Zmluva
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatvorená medzi

Východoslovenský ústav srdcových a cievnych chorôb, a. s.

so sídlom	Ondavská 8, 040 11 Košice - mestská časť Západ
Štatutárny orgán:	MUDr. Štefan Lukačín, PhD., MHA, predseda predstavenstva Ing. Marián Albert, PhD., MBA, podpredseda predstavenstva doc. MUDr. Ingrid Schusterová, PhD., MHA, člen predstavenstva
IČO:	36 601 284
DIČ:	2022108704
IČ DPH:	SK2022108704
Bankové spojenie:	Slovenská sporiteľňa, a. s., č. účtu: 0445952274/0900,
IBAN:	SK4809000000000445952274

Spoločnosť je zapísaná v Obchodnom registri Mestského súdu Košice, vložka č. 1360/V, oddiel: Sa
(ďalej len **„prevádzkovateľ základnej služby")**

a

.....

so sídlom	
Štatutárny orgán:	
IČO:	
DIČ:	
IČ DPH:	
Bankové spojenie:	
IBAN:	

Spoločnosť je zapísaná v
(ďalej len **„dodávateľ"')**
(prevádzkovateľ základnej služby a dodávateľ spoločne ďalej len **„zmluvné strany")**

Článok 1
ÚVODNÉ USTANOVENIA

1.1 Spoločnosť Východoslovenský ústav srdcových a cievnych chorôb, a. s. 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 o kybernetickej bezpečnosti").**

1.2 Zmluvné strany uzatvorili dňa ..... zmluvu č. ..... (VÚSCH č. .....) (ďalej len „hlavná zmluva"), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov ako sú definované v zákone o kybernetickej bezpečnosti pre prevádzkovateľa základnej služby.

1.3 Prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti.

1.4 Zmluva stanovuje 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 dodávateľom.

1.5 Pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

1.6 Za kybernetický incident sa podľa tejto zmluvy považuje 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 hlavnej zmluvy,
c) a ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k takému narušeniu kybernetickej bezpečnosti, príp. integrity alebo dostupnosti služby prevádzkovateľa základnej služby

alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby prevádzkovateľa alebo k zníženiu kvality poskytovanej služby prevádzkovateľa základnej služby.

Článok 2
PREDMET ZMLUVY

2.1 V zmysle § 19 ods. 2 zákona o kybernetickej bezpečnosti a s ohľadom na hlavnú zmluvu je predmetom tejto zmluvy stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na hlavnú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby (s ktorými priamo súvisí výkon činností dodávateľa na základe hlavnej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť prevádzkovateľa základnej služby a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov prevádzkovateľa.

2.2 Plnenie povinností podľa tejto zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania zmluvy, a v prípade vzniknutých incidentov a auditu, aj po dobe trvania zmluvy, a to v súlade s platnou legislatívou v oblasti kybernetickej bezpečnosti.

Článok 3
ROZSAH ČINNOSTI DODÁVATEĽA

3.1 Dodávateľ sa zaviazal pre prevádzkovateľa základnej služby poskytovať služby podľa hlavnej zmluvy. Na plnenie predmetu hlavnej zmluvy budú dodávateľovi poskytnuté/sprístupnené nasledovné aktíva:

a) Virtuálny server PACS-TM
b) Virtuálny server Tomocon-Go
c) NAS offline PACS archív 1
d) NAS offline PACS archív 2

Pokiaľ dôjde k vytvoreniu nového aktíva, tak jeho definovanie a sprístupnenie bude vykonané v rámci projektovej dokumentácie.

3.2 Pri prístupe k IKT aktívam:

a) Dodávateľ sa zaväzuje v súvislosti s plnením predmetu hlavnej zmluvy dodržiavať klasifikáciu informácií uvedenú v Tabuľke č. 1. Všetky údaje poskytnuté Dodávateľovi na základe Hlavnej zmluvy sa považujú za prísne chránené.

b) Dodávateľ berie na vedomie, že poskytovanie prístupov v rámci siete prevádzkovateľa základnej služby vrátane vykonávania zmien sprístupnených informácií/aktív, je riadené, monitorované a auditované v súlade s platnou internou dokumentáciou.

c) Akceptovateľné použitie informácií/IKT aktív je:
   I. zhotovovať obrazový záznam IKT aktív len po predchádzajúcom súhlase Manažéra a kybernetickej bezpečnosti. Súhlas musí byť vydaný v dokumentovanej podobe,
   II. pristupovať k P2P sieťam len v správe prevádzkovateľa základnej služby,
   III. mimo prostredia prevádzkovateľa základnej služby vynášať IKT zariadenia len so súhlasom oprávneného zamestnanca prevádzkovateľa základnej služby. Súhlas musí byť vydaný v dokumentovanej podobe s uvedením dôvodu a dátumu návratu zariadenia, ak sa predpokladá jeho návrat,
   IV. k zariadeniam, ktoré sú pripojené do siete prevádzkovateľa základnej služby, 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 prevádzkovateľa základnej služby, alebo boli schválené na používanie v sieti prevádzkovateľa základnej služby,
   V. využívať zariadenia/softvér na prienik do dátových sietí, testovanie zraniteľností, odpočúvanie a zaznamenávanie dátovej komunikácie len po predchádzajúcom súhlase osôb určených prevádzkovateľom základnej služby.

3.3 Neakceptovateľné použitie IKT aktív je:
a) využívať pripojenie na Internet na nepracovné účely, s výnimkou využitia nezabezpečenej siete WiFi prevádzkovanej prevádzkovateľom základnej služby,
b) umožniť zariadeniam fyzicky pripojeným do siete prevádzkovateľa základnej služby súčasné pripojenie do inej siete (napr. GSM internet, Wi-Fi).

3.4 Na prístup k IKT aktívam prevádzkovateľa základnej služby, uvedeným v bode 3.1 tohto článku zmluvy, budú autorizovaní zamestnanci dodávateľa:[1]

1. .....
2. .....
3. .....
4. .....

Poskytnutie nových, prípadne zmena existujúcich, prístupových práv k IKT aktívu sa vykonáva výhradne na základe Žiadosti o pridelenie/zmenu prístupu k IKT aktívu vlastníkovi IKT aktíva formou e-mailu. Všetky prístupové práva, ktoré nie sú výslovne povolené prevádzkovateľom základnej služby, sú zakázané.

3.5 Ak má dodávateľ fyzický prístup k IKT aktívam prevádzkovateľa základnej služby, zaväzuje sa, že počas pobytu v priestoroch prevádzkovateľa základnej služby, bude dodržiavať všeobecné zásady bezpečnosti práce, protipožiarnej ochrany a ochrany životného prostredia.

3.6 Ak má dodávateľ prístup k osobným údajom, zaväzuje sa zabezpečiť ochranu osobných údajov v súlade s Nariadením Európskeho parlamentu a Rady 2016/679 a Zákonom o ochrane osobných údajov.

3.7 Neprerušiteľnosť spracovania: Dodávateľ je povinný realizovať predmet hlavnej zmluvy tak, aby nedošlo k prerušeniu, alebo obmedzeniu prevádzky prevádzkovateľa základnej služby. V prípade, ak plnenie predmetu hlavnej zmluvy nevyhnutne vyžaduje prerušenie alebo obmedzenie prevádzky prevádzkovateľa základnej služby, je dodávateľ povinný vopred preukázateľne o tejto skutočnosti informovať prevádzkovateľa základnej služby a do doby, pokiaľ dodávateľ nedostane inštrukcie od prevádzkovateľa základnej služby o ďalšom postupe, alebo súhlas s plnením predmetu hlavnej zmluvy je dodávateľ povinný zdržať sa takého vykonávania predmetu hlavnej zmluvy, ktoré by mohlo spôsobiť prerušenie, alebo obmedzenie prevádzky prevádzkovateľa základnej služby. V opačnom prípade zodpovedá dodávateľ za škody, ktoré týmto spôsobí prevádzkovateľovi základnej služby.

3.8 Vrátenie aktív: Zmluvné strany sú povinné po zániku hlavnej zmluvy:

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

3.9 Dodávateľ sa zaväzuje urobiť opatrenia, aby:

a) pri plnení jeho záväzkov podľa hlavnej zmluvy nedochádzalo z jeho strany k porušovaniu licenčných pravidiel platných pre písomne odsúhlasené alebo v hlavnej zmluve uvedené verzie operačných systémov, databázového prostredia a ďalších podporných a integračných softvérov, slúžiacich pre prevádzku aplikačného softvéru prevádzkovateľa základnej služby, ktorého dodávka/úprava/podpora je predmetom záväzku dodávateľa podľa hlavnej zmluvy, alebo ktorého sa týka poskytnutie služieb v zmysle hlavnej zmluvy (ďalej len „pravidlá licenčnej politiky“) a
b) aby plnenie, ktoré prevádzkovateľovi na základe hlavnej zmluvy poskytne, neporušovalo pravidlá licenčnej politiky. Ak sa preukáže porušenie pravidiel licenčnej politiky, ktoré bolo spôsobené činnosťou dodávateľa, dodávateľ sa zaväzuje uhradiť prevádzkovateľovi základnej služby všetky náhrady škody, prípadne všetky iné finančné náklady, ktoré prevádzkovateľovi základnej služby vzniknú v dôsledku takéhoto porušenia pravidiel licenčnej politiky dodávateľom a budú uplatnené autorom softvéru, prípadne inou oprávnenou osobou voči prevádzkovateľovi základnej služby. Akákoľvek limitácia náhrady škody dohodnutá v hlavnej zmluve sa nevzťahuje na náhradu škody, ktorú je dodávateľ povinný zaplatiť prevádzkovateľovi základnej služby v zmysle tohto bodu zmluvy. Povinnosť nahradiť vzniknutú škodu alebo iné finančné náklady, ktoré prevádzkovateľovi základnej služby vzniknú v dôsledku porušenia pravidiel licenčnej politiky dodávateľom trvá aj po ukončení platnosti hlavnej zmluvy, a to aj v prípade, ak bol nárok na ich zaplatenie uplatnený voči prevádzkovateľovi základnej služby po ukončení platnosti hlavnej zmluvy.

3.10 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

[1] Dodávateľ uvedie titul, meno, priezvisko, pracovné zaradenie a kontaktné údaje (telefónne číslo a e-mailová adresa) autorizovaných zamestnancov; doplní riadky podľa potreby.

skontrolované, či neobsahujú malvér (škodlivý kód) a počas prenosu s nimi bude narábané v súlade s ustanoveniami uvedenými v Tabuľke č. 1 tejto zmluvy:

		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 VÚSCH, a. s. 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 možnosti náhodného zverejnenia.	Primeraná fyzická ochrana; zamedziť možnosti náhodného zverejnenia.
	Prenos e-mail	Bez osobitných opatrení.	V rámci domény VUSCH.SK bez osobitných opatrení; mimo domény VUSCH.SK šifrovane.	V rámci domény VUSCH.SK aj mimo nej šifrovane.	V rámci domény VUSCH.SK aj mimo nej šifrovane.
	Prenos - ostatné elektronické kanály	Bez osobitných opatrení.	V rámci domény VUSCH.SK bez osobitných opatrení; mimo domény VUSCH.SK šifrovane.	V rámci domény VUSCH.SK aj mimo nej šifrovane.	V rámci domény VUSCH.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 VÚSCH, a. s. a definované osoby zmluvného	S povolením spracovateľa.	S povolením spracovateľa.

			subjektu neobmedzené.		
	Kopírovanie (rozmnožovanie)	Bez osobitných opatrení.	Pre potreby zamestnancov VÚSCH, a. s. 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 neautorizovaném u prístupu (napr. uzamykateľná skriňa, uzamykateľná zásuvka, a pod.)	Primeraná fyzická ochrana; zamedziť neautorizovaném u 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 Po-06 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.

3.11 Dokumentácia dodávaná dodávateľom k plneniam podľa hlavnej zmluvy bude klasifikovaná v súlade s klasifikáciou informácii prevádzkovateľa základnej služby v súlade s požiadavkami zákona o kybernetickej bezpečnosti 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“. Dodávateľ 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 4
POVINNOSTI DODÁVATEĽA

4.1 Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam bezpečnostných opatrení prevádzkovateľa základnej služby a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v Prílohe č. 1 tejto zmluvy. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami uvedenými v tejto zmluve a bude spĺňať minimálne požiadavky na bezpečnostné opatrenia v závislosti od kategorizácie sietí a informačných systémov pre kategóriu III v súlade s Prílohou č. 3 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.

4.2 Dodávateľ je zároveň povinný dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby, prevádzkovateľom základnej služby vydané bezpečnostné smernice a štandardy (ďalej len ako „bezpečnostné politiky"), s ktorými ho prevádzkovateľ základnej služby písomne oboznámi. Dodávateľ berie na vedomie, že bezpečnostné politiky predložené dodávateľovi sú predmetom ochrany podľa zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami prevádzkovateľa základnej služby. Platnú bezpečnostnú politiku prevádzkovateľ základnej služby poskytne dodávateľovi po nadobudnutí účinnosti tejto zmluvy.

4.3 Dodávateľ 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 dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby.

4.4 Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy.

4.5 Dodávateľ 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.

4.6 Dodávateľ je povinný doručiť prevádzkovateľovi úplný zoznam svojich zamestnancov, ktorí sa budú podieľať na plnení hlavnej zmluvy a tejto zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby ako Zoznam pracovných rolí, ktorý tvorí Prílohu č. 2 tejto zmluvy, a každú zmenu v personálnom obsadení je dodávateľ povinný prevádzkovateľovi základnej služby písomne oznámiť, a to najneskôr do 5 pracovných dní odo dňa uzatvorenia tejto zmluvy, resp. odo dňa účinnosti personálnej zmeny.

4.7 Dodávateľ sa zaväzuje zabezpečiť a odovzdať Objednávateľovi písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia hlavnej zmluvy (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 o kybernetickej bezpečnosti dozvedela a ktoré nie sú verejne známe. Povinnosť zúčastnenej osoby zachovávať mlčanlivosť podľa tohto bodu zmluvy trvá aj po skončení právneho vzťahu medzi zúčastnenou osobou a dodávateľom; tým nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

4.8 Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi základnej služby na nahliadnutie a zhotovenie kópií.

4.9 Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti v rozsahu podľa vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúr bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, a v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa základnej služby.

4.10 Dodávateľ je povinný prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa základnej služby.

4.11 Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa základnej služby podľa zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania zmluvy.

4.12 Odplata za plnenie povinností dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom základnej služby dodávateľovi podľa hlavnej zmluvy

a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto zmluvy o prevádzkovateľa základnej služby nemá nárok.

4.13 Dodávateľ sa zaväzuje, že nezapojí ďalšieho dodávateľa (ďalej len „**subdodávateľ**“) úplne alebo čiastočne zabezpečujúceho plnenie tejto zmluvy predtým, než dostane písomný súhlas Prevádzkovateľa základnej služby. Dodávateľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným personálnym, technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Dodávateľa uvedené v tejto zmluve. Dodávateľ je plne zodpovedný voči prevádzkovateľovi základnej služby za plnenie povinností subdodávateľa tak, ako by ich poskytoval sám.

4.14 Dodávateľ sa zaväzuje dodržiavať nasledovné základné bezpečnostné požiadavky (t. j. aplikovateľné bez ohľadu na typ produktu alebo služby) počas celej doby trvania zmluvy:

a) dodávateľ poskytuje aktuálny zoznam všetkých komponentov použitých v riešení na úrovni výrobcov a verzií,
b) produkt/služba sú dodávané vo výrobcom alebo výrobcami jednotlivých komponentov podporovaných verziách,
c) dodávateľ včas upozorňuje prevádzkovateľa základnej služby na zistené bezpečnostné (technické) zraniteľnosti dodávaného produktu/služby, vrátane všetkých komponentov, ktoré zistil sám alebo o ktorých sa dozvedel,
d) dodávaný produkt/služba je pravidelne aktualizovaný na bezpečnostné záplaty – buď priamo dodávateľom alebo nepriamo prostredníctvom aktualizovaných návodov od dodávateľa,
e) dodávateľ upozorňuje prevádzkovateľa základnej služby na všetky udalosti, zmeny v ním dodávanom produkte/službe, ktoré môžu alebo mohli viesť k bezpečnostnému incidentu (nesprávna konfigurácia, neoprávnený alebo pokus o neoprávnený prístup, zneužitie prístupov oprávnenou osobou, chýbajúce bezpečnostné záplaty, výsledok scanu na technické zraniteľnosti a pod.),
f) dodávateľ dodáva produkt/službu v minimálne nevyhnutnej a zabezpečenej konfigurácii.

Článok 5
PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

5.1. Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby, (ďalej len **„incidenty"):**

a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa základnej služby,
b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy a tejto zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby,
c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
d) sledovať hrozby dotýkajúce sa dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,
e) predchádzať vzniku incidentov,
f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
g) prijímať od prevádzkovateľa základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,
h) zasielať prevádzkovateľovi základnej služby včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a
i) spolupracovať s prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.

Článok 6
REAKTIVITA PRI RIEŠENÍ INCIDENTOV

6.1. Dodávateľ je povinný bezodkladne hlásiť každý incident prevádzkovateľovi základnej služby kontaktnej osobe uvedenej v článku 8 bod 8.2 tejto zmluvy na e-mailovú adresu kontaktnej osoby, v rozsahu nasledovných informácií:

a) informácie o tom, kto hlási kybernetický bezpečnostný incident:
   I. identifikačné údaje dodávateľa,
   II. funkcia a pracovné zaradenie osoby dodávateľa, ktorá hlási kybernetický bezpečnostný incident,
   III. identifikačné údaje ďalších organizácií dotknutých kybernetickým bezpečnostným incidentom,

b) informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu:
   I. kategória kybernetického bezpečnostného incidentu (bezpečnostný incident I. stupňa, bezpečnostný incident II. stupňa, bezpečnostný incident III. stupňa),
   II. typ závažného kybernetického bezpečnostného incidentu
      a. nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),

b. škodlivý kód (vírus, malvér, ransomvér),
c. získavanie informácií (skenovanie siete, odpočúvanie, sociálne inžinierstvo),
d. pokus o prienik do systému,
e. podozrenie na úspešný prienik do systému vrátane APT,
f. nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby),
g. neoprávnený prístup k informáciám, únik informácií, poškodenie informácií,
h. podvod (neautorizované využitie prostriedkov, porušenia autorských práv),
i. zraniteľnosť (ich existencia),
j. iné,

III. časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu
a. čas začiatku incidentu (ak je známy), čas a spôsob zistenia incidentu, informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,

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

c) informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom:
I. prvotne zasiahnuté aktíva (Host/IP), vrátane identifikácie informačného systému a prevádzkových parametrov služby,
II. 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,
III. stav riešenia závažného kybernetického bezpečnostného incidentu,
IV. informácia o vykonaní nápravných opatrení smerujúcich k riešeniu hláseného závažného kybernetického bezpečnostného incidentu,
V. opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,
VI. popis možných negatívnych dopadov, opatrení a možných dôsledkov závažného kybernetického bezpečnostného incidentu,
VII. výsledok opatrení,
VIII. dátum a čas realizácie opatrení.

6.2. Dodávateľ je povinný hlásiť prevádzkovateľovi základnej služby ďalšie informácie požadované prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti, 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 o kybernetickej bezpečnosti,
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 o kybernetickej bezpečnosti 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 o kybernetickej bezpečnosti.

6.3. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, dodávateľ je povinný odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

6.4. Dodávateľ je povinný riešiť incidenty najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len **„reaktívne opatrenie").** Pri riešení incidentov je dodávateľ povinný na žiadosť prevádzkovateľa základnej služby spolupracovať s prevádzkovateľom základnej služby, Národným bezpečnostným úradom a Ministerstvom zdravotníctva Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.

6.5. Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho prevádzkovateľovi základnej služby.

6.6. Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.

6.7. Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.

6.8. Po vyriešení incidentu je dodávateľ na výzvu prevádzkovateľa základnej služby v určenej lehote povinný predložiť prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len **„ochranné opatrenia")** na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom základnej služby na jeho návrhu.

6.9. Po schválení ochranného opatrenia prevádzkovateľom základnej služby je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať.

6.10. Po vykonaní ochranného opatrenia dodávateľom je dodávateľ povinný preveriť jeho účinnosť.

Článok 7
MLČANLIVOSŤ

7.1. Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením hlavnej zmluvy a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.

7.2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.

7.3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.

7.4. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu alebo obchodného vzťahu.

7.5. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. tieto podľa pokynu prevádzkovateľa základnej služby zničiť.

Článok 8
KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

8.1 Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom základnej služby spôsobom určeným prevádzkovateľom základnej služby, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

8.2 Prevádzkovateľ základnej služby určuje nasledovnú kontaktnú osobu pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti: Ing. Marián Albert, PhD., MBA, manažér kybernetickej bezpečnosti, t. č. 055/789 2698, e-mail: marian.albert@vusch.sk

8.3 Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti: _____[2].

8.4 Kontaktné osoby podľa odsekov 8.2 alebo 8.3 tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok 9
SPOLOČNÉ USTANOVENIA

9.1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

9.2. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto zmluvy v súlade so sektorovými bezpečnostnými opatreniami, ktoré vydáva Ministerstvo zdravotníctva Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.

9.3. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov

[2] Dodávateľ uvedie titul, meno, priezvisko, pracovné zaradenie a kontaktné údaje (telefónne číslo a e-mailová adresa) ním určenej kontaktnej osoby.

prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

9.4. Dodávateľ je povinný mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto zmluvy v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.

9.5. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa základnej služby mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.

9.6. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy bezodkladne, pokiaľ nie je v tejto zmluve alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.

9.7. V prípade, ak dodávateľ plní zmluvu prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, 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 základnej služby mohol vykonať audit v súlade s ustanoveniami tejto zmluvy aj u týchto subdodávateľov.

9.8. Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto zmluvy ohrozuje plnenie cieľov tejto zmluvy, pričom za dôsledky incidentov, ktoré by sa pri riadnom a včasnom plnení povinností dodávateľa podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá prevádzkovateľovi základnej služby v plnom rozsahu (zodpovednosť za výsledok).

9.9. V prípade, ak dodávateľ spôsobí prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov. Pre odstránenie právnych pochybností, zodpovednosť dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti dodávateľom.

9.10. Miestom pre doručovanie písomností sú adresy zmluvných strán uvedené v záhlaví tejto zmluvy. Každá zo zmluvných strán je povinná písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu ohľadne doručovania, a to najneskôr do 5 pracovných dní po tom, čo k takejto zmene dôjde. Pokiaľ sa z dôvodu oneskoreného alebo nevykonaného oznámenia o zmene miesta doručovania nepodarí včas a riadne doručiť písomnosť druhej zmluvnej strane, považuje sa deň neúspešného pokusu o opakované doručenie písomnosti za deň doručenia písomnosti druhej zmluvnej strane so všetkými právnymi dôsledkami pre dotknutú zmluvnú stranu.

9.11. 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 Prílohe č. 7 (Postup nahlasovania incidentov) bode 6 hlavnej zmluvy alebo zmluvnými stranami oznámeným iným preukázateľným spôsobom. Zmluvné strany sú oprávnené dohodnúť si aj iný spôsob komunikácie a výmeny informácií pre prípady identifikované týmto bodom, napr. formou osobitného spôsobu 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 10
KONTROLA A AUDIT KYBERNETICKEJ BEZPEČNOSTI

10.1. Prevádzkovateľ základnej služby je oprávnený vykonať u dodávateľa kontrolu a 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.

10.2. Dodávateľ sa zaväzuje, že prevádzkovateľovi základnej služby umožní kedykoľvek vykonať kontrolu a audit, ktorým si prevádzkovateľ základnej služby overí mieru a efektívnosť plnenia povinností dodávateľom uvedených v bode 10.1. tohto článku zmluvy, 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.

10.3. Prípadné nedostatky zistené kontrolou alebo auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.

10.4. Prevádzkovateľ základnej služby môže kontrolu a audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti prevádzkovateľa základnej služby pri výkone auditu realizuje prevádzkovateľom základnej služby poverená tretia osoba. Prevádzkovateľ základnej služby včas oznámi dodávateľovi identifikačné údaje osoby/osôb, prostredníctvom ktorej/ktorých vykoná kontrolu/audit.

10.5. Dodávateľ 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.

10.6. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

10.7. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi základnej služby 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. Takisto je povinný umožniť prevádzkovateľovi základnej služby prístup k spracovávaným alebo uchovávaným na základe tejto zmluvy a hlavnej zmluvy, resp. s nimi súvisiacimi.

10.8. Prevádzkovateľ základnej služby je povinný oznámiť dodávateľovi najmenej tri (3) pracovné dni vopred svoj zámer realizovať u dodávateľa audit. Dodávateľ je povinný bez zbytočného odkladu termín auditu potvrdiť alebo navrhnúť iný termín tak, aby sa audit uskutočnil najneskôr do 10 kalendárnych dní odo dňa zaslania oznámenia. Pokiaľ dodávateľ termín auditu nepotvrdí, má sa za to, že s termínom auditu súhlasí.

10.9. Vykonanie alebo nevykonanie auditu prevádzkovateľom základnej služby nezbavuje dodávateľa zodpovednosti za plnenie povinností dodávateľa vyplývajúcich z tejto zmluvy.

10.10. Dodávateľ je povinný písomne informovať prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom.

10.11. Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

10.12. Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Ustanovenia článku 7 ods. 7.2 a 7.3 tejto zmluvy platia rovnako a ustanovenie článku 7 ods. 7.4 tejto zmluvy platí primerane.

10.13. Prevádzkovateľ základnej služby a jeho zamestnanci 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 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 dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne dodávateľ. Dodávateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby 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.

10.14. Prevádzkovateľ základnej služby je oprávnený vykonávať audit u dodávateľ nasledovne, pričom zmluvné strany majú pri výkone auditu nasledovné práva a povinnosti

Článok 11
SANKCIE A NÁHRADA ŠKODY

11.1. V prípade, ak dodávateľ 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 o kybernetickej bezpečnosti,
   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 dodávateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení dodávateľom s bezpečnostnou politikou prevádzkovateľa základnej služby,

e) najneskôr v lehote 30 pracovných dní odo dňa zistenia nesúladu dodávateľom prijatých bezpečnostných opatrení so zákonom o kybernetickej bezpečnosti alebo s bezpečnostnou politikou prevádzkovateľa základnej služby zabezpečiť nápravu,
f) neodkladne oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote najneskôr do 5 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 4 bod 4.7 tejto zmluvy,
h) podľa článku 6. tejto Zmluvy,

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

11.2. 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.

11.3. V prípade, ak dodávateľ poruší svoje povinnosti podľa článku 12 bod 12.7 tejto zmluvy, vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 100.000,- € (slovom: stotisíc Eur).

11.4. Uplatnením ktorejkoľvek zmluvnej pokuty alebo zmluvných pokút v zmysle tohto článku zmluvy 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 základnej služby 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 dodávateľovi svoje pohľadávky vzniknuté z titulu zmluvnej pokuty a/alebo náhrady škody uplatnenej podľa tejto zmluvy s pohľadávkami dodávateľa vzniknutými z plnenia hlavnej zmluvy.

Článok 12
ZÁVEREČNÉ USTANOVENIA

12.1. Táto zmluva sa uzatvára na dobu určitú, a to počas platnosti hlavnej zmluvy.

12.2. Prevádzkovateľ základnej služby je oprávnený od tejto zmluvy odstúpiť v prípadoch:
a) podstatného porušenia tejto zmluvy zo strany dodávateľa;
b) ak je na dodávateľa vyhlásený konkurz, alebo bola povolená reštrukturalizácia, alebo ak bolo vyhlásenie konkurzu odmietnuté alebo zrušené pre nedostatok majetku alebo ak dodávateľ vstúpil do likvidácie alebo iným spôsobom ukončí svoju podnikateľskú činnosť;
c) dodávateľ stratí predpoklady na plnenie tejto zmluvy.

12.3. Za podstatné porušenie zmluvy sa považuje:
a) porušenie povinností uvedených v článku 4 bod 4.1 a 4.8, článku 6, článku 7 tejto zmluvy;
b) ak dodávateľ vedel v čase uzavretia zmluvy alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola zmluva uzavretá, že prevádzkovateľ základnej služby nebude mať záujem na plnení povinností pri takom porušení zmluvy;
c) dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto zmluvy.

12.4. Odstúpenie od tejto zmluvy sa musí urobiť písomne, inak sa na neho neprihliada. Pre doručovanie odstúpenia od tejto zmluvy sa použijú ustanovenia zmluvy o doručovaní.

12.5. Zrušenie tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto zmluvy, a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do zrušenia tejto zmluvy.

12.6. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán, a to ku dňu dohodnutému v písomnom vyhotovení dohody o ukončení tejto zmluvy, nikdy však nie pred uplynutím účinnosti hlavnej zmluvy. V prípade, ak zmluvné strany dohodnú deň ukončenia tejto zmluvy pred dňom uplynutia účinnosti hlavnej zmluvy, táto zmluvy zaniká súčasne so zánikom účinnosti hlavnej zmluvy (dohodou/výpoveďou/odstúpením od hlavnej zmluvy).

12.7. Po ukončení tejto zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich (5) rokov po ukončení tejto zmluvy. Alternatívou k postupu podľa predchádzajúcej vety je využitie služby Software Escrow, na ktorej sa dohodnú zmluvné strany, pričom vzniknuté náklady budú znášať rovným dielom.

12.8. Táto zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka č. 513/1991 Zb. v znení neskorších predpisov a súvisiacimi predpismi.

12.9. Prípadné spory vyplývajúce z tejto zmluvy budú riešené predovšetkým mimosúdne. Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov týkajúcich sa tejto zmluvy. V prípade, ak dodávateľom bude zahraničná osoba, zmluvné strany sa dohodli, že miestne príslušným súdom bude súd, v obvode ktorého má sídlo prevádzkovateľ základnej služby.

12.10. Táto zmluva sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo zmluvy nevyplýva niečo iné.

12.11. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto zmluvy na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.

12.12. Táto zmluva sa uzatvára v slovenskom jazyku a zmluvné strany sa dohodli, že v slovenskom jazyku budú vzájomne komunikovať.

12.13. Ak niektoré ustanovenia tejto zmluvy budú zmluvné strany, súd alebo iné kompetentné orgány považovať za neplatné alebo nevymáhateľné, potom takéto ustanovenie bude neplatné iba v dotknutom a v najužšom možnom rozsahu, pričom jeho zvyšná časť, význam a dopady, ako aj ostatné ustanovenia tejto zmluvy zostávajú v platnosti. Zmluvné strany budú v takom prípade postupovať tak, aby účel ustanovení považovaných za nevymáhateľné alebo neplatné bol v maximálne možnej miere rešpektovaný a pre zmluvné strany právne záväzný vo forme umožňujúcej jeho právnu vymáhateľnosť.

12.14. Táto zmluva tvorí úplnú dohodu medzi zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto zmluvy zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto zmluvy a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych v tejto zmluve neuvedených ústnych dojednaní a dohôd.

12.15. Táto zmluva bola vyhotovená v štyroch (4) rovnopisoch, (2) dve vyhotovenia pre každú zmluvnú stranu.

12.16. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
a) Príloha č. 1 - Zoznam minimálnych bezpečnostných opatrení
b) Príloha č. 2 - Zoznam pracovných rolí
c) Príloha č. 3 - Zoznam subdodávateľov

12.17. Táto zmluva nadobúda platnosť a účinnosť dňom podpisu oboma zmluvnými stranami.

12.18. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.

Prevádzkovateľ základnej služby:

V Košiciach, dňa

.....
Východoslovenský ústav srdcových
a cievnych chorôb, a. s.
MUDr. Štefan Lukačín, PhD., MHA
predseda predstavenstva

.....
Východoslovenský ústav srdcových
a cievnych chorôb, a. s.
Ing. Marián Albert, PhD., MBA
podpredseda predstavenstva

Dodávateľ:

V Košiciach, dňa

.....

Príloha č. 1 Zoznam minimálnych bezpečnostných opatrení

1. Pre oblasť technických zraniteľností informačných systémov a zariadení dodávateľ najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb 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 dodávateľ 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 dodávateľ 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 dodávateľ 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 dodávateľ 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.

Príloha č. 2 Zoznam pracovných rolí

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou základnej služby**	**Telefónny kontakt**	**Email**

Príloha č. 3 Zoznam subdodávateľov

P. č.	Subdodávateľ	Údaje o osobe oprávnenej konať za subdodávateľa	Predmet subdodávky
1.			
2.			
3.			
4.			
5.			