

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená v zmysle 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**“)
(ďalej len „**zmluva**“)

medzi zmluvnými stranami:

Prevádzkovateľ:	Kancelária Národnej rady Slovenskej republiky
Sídlo:	Námestie Alexandra Dubčeka 1, 812 80 Bratislava 1
IČO:	XXXXXX
Zastúpený:	XXXXXX, vedúci Kancelárie NR SR

(ďalej len „**Prevádzkovateľ základnej služby**“)

a

Dodávateľ:
Sídlo:
IČO:
IČ DPH:
Zastúpený:
Zapísaný:

(ďalej len „**Dodávateľ**“)

(Prevádzkovateľ základnej služby a Dodávateľ spolu ďalej len „**zmluvné strany**“)

Článok I. ÚVODNÉ USTANOVENIA

1. **Kancelária Národnej rady Slovenskej republiky** je Prevádzkovateľom základnej služby podľa zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby.
2. Prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom túto zmluvu podľa zákona o kybernetickej bezpečnosti.
3. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na Zmluvu o zo dňa (ďalej aj len ako „**dodávateľská zmluva**“), na základe ktorej Dodávateľ bude poskytovať Prevádzkovateľovi výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby.
4. Plnenie povinností podľa zákona o kybernetickej bezpečnosti a tejto zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania zmluvy, pokiaľ zo všeobecne záväzných

právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľskej zmluvy.

Článok II. ZÁKLADNÉ POJMY

1. Na účely tejto zmluvy sa rozumie:

- a) sieťou elektronická komunikačná sieť podľa zákona č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov,
- b) informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,
- c) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,
- d) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
- e) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
- f) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
- g) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
- h) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,
- i) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
- j) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
- k) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
 - strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
 - obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
 - vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
 - ohrozenie bezpečnosti informácií,
- l) kybernetickým bezpečnostným incidentom je aj udalosť:
 - ktorú zistí alebo o ktorej sa dozvie Dodávateľ,

- ktorá sa týka informačných systémov alebo sietí vo vzťahu ku ktorým Dodávateľ poskytuje výkon činností podľa dodávateľskej zmluvy,
 - a ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k takému narušeniu kybernetickej bezpečnosti príp. integrity alebo dostupnosti služby Prevádzkovateľa, alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby Prevádzkovateľa alebo k zníženiu kvality poskytovanej služby Prevádzkovateľa.
- m) základnou službou služba, ktorá je zaradená v zozname základných služieb a
- závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona o kybernetickej bezpečnosti alebo
 - je prvkom kritickej infraštruktúry,
- n) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písm. m) tohto článku tejto zmluvy
- o) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2 zákona o kybernetickej bezpečnosti,
- p) manažér informačnej bezpečnosti (MIB) je osoba poverená riadením informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti definované v Politike informačnej bezpečnosti a ďalších smerniciach Prevádzkovateľa základnej služby. Ide najmä o kontrolné činnosti, riešenie bezpečnostných a kybernetických incidentov, riadenie implementácie bezpečnostných opatrení, konzultačné a metodické činnosti pre oblasť informačnej a kybernetickej bezpečnosti a ďalšie,
- q) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

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

Článok III. PREDMET ZMLUVY

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na dodávateľskú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov Prevádzkovateľa základne služby (s ktorými priamo súvisí výkon činností Dodávateľa na základe dodávateľskej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť Prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov Prevádzkovateľa.

Článok IV. POVINNOSTI DODÁVATEĽA

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa základnej služby 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. 2 tejto zmluvy.

2. Dodávateľ vyhlasuje, že súhlasí so stanovenými bezpečnostnými opatreniami v tejto zmluve.
3. Dodávateľ je povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby, s ktorými ho Prevádzkovateľ základnej služby písomne oboznámil. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa základnej služby.
4. 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. Dodávateľ sa zaväzuje dodržiavať takto zmenené alebo doplnené bezpečnostné opatrenia Prevádzkovateľa základnej služby od okamihu, v ktorom ho s nimi Prevádzkovateľ základnej služby preukázateľne oboznámi.
5. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto zmluvy.
6. 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 dodávateľskej zmluvy a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy od Prevádzkovateľa základnej služby nemá nárok.
7. 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. Zoznam subdodávateľov tvorí prílohu č. 3 tejto zmluvy. Dodávateľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným 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, pričom dodávateľ je povinný garantovať dodržiavanie bezpečnostných opatrení vyplývajúcich z tejto zmluvy aj subdodávateľom
8. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa základnej služby podľa dodávateľskej zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania dodávateľskej zmluvy.
9. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.

10. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek kladených na Prevádzkovateľa základnej služby podľa zákona o kybernetickej bezpečnosti alebo vyhlášky, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve.
11. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi základnej služby dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany“ v zmysle zákona o kybernetickej bezpečnosti.
12. Ostatný konkrétny rozsah činnosti Dodávateľa je stanovený dodávateľskou zmluvou.

Článok V.

BEZPEČNOSTNÉ OPATRENIA

1. Dodávateľ sa zaväzuje, že má zavedené a implementované bezpečnostné opatrenia minimálne v rozsahu:
 - organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
 - riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
 - personálnej bezpečnosti,
 - riadenia prístupov,
 - riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
 - bezpečnosti pri prevádzke informačných systémov a sietí,
 - hodnotenia zraniteľností a bezpečnostných aktualizácií,
 - ochrany proti škodlivému kódu,
 - sieťovej a komunikačnej bezpečnosti,
 - akvizície, vývoja a údržby informačných sietí a informačných systémov,
 - zaznamenávania udalostí a monitorovania,
 - fyzickej bezpečnosti a bezpečnosti prostredia,
 - riešenia kybernetických bezpečnostných incidentov,
 - kryptografických opatrení,
 - kontinuity prevádzky,
 - auditu, riadenia súladu a kontrolných činností.
2. Bezpečnostné opatrenia musia zahŕňať najmenej:
 - určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
 - detekciu kybernetických bezpečnostných incidentov,
 - evidenciu kybernetických bezpečnostných incidentov,
 - postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
 - určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
 - pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálného systému včasného varovania.
3. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu v organizácii.

4. Obsah a štruktúra bezpečnostnej dokumentácie:

- Schválená bezpečnostná stratégia kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,
- Klasifikácia informácií a kategorizácia sietí a informačných systémov,
- Zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
- Vykonaná analýza rizík kybernetickej bezpečnosti,
- Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti (§ 29 zákona o kybernetickej bezpečnosti).

Článok VI.

PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje 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 dodávateľskej 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.
2. Dodávateľ sa riadne oboznámil s rozsahom a povahou záväzkov podľa tejto zmluvy a sa zaväzuje počas trvania tejto zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto zmluvy.
3. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí sa budú podieľať na plnení dodávateľskej zmluvy a tejto zmluvy a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby, je uvedený v prílohe č. 1. tejto zmluvy. Dodávateľ je povinný písomne oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení a to bezodkladne po tom, ako táto zmena v personálnom obsadení

nastane; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Dodávateľ je povinný zaviazť povinnosťou mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení podľa tohto bodu.

4. Dodávateľ sa zaväzuje 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.
5. Dodávateľ sa zaväzuje prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN 150/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
6. Dodávateľ sa zaväzuje prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa §8, §9, §10, §12, §14 a §15 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 a v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
7. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

Článok VII. POSTUP PRI RIEŠENÍ INCIDENTOV

1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý incident Prevádzkovateľovi základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Dodávateľ sa zaväzuje riešiť incidenty najmä odozvou alebo inou reakciou na incident, ohraňovaním 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**“) a to ako na výzvu Prevádzkovateľa základnej služby, tak aj bez jeho výzvy, ak sa o incidente dozvie. Pri riešení incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a Ministerstvom hospodárstva 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.
3. Dodávateľ pri riešení a reakcii na incident postupuje v súlade so všeobecne záväznými právnymi predpismi, ako aj svojimi internými procedúrami a postupmi tak, aby bol incident a jeho dôsledky odstránené v čo najkratšom možnom čase.

4. Dodávateľ sa zaväzuje oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby.
6. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.
7. 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.
8. Po schválení ochranného opatrenia Prevádzkovateľom základnej služby, je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní ochranného opatrenia Dodávateľom, je Dodávateľ povinný preveriť jeho účinnosť.

Článok VIII.

ZÁVÄZOK MLČANLIVOSTI

1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením dodávateľskej zmluvy a tejto zmluvy, a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti. Dodávateľ je povinný chrániť najmä 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. Dodávateľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Dodávateľovi.
2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.
4. Dodávateľ sa zaväzuje zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu, obchodného vzťahu alebo iného vzťahu.
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.
6. Dodávateľ je povinný zabezpečiť, aby sa každá osoba uvedená v Prílohe č. 1 tejto zmluvy zaviazala zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti. Tento záväzok mlčanlivosti je Dodávateľ povinný preukázať Prevádzkovateľovi základnej

služby u každej z týchto osôb. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom základnej služby a Dodávateľom.

Článok IX.

KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Dodávateľ sa zaväzuje 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.
2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.
3. Dodávateľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.
4. Kontaktné osoby podľa prílohy č. 1 tejto zmluvy môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Pre oznamovanie novej kontaktnej osoby sa primerane použijú ustanovenia tejto zmluvy o doručovaní (článok X. bod 9., 10. a 11.).

Článok X.

SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje 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.
2. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto zmluvy v súlade so sektorovými bezpečnostnými opatreniami, ktoré vydáva Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.
3. Dodávateľ sa zaväzuje 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 Prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernoscť, autentickosť a integrita.
4. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto zmluvy na zabezpečenom priestore tak, aby nebola narušená ich dôvernoscť, autentickosť a integrita.

5. Dodávateľ sa zaväzuje 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.
6. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy bezodkladne, pokiaľ to nie je v tejto zmluve alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
7. V prípade, ak Dodávateľ plní zmluvu prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby, Dodávateľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto zmluvy aj u týchto subdodávateľov.
8. 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 nevyklučuje 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 vrátane náhrady pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa základnej služby nahradiť tretej osobe nemajetkovú ujmu vyvolanú incidentom).
9. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej zmluvnej strane (ďalej len „písomnosti“) musia byť doručené, ak zmluva neustanovuje inak:
 - a) v písomnej forme prostredníctvom pošty doporučené s doručenkou; za deň doručenia sa považuje dátum prevzatia zásielky alebo
 - b) osobne do sídla druhej zmluvnej strany.
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.
11. Dodávateľ sa zaväzuje oznamovať všetky skutočnosti majúce vplyv na zmluvu, ako aj hlásiť ďalšie informácie požadované Prevádzkovateľom základnej služby, písomne na adresu sídla Prevádzkovateľa základnej služby.

12. V prípade porušenia povinnosti alebo záväzku Dodávateľa vyplývajúceho mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky, je Dodávateľ povinný Prevádzkovateľovi základnej služby zaplatiť zmluvnú pokutu vo výške 15 000,- EUR. Zaplatením zmluvnej pokuty Dodávateľom nie je dotknuté právo Prevádzkovateľa základnej služby na náhradu škody v vzniknutej v dôsledku porušenia povinnosti alebo záväzku Dodávateľa vyplývajúceho mu z tejto zmluvy.
13. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom základnej služby a Dodávateľom.
14. 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; tento záväzok trvá po dobu najmenej 5 rokov po ukončení tejto zmluvy. Ustanovenia o autorských právach (licenciách) k výsledkom služieb Dodávateľa, ktoré sú obsiahnuté v dodávateľskej zmluve, nie sú týmto dotknuté.

Článok XI.

AUDIT KYBERNETICKEJ BEZPEČNOSTI

1. Prevádzkovateľ základnej služby je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto zmluvy. Výdavky Prevádzkovateľa základnej služby spojené s vykonaním auditu znáša Prevádzkovateľ základnej služby.
2. Dodávateľ je povinný predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.
3. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
4. Prevádzkovateľ základnej služby môže 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.
5. Dodávateľ sa zaväzuje 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, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
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.

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. Preukázanie skutočností uvedených v predchádzajúcej vete môže Dodávateľ realizovať napr. prostredníctvom predloženia relevantných certifikátov, poučení, prezenčných listín a inej dokumentácie.
8. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej (10) desiat pracovných dní vopred svoj zámer realizovať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
10. Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku VIII. ods. 2, 3 a 4 tejto zmluvy sa uplatňujú primerane.
11. 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 sa zaväzuje 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.

Článok XII. ZÁVEREČNÉ USTANOVENIA

1. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania dodávateľskej zmluvy alebo iného jej ukončenia.
2. Každá zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade uvedenom vo všeobecne záväznom právnom predpise alebo tejto zmluve.

3. Prevádzkovateľ základnej služby je oprávnený od tejto zmluvy písomne 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;
- c) ak je Dodávateľ v likvidácii.

Odstúpenie od tejto zmluvy je platné a účinné dňom preukázateľného doručenia písomného odstúpenia od tejto zmluvy Dodávateľovi.

4. Za podstatné porušenie zmluvy sa považuje:

- a) porušenie povinností dodávateľom uvedených v čl. IV ods. 1, 7, čl. VI. ods. 3, 4, čl. VII a čl. VIII tejto zmluvy;
- b) konanie Dodávateľa, ktorý už v čase uzavretia zmluvy vedel alebo v tomto čase mohol predvídať s prihliadnutím na účel zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola zmluva uzavretá, že nedodrží, poruší a/alebo nebude plniť zmluvnú povinnosť dojednanú touto zmluvou a to bez ohľadu na to, či ide o zmluvnú povinnosť uvedenú v predchádzajúcom písm. a) a je zrejmé, že Prevádzkovateľ základnej služby by nemal záujem uzatvoriť túto zmluvu pri takom porušení zmluvy;
- c) Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto zmluvy.

5. Túto zmluvu je možné vypovedať Prevádzkovateľom základnej služby písomnou výpoveďou, aj bez uvedenia dôvodu s výpovednou dobou 1 mesiac, ktorá začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená Dodávateľovi.

6. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán. V tomto prípade zmluva zaniká ku dňu, ktorý bude v tejto dohode určený ako deň zániku zmluvy. Ak takýto deň určený nie je, táto zmluva zaniká ku dňu nadobudnutia účinnosti takejto dohody.

7. 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.

8. Táto zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.

9. Prípadné spory vyplývajúce z tejto zmluvy budú riešené predovšetkým mimosúdne. Podpisom tejto zmluvy zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto zmluvy sú príslušné súdy Slovenskej republiky.

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

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. 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.
13. 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 alebo písomných dojednaní a dohôd.
14. Táto zmluva bola vyhotovená v šiestich rovnopisoch, a to v štyroch rovnopisoch pre Prevádzkovateľa základnej služby a vo dvoch rovnopisoch pre Dodávateľa.
15. Zmluvné strany berú na vedomie, že Prevádzkovateľ základnej služby je v zmysle § 2 ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov povinnou osobou, a preto je táto zmluva v zmysle § 5a tohto zákona v spojení s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov povinne zverejňovanou zmluvou.
16. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR, nie však skôr ako dňom nadobudnutia účinnosti dodávateľskej zmluvy.
17. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
 - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa
 - Príloha č. 2 - Bezpečnostné opatrenia v organizácii Prevádzkovateľa základnej služby, ktoré sa vzťahujú na Dodávateľa,
 - Príloha č. 3 – Zoznam subdodávateľov
18. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná vôľnosť 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.

V Bratislave dňa ____.

V

dňa ____.

Prevádzkovateľ základnej služby:

Dodávateľ:

**Kancelária Národnej
rady SR**

(obchodné meno)
(štatutár)
(funkcia)

Príloha 1: Zoznam pracovných rolí a kontaktov prevádzkovateľa základnej služby a dodávateľa
- VZOR

Prevádzkovateľ základnej služby:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email
	MIB	Riadenie informačnej bezpečnosti		
	Riaditeľ OIaKT	Riadenie procesov		
	Vedúci oddelenia OISPESaBIKT	Zodpovednosť sa chod projektu / implementáciu projektu		

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email
	DB administrátor	Správa DB systému		
	NET administrátor	Administrácia časti siete, konfigurácia sieťových prvkov		
	Security operátor	Správa a konfigurácia bezpečnostných prvkov		

		(firewall, VPN koncentrátor)		
	Helpdesk operátor	Riešenie problémov používateľov PC, problémov s funkčnosťou aplikácie		

Príloha č. 2:

Bezpečnostné opatrenia v organizácii Prevádzkovateľa základnej služby, ktoré sa vzťahujú na Dodávateľa:

Príloha č. 3:

Zoznam subdodávateľov: