy o poskytovaní služieb vyššej podpory s č. v CEEZ 431/2022 (ďalej len „Zmluva o poskytovaní služieb“), sa Poskytovateľ zaviazal pre Objednávateľa poskytovať systémové služby vyššej podpory na vyžiadanie, ktoré zahŕňajú aj štandardnú podporu výrobcu pre bezpečnostné systémy prevádzkované v prostredí IS Slovenskej pošty, a.s. (ďalej len „služby“). Podrobný popis poskytovaných služieb Poskytovateľa v rámci predmetu Zmluvy o poskytovaní služieb je uvedený v *Prílohe č. 1* Zmluvy o poskytovaní služieb.
2. Objednávateľ je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon“).
3. Poskytovateľ uzatvára s prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona, ktorej predmet priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v Zákone, pre prevádzkovateľa základnej služby.
4. Základnou službou prevádzkovateľa základnej služby je zabezpečovanie Univerzálnej poštovej služby – medzinárodného aj vnútroštátneho poštového styku a poštového platobného styku.
5. Prevádzkovateľ základnej služby je povinný uzatvoriť s Poskytovateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona (ďalej len „Zmluva“).
6. Zmluva obsahuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa základnej služby, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany prevádzkovateľa základnej služby (ďalej len „ciele“), a to aj v spolupráci s Poskytovateľom.

Článok II.
Definícia pojmov

1. Pojmy používané v tejto Zmluve majú význam im priradený v Zákone a jeho vykonávacích predpisoch.

Článok III.
Rozsah činnosti Poskytovateľa

1. Poskytovateľ sa zaviazal pre Objednávateľa poskytovať služby podľa Zmluvy o poskytovaní služieb.

   Na plnenie predmetu Zmluvy o poskytovaní služieb budú Poskytovateľovi poskytnuté/sprístupnené nasledovné aktíva:
   a) Bezpečnostné zariadenia sieťovej ochrany

2. Pri prístupe k IKT aktívam:

   2.1. Poskytovateľ sa zaväzuje v súvislosti s plnením predmetu Zmluvy o poskytovaní služieb dodržiavať klasifikáciu informácií uvedenú v Tabuľke č.1

   2.2. Poskytovateľ berie na vedomie, že poskytovanie prístupov v rámci siete Objednávateľa vrátane vykonávania zmien sprístupnených informácií/aktív, je riadené, monitorované a auditované v súlade s platnou internou dokumentáciou

   2.3. Akceptovateľné použitie informácií/IKT aktív je:
   - 2.3.1. zhotovovať obrazový záznam IKT aktív len po predchádzajúcom súhlase Manažéra informačnej a kybernetickej bezpečnosti. Súhlas musí byť vydaný v dokumentovanej podobe,
   - 2.3.2. pristupovať k P2P sieťam len v správe Objednávateľa,
   - 2.3.3. mimo prostredia Objednávateľa vynášať IKT zariadenia len so súhlasom oprávneného zamestnanca Objednávateľa. Súhlas musí byť vydaný v dokumentovanej podobe s uvedením dôvodu a dátumu návratu zariadenia, ak sa predpokladá jeho návrat,
   - 2.3.4. k zariadeniam, ktoré sú pripojené do siete Objednávateľa, pripájať len zariadenia (dátové úložiská: USB kľúče, napaľovačky CD/DVD/BlueRay, externé HDD/SD a pod.; mobilné telefóny a modemy; rôzne sieťové zariadenia: Wi-Fi router, switch, hub, koncové zariadenia s káblovým

pripojením: počítače/tablety; ostatné zariadenia: scannery, tlačiarne, fotoaparáty, kamery a pod.), ktoré sú v správe Objednávateľa, alebo boli schválené na používanie v sieti Objednávateľa,

2.3.5. využívať zariadenia/softvér na prienik do dátových sietí, testovanie zraniteľností, odpočúvanie a zaznamenávanie dátovej komunikácie len po predchádzajúcom súhlase osôb určených Objednávateľom.

2.4. Neakceptovateľné použitie IKT aktív je:

2.4.1. využívať pripojenie na Internet na nepracovné účely, s výnimkou využitia nezabezpečenej siete WiFi prevádzkovanej Objednávateľom

2.4.2. umožniť zariadeniam fyzicky pripojeným do siete Objednávateľa súčasné pripojenie do inej siete (napr. GSM internet, Wi-Fi)

2.5. Poskytnutie prístupových práv k IKT aktívu sa vykonáva výhradne na základe Žiadosti o pridelenie/zmenu prístupu k IKT aktívu vlastníkovi IKT aktíva formou e-mailu.

2.6. Ak má Poskytovateľ fyzický prístup k IKT aktívam Objednávateľa, zaväzuje sa, že počas pobytu v priestoroch Objednávateľa, bude dodržiavať všeobecné zásady bezpečnosti práce, protipožiarnej ochrany a ochrany životného prostredia

2.7. Ak má Poskytovateľ prístup k osobným údajom, zaväzuje sa zabezpečiť ochranu osobných údajov v súlade so Zákonom o ochrane osobných údajov

2.8. Neprerušiteľnosť spracovania:

Poskytovateľ je povinný realizovať predmet Zmluvy o poskytovaní služieb tak, aby nedošlo k prerušeniu, alebo obmedzeniu prevádzky Objednávateľa. V prípade, ak plnenie predmetu Zmluvy o poskytovaní služieb nevyhnutne vyžaduje prerušenie alebo obmedzenie prevádzky Objednávateľa, je Poskytovateľ povinný vopred preukázateľne o tejto skutočnosti informovať Objednávateľa a do doby, pokiaľ Poskytovateľ nedostane inštrukcie od Objednávateľa o ďalšom postupe, alebo súhlas s plnením predmetu Zmluvy o poskytovaní služieb je Poskytovateľ povinný zdržať sa takého vykonávania predmetu Zmluvy o poskytovaní služieb, ktoré by mohlo spôsobiť prerušenie, alebo obmedzenie prevádzky Objednávateľa. V opačnom prípade zodpovedá Poskytovateľ za škody, ktoré týmto spôsobí Objednávateľovi

2.9. Vrátenie aktív:

Zmluvné strany sú povinné po zániku Zmluvy o poskytovaní služieb:

- v lehote 60 dní od zániku Zmluvy o poskytovaní služieb vrátiť druhej zmluvnej strane všetky fyzické a elektronické aktíva patriace tejto zmluvnej strane, ktoré im boli v súvislosti s plnením predmetu Zmluvy o poskytovaní služieb poskytnuté; to neplatí ak v rovnakej lehote bude uzatvorená alebo je v rokovacom konaní nová zmluva medzi stranami s rovnakým alebo podobným predmetom plnenia ako je Zmluvy o poskytovaní služieb,
- v lehote 60 dní od zániku Zmluvy o poskytovaní služieb zabezpečiť bezpečné odstránenie elektronických aktív druhej zmluvnej strany v prípade, ak sú elektronické aktíva patriace jednej zmluvnej strane v súvislosti s plnením predmetu Zmluvy o poskytovaní služieb umiestnené na zariadení druhej zmluvnej strany; to neplatí ak v rovnakej lehote bude uzatvorená alebo je v rokovacom konaní nová zmluva medzi stranami s rovnakým alebo podobným predmetom plnenia ako je predmet Zmluvy o poskytovaní služieb.

2.10. Poskytovateľ sa zaväzuje urobiť opatrenia, aby:

2.10.1. pri plnení jeho záväzkov podľa Zmluvy o poskytovaní služieb nedochádzalo z jeho strany k porušovaniu licenčných pravidiel platných pre písomne odsúhlasené alebo v Zmluvy o poskytovaní služieb uvedené verzie operačných systémov, databázového prostredia a ďalších podporných a integračných softvérov, slúžiacich pre prevádzku aplikačného softvéru Objednávateľa, ktorého dodávka/úprava/podpora je predmetom záväzku Poskytovateľa podľa Zmluvy o poskytovaní služieb, alebo ktorého sa týka poskytnutie služieb v zmysle Zmluvy o poskytovaní služieb (ďalej len pravidlá licenčnej politiky) a

2.10.2. aby plnenie, ktoré Objednávateľovi na základe Zmluvy o poskytovaní služieb poskytne, neporušovalo pravidlá licenčnej politiky.

Ak sa preukáže porušenie pravidiel licenčnej politiky, ktoré bolo spôsobené činnosťou Poskytovateľa, Poskytovateľ sa zaväzuje uhradiť Objednávateľovi všetky náhrady škody prípadne všetky iné finančné náklady, ktoré Objednávateľovi vzniknú v dôsledku takéhoto porušenia pravidiel licenčnej politiky Poskytovateľom a budú uplatnené autorom softvéru prípadne inou oprávnenou osobou voči Objednávateľovi. Akákoľvek limitácia náhrady škody dohodnutá v Zmluvy o poskytovaní služieb sa nevzťahuje na náhradu škody, ktorú je Poskytovateľ povinný zaplatiť Objednávateľovi v zmysle tohto bodu Zmluvy. Povinnosť nahradiť vzniknutú škodu alebo iné finančné náklady, ktoré Objednávateľovi vzniknú v dôsledku porušenia pravidiel licenčnej politiky Poskytovateľom trvá aj po ukončení platnosti Zmluvy o poskytovaní služieb a to aj v prípade, ak bol nárok na ich zaplatenie uplatnený voči Objednávateľovi po ukončení platnosti Zmluvy o poskytovaní služieb.

2.11. Zmluvné strany sa dohodli, že prenos informácií sa bude realizovať v elektronickej, alebo papierovej podobe. Elektronické informácie budú odosielané vo vopred dohodnutom formáte, pred ich odoslaním budú skontrolované, či neobsahujú malvér (škodlivý kód) a počas prenosu s nimi bude narábané v súlade s ustanoveniami uvedenými v Tabuľke č. 1:

Tabuľka č.1

		Klasifikácia informácií			
Forma záznamu informácií	**Činnosť**	**Verejné**	**Interné**	**Chránené**	**Prísne chránené**
Elektronická	**Prístup**	Bez osobitných opatrení.	Len pre autorizované osoby, autentifikácia minimálne na základe hesla.	Len pre autorizované osoby, autentifikácia minimálne na základe hesla.	Len pre autorizované osoby, autentifikácia minimálne na základe hesla.
	Modifikácia	Podlieha autorizácii.	Podlieha autorizácii.	Podlieha autorizácii.	Podlieha autorizácii.
	Kopírovanie (rozmnožovanie)	Neobmedzené.	Pre potreby zamestnancov SP a definované osoby zmluvného subjektu neobmedzené.	S povolením spracovateľa.	S povolením spracovateľa.
	Počet exemplárov	Neobmedzený	Neobmedzený	Neobmedzený	Neobmedzený
	Uloženie	Bez osobitných opatrení.	Primeraná fyzická ochrana; zamedziť možnosti náhodného zverejnenia.	Primeraná fyzická ochrana; zamedziť neautorizovanému prístupu; šifrovanie.	Primeraná fyzická ochrana; zamedziť neautorizovanému prístupu; šifrovanie.
	Prenos - e-mail	Bez osobitných opatrení.	V rámci domény SLPOSTA.SK bez osobitných opatrení; mimo domény SLPOSTA.SK šifrovane.	V rámci domény SLPOSTA.SK aj mimo nej šifrovane.	V rámci domény SLPOSTA.SK aj mimo nej šifrovane.
	Prenos- ostatné elektronické kanály	Bez osobitných opatrení.	V rámci domény SLPOSTA.SK bez osobitných opatrení; mimo domény SLPOSTA.SK šifrovane.	V rámci domény SLPOSTA.SK aj mimo nej šifrovane.	V rámci domény SLPOSTA.SK aj mimo nej šifrovane.
	Prenos -na fyzickom nosiči (CD, USB...)	Bez osobitných opatrení.	Dôveryhodný spôsob transportu; ochrana pred fyzickým poškodením počas transportu; šifrovanie.	Dôveryhodný spôsob transportu; ochrana pred fyzickým poškodením počas transportu; balenie, ktoré prezradí pokus o otvorenie prepravného obalu; šifrovanie.	Dôveryhodný spôsob transportu; ochrana pred fyzickým poškodením počas transportu; balenie, ktoré prezradí pokus o otvorenie prepravného obalu; šifrovanie.
	Likvidácia	Bez osobitných opatrení.	Štandard DoD II/ demagnetizácia/ mechanická deštrukcia.	Štandard DoD II/ demagnetizácia / mechanická deštrukcia.	Štandard DoD II/ demagnetizácia / mechanická deštrukcia.
Papierová	**Prístup**	Bez osobitných opatrení.	Pre potreby zamestnancov SP a definované osoby zmluvného subjektu neobmedzené.	S povolením spracovateľa.	S povolením spracovateľa.

	Kopírovanie (rozmnožovanie)	Bez osobitných opatrení.	Pre potreby zamestnancov SP a definované osoby zmluvného subjektu neobmedzené.	S povolením spracovateľa.	S povolením spracovateľa.
	Počet exemplárov	Neobmedzený	Neobmedzený	Neobmedzený	Neobmedzený
	Uloženie	Bez osobitných opatrení.	Primeraná fyzická ochrana; zamedziť možnosti náhodného zverejnenia.	Primeraná fyzická ochrana; zamedziť neautorizovanému prístupu (napr. uzamykateľná skriňa, uzamykateľná zásuvka, a pod.)	Primeraná fyzická ochrana; zamedziť neautorizovanému prístupu (napr. uzamykateľná skriňa, uzamykateľná zásuvka, a pod.)
	Prenos - fax	Bez osobitných opatrení.	Bez osobitných opatrení.	Pod dohľadom pri prijímajúcom faxe.	Pod dohľadom pri prijímajúcom faxe.
	Prenos - papierová forma	Bez osobitných opatrení.	Dôveryhodný spôsob transportu; ochrana pred fyzickým poškodením počas transportu.	Dôveryhodný spôsob transportu; ochrana pred fyzickým poškodením počas transportu; balenie, ktoré prezradí pokus o otvorenie prepravného obalu; adresa prijímateľa musí obsahovať aj meno konkrétnej osoby, pre ktorú sú informácie určené.	Dôveryhodný spôsob transportu; ochrana pred fyzickým poškodením počas transportu; balenie, ktoré prezradí pokus o otvorenie prepravného obalu; adresa prijímateľa musí obsahovať aj meno konkrétnej osoby, pre ktorú sú informácie určené.
	Likvidácia vyradených registratúrnych záznamov (riadi sa OS-13 Registratúrny poriadok)	Skartácia podľa DIN 32757 stupeň 3	Skartácia podľa DIN 32757 stupeň 3	Skartácia podľa DIN 32757 stupeň 3	Skartácia podľa DIN 32757 stupeň 3
	Likvidácia papierových nosičov nepodliehajúcich vyraďovaciemu konaniu	Bez osobitných opatrení.	Skartácia podľa DIN 32757 stupeň 3	Skartácia podľa DIN 32757 stupeň 3	Skartácia podľa DIN 32757 stupeň 3
Osobná	**Telefonicky, ústnym podaním**	Bez osobitných opatrení.	Upozorniť prijímateľa, že ide o interné informácie.	Upozorniť prijímateľa, že ide o chránené informácie.	Upozorniť prijímateľa, že ide o prísne chránené informácie.

2.12. Dokumentácia dodávaná Poskytovateľom k plneniam podľa Zmluvy o poskytovaní služieb bude klasifikovaná v súlade s klasifikáciou informácii Objednávateľa v súlade s požiadavkami Zákona a príslušných vyhlášok.

Vo všeobecnosti platí, že bežná používateľská dokumentácia, ktorá neobsahuje prístupové údaje k informačným systémom (mená, kontá, heslá) a iné citlivé informácie, je klasifikovaná v triede „interné“.

Administrátorská a obdobná dokumentácia, ktorá obsahuje inštalačné a konfiguračné postupy, citlivé prístupové údaje a vyhradené informácie, je klasifikovaná v triede „chránené“
Poskytovateľ sa zaväzuje počas zmluvného vzťahu dodať a udržiavať dokumentáciu (inštalačnú, prevádzkovú, administrátorskú, používateľskú) zodpovedajúcu aktuálnemu stavu a podľa požiadaviek Objednávateľa.

Objednávateľom preferovaný formát dokumentácie je docx/doc, alternatívny formát je pdf.

Článok IV.
Obdobie trvania Zmluvy

1. Táto Zmluva nadobúda platnosť dňom jej podpísania zmluvnými stranami. Táto Zmluva je povinne zverejňovanou zmluvou v zmysle § 5a zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v platnom znení. Zmluvné strany berú na vedomie a súhlasia, že táto Zmluva vrátane všetkých jej súčastí bude zverejnená v Centrálnom registri zmlúv (ďalej len „register"). Register je verejný zoznam povinne zverejňovaných zmlúv, ktorý vedie Úrad vlády Slovenskej republiky v elektronickej podobe. Zverejnenie zmluvy v registri sa nepovažuje za porušenie ani za ohrozenie obchodného tajomstva a informácie označené v tejto Zmluve ako dôverné v zmysle § 271 ods. 1 Obchodného zákonníka sa nepovažujú za dôverné informácie. Zmluva je účinná dňom nasledujúcim po dni jej zverejnenia v registri.
2. Zmluva sa uzatvára na dobu určitú – na dobu platnosti a účinnosti Zmluvy o poskytovaní služieb. Tým nie sú dotknuté ustanovenia Zmluvy, ktoré majú ostať podľa svojej povahy v platnosti i po zániku Zmluvy.

Článok V.
Povinnosť Poskytovateľa dodržiavať bezpečnostnú politiku prevádzkovateľa základnej služby a prijať bezpečnostné opatrenia

1. Poskytovateľ sa zaväzuje dodržiavať platné bezpečnostné politiky prevádzkovateľa základnej služby, ktoré sú normatívne upravené v dokumentoch prevádzkovateľa základnej služby.
2. Poskytovateľ vyhlasuje, že sa s bezpečnostnou politikou prevádzkovateľa základnej služby oboznámil a vyjadruje súhlas s bezpečnostnou politikou prevádzkovateľa základnej služby.
3. Poskytovateľ súhlasí s tým, že bezpečnostné politiky prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa základnej služby a aktuálnym hrozbám dotýkajúcim sa Poskytovateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby.
4. Poskytovateľ je povinný a zaväzuje sa chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby.
5. Poskytovateľ sa zaväzuje dodržiavať a prijať bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) Zákona, a to najneskôr v lehote do 3 mesiacov odo dňa nadobudnutia účinnosti tejto Zmluvy. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.
6. Poskytovateľ je povinný oboznámiť prevádzkovateľa základnej služby s prijatými bezpečnostnými opatreniami a umožniť prevádzkovateľovi základnej služby vykonať audit Poskytovateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení Poskytovateľom s bezpečnostnou politikou prevádzkovateľa základnej služby. V prípade, ak výsledkom auditu bude nesúlad Poskytovateľom prijatých bezpečnostných opatrení so Zákonom alebo s bezpečnostnou politikou prevádzkovateľa základnej služby, je Poskytovateľ povinný najneskôr v lehote 30 pracovných dní odo dňa zistenia nesúladu zabezpečiť nápravu.
7. Odplata za plnenie povinností Poskytovateľa podľa tejto Zmluvy a náhrada všetkých nákladov vynaložených Poskytovateľom v súvislosti s plnením povinností Poskytovateľa podľa tejto Zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom základnej služby Poskytovateľovi podľa Zmluvy o poskytovaní služieb a na žiadne ďalšie peňažné plnenia Poskytovateľ za plnenie povinností podľa tejto Zmluvy od prevádzkovateľa základnej služby nemá nárok.

Článok VI.
Špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma Poskytovateľ a vyjadrenie súhlasu s nimi

1. Pre oblasť technických zraniteľností informačných systémov a zariadení Poskytovateľ najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva *pri poskytovaní službieb* prevádzkovateľovi základnej služby, prostredníctvom nasledujúcich opatrení:
   a. Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
   b. Zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,

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

2. Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje Poskytovateľ nasledovné opatrenia:
   a. Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom.
   b. Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
   c. Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
   d. Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.
   e. Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
   f. Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
   g. Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
   h. Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.
   i. Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
   j. Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
   k. Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.
   l. Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.
   m. Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.
   n. Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.
   o. Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

3. Pre oblasť riadenia prístupov 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 siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
   b. Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa 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 vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.
   d. Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
   e. Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
   f. Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny

oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).

g. Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
h. Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

4. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Poskytovateľ nasledovné opatrenia, pričom najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na výkon činnosti pre prevádzkovateľa základnej služby:
   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.
   b. Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb prevádzkovateľovi základnej služby.
   c. Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
   d. Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.
   e. Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov prevádzkovateľa základnej služby.
   f. Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s prevádzkovateľom základnej služby.

5. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Poskytovateľ opatrenia podľa § 15 vyhlášky NBÚ č. 362/2018 Z.z., 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 *vykonávaní služieb* prevádzkovateľovi základnej služby.

Článok VII.
Ďalšie povinnosti Poskytovateľa

1. Poskytovateľ sa zaväzuje doručiť do 5 pracovných dní od nadobudnutia účinnosti tejto Zmluvy Objednávateľovi zoznam pracovných rolí Poskytovateľa s uvedením identifikačných údajov osôb zastávajúcich niektorú z pracovných úloh v rozsahu (meno, priezvisko, kontakt), ktoré majú mať prístup k informáciám a údajom Objednávateľa.
2. Poskytovateľ je povinný oznámiť Objednávateľovi každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny.
3. Poskytovateľ sa zaväzuje zabezpečiť a odovzdať Objednávateľovi písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia Zmluvy o poskytovaní služieb (ďalej aj len **„zúčastnená osoba“**); ktoré bude zúčastnenou osobou osobne vlastnoručne podpísané; každá zúčastnená osoba je povinná zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa Zákona dozvedela a ktoré nie sú verejne známe. Povinnosť zúčastnenej osoby zachovávať mlčanlivosť podľa tohto bodu tejto Zmluvy trvá aj po skončení právneho vzťahu medzi zúčastnenou osobou a Poskytovateľom; tým nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.
4. Poskytovateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je 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 cieľov tejto Zmluvy.

Článok VIII.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u Poskytovateľa

1. Objednávateľ je oprávnený vykonávať kontrolnú činnosť a audit u Poskytovateľa, a to v rozsahu a za účelom kontroly plnenia povinnosti Poskytovateľa v zmysle Zákona a tejto Zmluvy.
2. Objednávateľ je oprávnený vykonať kontrolnú činnosť a audit u Poskytovateľa prostredníctvom osoby, ktorej identifikačné údaje je Objednávateľ povinný Poskytovateľovi včas oznámiť.
3. Objednávateľ je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu pravidelne raz za kalendárny rok; v prípade podozrenia z porušenia tejto Zmluvy alebo Zákona; v prípade nedodržania bezpečnostných opatrení a v prípade žiadosti dozorného orgánu podľa Zákona.
4. Objednávateľ informuje o termíne vykonania auditu alebo kontroly Poskytovateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 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 dní odo dňa zaslania oznámenia. Pokiaľ Poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.
5. Objednávateľ je oprávnený vykonávať audit u Poskytovateľa nasledovne, pričom zmluvné strany majú pri výkone kontrolných činností a auditu nasledovné práva a povinnosti:
   a. Objednávateľ je oprávnený vykonať u Poskytovateľa audit zameraný na overenie plnenia povinností Poskytovateľa podľa tejto Zmluvy 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 Zmluvy.
   b. Prípadné nedostatky zistené auditom je Poskytovateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
   c. Objednávateľ môže audit u Poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Objednávateľa pri výkone auditu realizuje prevádzkovateľom základnej služby poverená tretia osoba.
   d. Poskytovateľ je povinný pri audite spolupracovať s 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 Zmluvy.
   e. Objednávateľ je v rámci auditu oprávnený klásť otázky zamestnancom Poskytovateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
   f. V rámci auditu je Poskytovateľ povinný preukázať Objednávateľovi súlad s touto Zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
   g. Vykonanie alebo nevykonanie auditu Objednávateľom nezbavuje Poskytovateľa zodpovednosti za plnenie povinností Poskytovateľa vyplývajúcich z tejto Zmluvy.
   h. Ak Poskytovateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
   i. Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.
   j. Objednávateľ 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.

6. Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť Objednávateľovi na účely kontroly a auditu v zmysle ust. § 28 a 29 Zákona.
7. Poskytovateľ je povinný v lehote určenej Objednávateľom prijať opatrenia na nápravu nedostatkov zistených auditom u prevádzkovateľa základnej služby a poskytnúť potrebnú súčinnosť prevádzkovateľovi základnej služby na ich odstránenie.

Článok IX.

Podmienky a možnosti zapojenia ďalšieho Poskytovateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto Poskytovateľa a podmienky a možnosti zapojenia subdodávateľa prostredníctvom Poskytovateľa

1. Poskytovateľ je povinný dodržiavať podmienky zapojenia nového poskytovateľa do poskytovania služieb tak, ako sú upravené v tejto Zmluve.
2. Poskytovateľ je povinný vopred informovať prevádzkovateľa základnej služby o zapojení nového poskytovateľa, a to zaslaním žiadosti o zapojenie nového poskytovateľa prostredníctvom emailu na kontakt uvedený v záhlaví tejto Zmluvy.
3. Poskytovateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb prevádzkovateľovi základnej služby nového poskytovateľa bez predchádzajúceho výslovného písomného súhlasu prevádzkovateľa základnej služby.
4. Ak Poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb prevádzkovateľovi základnej služby nového poskytovateľa, tomuto novému poskytovateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Zmluve. Zodpovednosť voči prevádzkovateľovi základnej služby nesie Poskytovateľ, ak nový poskytovateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

Článok X.

Povinnosť Poskytovateľa hlásiť kybernetický bezpečnostný incident a ďalšie informácie prevádzkovateľovi základnej služby vrátane povinností Poskytovateľa pri riešení kybernetického bezpečnostného incidentu

1. Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu Poskytovateľa o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie Zmluvy o poskytovaní služieb stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.
2. Poskytovateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident v zmysle Zákona a informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.
3. Poskytovateľ je povinný bezodkladne informovať prevádzkovateľa základnej služby podľa bodu 2 tohto článku tejto Zmluvy hlásením kybernetického bezpečnostného incidentu prostredníctvom zaslania hlásenia na e-mailovú adresu uvedenú v záhlaví tejto Zmluvy v rozsahu nasledovných informácií:
   a. informácie o tom, kto hlási kybernetický bezpečnostný incident:
      - identifikačné údaje Poskytovateľa,
      - funkcia a pracovné zaradenie osoby Poskytovateľa, ktorá hlási kybernetický bezpečnostný incident,
      - identifikačné údaje ďalších organizácií dotknutých kybernetickým bezpečnostným incidentom,
   b. informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu:
      - 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. informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom:
– 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. informácie o riešení závažného kybernetického bezpečnostného incidentu,
– 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.

4. Poskytovateľ je povinný hlásiť prevádzkovateľovi základnej služby ďalšie informácie požadované prevádzkovateľom základnej služby na plnenie jeho povinnosti vyplývajúcich zo Zákona, najmä je povinný poskytnúť 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. Prevádzkovateľ základnej služby je oprávnený požadovať od Poskytovateľa vykonanie reaktívneho opatrenia a Poskytovateľ je povinný vykonať reaktívne opatrenie v prípadoch, kedy bola prevádzkovateľovi základnej služby uložená povinnosť vykonať reaktívne opatrenie Národným bezpečnostným úradom v zmysle Zákona.
6. Poskytovateľ je povinný bezodkladne prevádzkovateľovi základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok a poskytnúť prevádzkovateľovi základnej služby všetku potrebnú súčinnosť pri splnení povinnosti prevádzkovateľa základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok pred Národným bezpečnostným úradom.
7. 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 /ďalej aj len „ochranné opatrenie“/. Ochranné opatrenie je prijímané na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.
8. Poskytovateľ je povinný bezodkladne prevádzkovateľovi základnej služby predložiť navrhované ochranné opatrenie na schválenie. Po schválení ochranného opatrenia Národným bezpečnostným úradom určí prevádzkovateľ základnej služby lehotu na vykonanie schváleného ochranného opatrenia.
9. V prípade, ak Poskytovateľ základnej služby nenavrhne ochranné opatrenie v lehote určenej prevádzkovateľom základnej služby alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je

Poskytovateľ povinný poskytnúť všetku potrebné súčinnosť prevádzkovateľovi základnej služby, ktorý je povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

Článok XI.
Spôsob a forma hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby

1. Poskytovateľ je povinný bez zbytočného odkladu informovať Prevádzkovateľa základnej služby o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti, o ktorých sa dozvedel. Týmto ustanovením nie je dotknutá povinnosť Prevádzkovateľa základnej služby sledovať a získavať informácie o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti vlastnou činnosťou alebo z iných zdrojov.
2. Zmluvné strany sú povinné vzájomne sa informovať o všetkých skutočnostiach, ktoré môžu mať akýkoľvek vplyv na Zmluvu, najmä na jej plnenie ktoroukoľvek Zmluvnou stranou
3. Z dôvodu rýchlosti a efektívnosti komunikácie Zmluvných strán, pokiaľ sa Zmluvné strany nedohodnú na širšom rozsahu komunikácie, bude komunikácia Zmluvných strán prebiehať prostredníctvom mailových adries Zmluvných strán uvedených v záhlaví Zmluvy alebo Zmluvnými stranami oznámenými iným preukázateľným spôsobom. Zmluvné strany sú oprávnené dohodnúť si aj iný spôsob komunikácie a výmeny informácií pre prípady identifikované týmto bodom, napr. formou osobitného spôsob komunikácie, a to prostredníctvom Tiketovacieho systému v rozsahu komunikácie identifikovanej týmto bodom Zmluvy. Informácia poskytovaná podľa tohto bodu Zmluvy sa považuje za doručenú deň nasledujúci po dni, v ktorom bola informácia Zmluvnou stranou odoslaná druhej Zmluvnej strane, a to aj napriek tomu, že sa o nej druhá Zmluvná strana nedozvedela, alebo sa s touto neoboznámila.

Článok XII.
Podmienky a spôsob ukončenia Zmluvy

1. Zmluvné strany môžu túto Zmluvu ukončiť vždy písomnou dohodou zmluvných strán; Zmluva zaniká dňom dohodnutým v písomnom vyhotovení dohody o ukončení tejto Zmluvy, nikdy nie pred uplynutím účinnosti Zmluvy o poskytovaní služieb. V prípade, ak zmluvné strany dohodnú deň ukončenia Zmluvy pred dňom uplynutia účinnosti Zmluvy o poskytovaní služieb, táto Zmluva zaniká súčasne so zánikom účinnosti Zmluvy o poskytovaní služieb (dohodou/výpoveďou/odstúpením od Zmluvy o poskytovaní služieb).
2. Prevádzkovateľ základnej služby je oprávnený písomne odstúpiť od tejto Zmluvy v prípade, ak Poskytovateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy.
3. Prevádzkovateľ základnej služby je oprávnený písomne vypovedať túto Zmluvu, ak
    a. Poskytovateľ neodôvodnene odmietne výkon kontrolnej činnosti a auditu prevádzkovateľom základnej služby,
    b. Poskytovateľ postúpi svoje práva a povinnosti na ďalšieho poskytovateľa v rozpore s touto Zmluvou,
    c. na majetok Poskytovateľa je vyhlásený konkurz, exekúcia, Poskytovateľ vstúpil do likvidácie, preruší, alebo iným spôsobom ukončí svoju podnikateľskú činnosť,
    d. Poskytovateľ, alebo osoba oprávnená konať v jeho mene je právoplatne odsúdená za trestný čin spáchaný v súvislosti s výkonom jeho činnosti, alebo s podnikaním,
    e. Poskytovateľ stratí predpoklady na plnenie tejto Zmluvy.

    Výpovedná lehota je jeden mesiac a začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.
4. Poskytovateľ je povinný po ukončení Zmluvy vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup prevádzkovateľovi základnej služby.
5. Poskytovateľ je povinný po ukončení Zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok Poskytovateľa ostáva v platnosti aj po ukončení Zmluvy po dobu 5 rokov.

Článok XIII.
Sankcie, zmluvné pokuty a náhrada škody

1. V prípade, ak Poskytovateľ poruší svoje povinnosti v zmysle tejto Zmluvy voči prevádzkovateľovi základnej služby, a to najmä povinnosť

a. dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
b. dodržiavať a prijímať bezpečnostné opatrenia minimálne v rozsahu najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) Zákona,
c. prijať bezpečnostnú dokumentáciu, ktorá musí byť pravidelne aktualizovaná a zodpovedať reálnemu stavu,
d. oboznámiť prevádzkovateľa základnej služby s prijatými bezpečnostnými opatreniami a umožniť prevádzkovateľovi základnej služby vykonať audit Poskytovateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení Poskytovateľom s bezpečnostnou politikou prevádzkovateľa základnej služby,
e. najneskôr v lehote 30 pracovných dní odo dňa zistenia nesúladu Poskytovateľom prijatých bezpečnostných opatrení so Zákonom alebo s bezpečnostnou politikou prevádzkovateľa základnej služby zabezpečiť nápravu,
f. oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny,
g. zabezpečiť a odovzdať prevádzkovateľovi základnej služby písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia; ktoré bude zúčastnenou osobou osobne vlastnoručne podpísané v zmysle článku VII. bod 3. tejto Zmluvy,
h. podľa článku X. tejto Zmluvy,

vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty za každé porušenie povinnosti zvlášť a Poskytovateľ sa zaväzuje za každé jedno porušenie povinnosti uhradiť zmluvnú pokutu vo výške 30 000,- EUR.

2. Prevádzkovateľ základnej služby je oprávnený uplatniť si zmluvné pokuty a náhradu škody kedykoľvek v priebehu plnenia predmetu Zmluvy, ako aj po zániku Zmluvy v prípade, ak porušenie zmluvných podmienok stanovených touto Zmluvou zistí po zániku zmluvného vzťahu vyplývajúceho zo Zmluvy.
3. V prípade, ak Poskytovateľ poruší svoje povinnosti podľa čl. XII. bod 5. tejto Zmluvy, vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 100 000,- EUR.
4. Uplatnením ktorejkoľvek zmluvnej pokuty alebo zmluvných pokút v zmysle tohto článku nie je dotknutý nárok prevádzkovateľa základnej služby na náhradu vzniknutej škody v celom rozsahu a právo na uplatnenie ďalšej zmluvnej pokuty podľa tejto Zmluvy. Prevádzkovateľ môže uplatňovať náhradu škody a zmluvnej pokuty kumulatívne, prevádzkovateľ základnej služby má nárok na zaplatenie zmluvnej pokuty a súčasne náhrady škody v plnom rozsahu. Prevádzkovateľ základnej služby je oprávnený jednostranne započítať voči Poskytovateľovi svoje pohľadávky vzniknuté z titulu zmluvnej pokuty a/alebo náhrady škody uplatnenej podľa tejto Zmluvy s pohľadávkami Poskytovateľa vzniknutých z plnenia Zmluvy o poskytovaní služieb.

Článok XIV.
Záverečné ustanovenia

1. Táto Zmluva sa vyhotovuje v štyroch (4) rovnopisoch, tri (3) vyhotovenia pre prevádzkovateľa základnej služby a jedno (1) vyhotovenie pre Poskytovateľa.
2. Akékoľvek dodatky a zmeny tejto Zmluvy sú platné len v písomnej forme, po ich odsúhlasení a podpísaní oboma zmluvnými stranami.
3. V prípade, že sa niektoré z ustanovení tejto Zmluvy stane neplatným, zmluvné strany sa zaväzujú nahradiť neplatné ustanovenie ustanovením platným tak, aby zodpovedalo účelu tejto Zmluvy a najmä vôli zmluvných strán pri uzatváraní tejto Zmluvy. Zostávajúce ustanovenia Zmluvy sú takouto zmenou nedotknuté.
4. Táto Zmluva sa riadi právnym poriadkom Slovenskej republiky, najmä ustanoveniami Obchodného zákonníka, Zákona a vyhláškou č. 362/2018 Z.z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
5. Práva a povinnosti zmluvných strán neupravené v tejto Zmluve sa riadia vyhláškou NBÚ, alebo inými právnymi predpismi vydanými v súlade so zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti a Zákonom.
6. Zmluvné strany vyhlasujú, že ich zmluvná voľnosť nebola žiadnym spôsobom obmedzená.

7. Zmluvné strany vyhlasujú, že táto Zmluva nebola uzavretá v tiesni ani za nápadne nevýhodných podmienok a ani v omyle.
8. Zmluvné strany vyhlasujú, že text tejto Zmluvy je určitým a zrozumiteľným vyjadrením ich vážnej a slobodnej vôle byť ňou viazaný, a že si Zmluvu pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom k nej pripájajú svoje vlastnoručné podpisy.

V Banskej Bystrici, dňa.....

Za Objednávateľa:

_____

Ing. Martin Ľupták, PhD.
predseda predstavenstva
Slovenská pošta, a.s.

_____

Ing. Ľubomír Mindek
podpredseda predstavenstva
Slovenská pošta, a.s.

V Bratislave, dňa .....

Za Poskytovateľa:

_____

Ing. Jozef Chebeň
konateľ
EMM, spol. s r.o.