KNR-ODPR-2441/2024-1 285/2024

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:	00151 491
Zastúpený:	Ing. Daniel Guspan, vedúci Kancelárie NR SR

(ďalej len „prevádzkovateľ základnej služby“)

a

Dodávateľ:	ForesServices, s. r. o.
Sídlo:	Prievozská 14, 821 09 Bratislava
IČO:	35692103
IČ DPH:	SK2020309863
V mene ktorého koná:	Peter Dzurjanin, konateľ spoločnosti
Zapísaný:	v OR OS Bratislava I, oddiel: Sro, vložka číslo: 11155/B

(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 informačných systémov pre prevádzkovateľa základnej služby.
2. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na Servisnú zmluvu č. 284/2024 (ďalej len „servisná zmluva“), na základe ktorej dodávateľ bude poskytovať prevádzkovateľovi základnej služby výkon činností, ktoré priamo súvisia s prevádzkou informačných systémov prevádzkovateľa základnej služby.
3. Plnenie povinností s čiastočným prihliadnutím na zákon o kybernetickej bezpečnosti a podľa tejto zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania servisnej 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 servisnej 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 servisnej zmluvy,
      - 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 základnej služby alebo k zníženiu kvality poskytovanej služby prevádzkovateľa základnej služby.

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 zmluvy,

o) digitálnou službou služba, ktorej druh je uvedený v 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 bezpečnostných 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

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 servisnú zmluvu, a to s cieľom čiastočne zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou informačných systémov prevádzkovateľa základnej služby, s ktorými priamo súvisí výkon činností dodávateľa na základe servisnej zmluvy, počas ich životného cyklu, čiastočne predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť prevádzkovateľa základnej služby, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania informačných systémov prevádzkovateľa základnej služby.

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. Bezpečnostné opatrenia v organizácii prevádzkovateľa základnej služby, ktoré sa vzťahujú na dodávateľa, sú nasledovné:
   - Dodávateľ sa zaväzuje sledovať informácie o bezpečnostných chybách od dodávateľov komponentov používaných v dodávaných riešeniach. V prípade výskytu zraniteľnosti dodávateľ vyhodnotí riziko v rámci dodávaných riešení, notifikuje prevádzkovateľa základnej služby a dohodnú sa na postupe odstránenia prípadnej zraniteľnosti dodávaného riešenia.
   - Dodávateľ sa zaväzuje zabezpečiť nastavenie výmeny dát medzi internými databázami a databázami v DMZ, aby nemohlo dôjsť k neželanému úniku dát.

- Dodávateľ sa zaväzuje nepoužívať produkčné dáta pri vývoji a údržbe riešenia mimo prostredia prevádzkovateľa základnej služby. V prípade nutnosti testovať mimo prostredia prevádzkovateľa základnej služby musia byť dáta anonymizované.
- Dodávateľ sa zaväzuje zabezpečiť ochranu prístupových údajov a prístupových prostriedkov do prostredia prevádzkovateľa základnej služby, aby nemohli byť použité neautorizovanými osobami.
- Dodávateľ sa zaväzuje využívať komunikačné nástroje a protokoly stanovené prevádzkovateľom základnej služby pre reportovanie incidentov, výmenu údajov a riešenie zmenových konaní.

2. Dodávateľ nie je povinný riadiť sa ustanoveniami prílohy č. 2 tejto zmluvy, ktoré nie sú uvedené v rámci zodpovedností dodávateľa v bode 1 tohto článku zmluvy.
3. Dodávateľ berie na vedomie, 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 potenciálne 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, len pokiaľ pôjde o drobné zmeny a doplnky. V opačnom prípade dodávateľ vypracuje návrh na adekvátnu úpravu ceny služieb poskytovaných v rámci servisnej zmluvy a zašle ho prevádzkovateľovi na vyjadrenie.
4. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam pracovných rolí a kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto zmluvy.
5. 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
6. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania servisnej zmluvy.
7. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí dodávateľa.
8. Ostatný konkrétny rozsah činnosti dodávateľa je stanovený servisnou zmluvou.

Článok V.
BEZPEČNOSTNÉ OPATRENIA

Dodávateľ vyhlasuje, že má zavedené a implementované bezpečnostné opatrenia minimálne v rozsahu:

- personálnej bezpečnosti,
- riadenia prístupov,
- 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,
- kontinuity prevádzky.

Článok VI.
PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálne 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) vytvárať a zvyšovať bezpečnostné povedomie svojich pracovníkov, ktorí sa budú podieľať na plnení servisnej zmluvy a tejto zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby,
   b) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
   c) sledovať hrozby dotýkajúce sa dodávateľa, ktoré by mohli mať potenciálne nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,
   d) predchádzať vzniku incidentov,
   e) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
   f) prijímať od prevádzkovateľa základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálne nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,
   g) zasielať prevádzkovateľovi základnej služby včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak a
   h) 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 zaväzuje sa 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, roly a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto zmluvy.
3. Zoznam pracovných rolí a kontaktov dodávateľa, ktorí sa budú podieľať na plnení servisnej 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.

Článok VII.
POSTUP PRI RIEŠENÍ INCIDENTOV

1. Dodávateľ sa zaväzuje 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“), a to ako na výzvu prevádzkovateľa základnej služby, tak aj bez jeho výzvy, ak sa o incidente dozvie.
2. 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.

3. 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.
4. 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 servisnej 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 zmluvy trvá aj po skončení tejto zmluvy.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku zmluvy upravuje zákon o kybernetickej bezpečnosti.
4. Dodávateľ sa zaväzuje zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho pracovníci, subdodávatelia a ich pracovníci, a to aj po zániku ich pracovnoprávneho vzťahu, obchodného vzťahu alebo iného vzťahu.
5. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť prevádzkovateľovi základnej služby 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 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. Citlivé informácie (chránené resp. prísne chránené) šifrovaným prenosom SSL (TLS v aktuálne všeobecne akceptovanej bezpečnej verzii), ssh v aktuálne všeobecne akceptovanej bezpečnej verzii, zabezpečenie šifrovaním (PGP email)
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 ods. 9, 10 a 11).

Článok X.
SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy s čiastočným prihliadnutím na zákon o kybernetickej bezpečnosti a jeho vykonávacie predpisy 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 sa zaväzuje 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.
3. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy bezodkladne, pokiaľ to nie je v tejto zmluve alebo v požiadavkách platnej legislatívy SR a EÚ stanovené inak.
4. V prípade, ak dodávateľ plní túto zmluvu prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby alebo toto plnenie priamo súvisí s prevádzkou 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.
5. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej zmluvnej strane (ďalej len „písomnosti“) musia byť doručené, ak táto zmluva neustanovuje inak:
   a) v písomnej forme prostredníctvom pošty doporučene s doručenkou; za deň doručenia sa považuje dátum prevzatia zásielky alebo
   b) osobne do sídla druhej zmluvnej strany.
6. 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.
7. Dodávateľ sa zaväzuje oznamovať všetky skutočnosti majúce vplyv na túto zmluvu, ako aj hlásiť ďalšie informácie požadované prevádzkovateľom základnej služby písomne na adresu sídla prevádzkovateľa základnej služby.
8. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa servisnej zmluvy alebo iných zmlúv uzatvorených medzi prevádzkovateľom základnej služby a dodávateľom.

Článok XI.
ZÁVEREČNÉ USTANOVENIA

1. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania servisnej 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 v 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 tejto zmluvy sa považuje:
   a) porušenie povinností dodávateľom uvedených v článku IV ods. 1 a 5, v článku VI ods. 3, v článku VII a v článku VIII tejto zmluvy,
   b) konanie dodávateľa, ktorý už v čase uzavretia tejto zmluvy vedel alebo v tom čase mohol predvídať s prihliadnutím na účel tejto zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola táto 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 každou zo zmluvných strán 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 druhej zmluvnej strane.
6. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán. V tomto prípade táto zmluva zaniká ku dňu, ktorý bude v tejto dohode určený ako deň zániku tejto zmluvy. Ak takýto deň určený nie je, táto zmluva zaniká ku dňu nadobudnutia účinnosti takejto dohody.
7. Ukončenie tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po ukončení tejto zmluvy, a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy.
8. Táto zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia na kolízne normy. 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 z tejto 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 ustanovenie 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 neplatné alebo nevymáhateľné 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 v 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 servisnej 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,
    - Príloha č. 3 – Zoznam subdodávateľov.
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 tejto 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 .....

Prevádzkovateľ základnej služby:

.....
Ing. Daniel Guspan
vedúci
Kancelárie Národnej rady
Slovenskej republiky

V Bratislava dňa .....

Dodávateľ:

.....
Peter Dzurjanin
konateľ spoločnosti
ForesServices, s.r.o.

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		
	Vedúci oddelenia projektového manažmentu a procesov	Riadenie procesov		
	Referent oddelenia OISPESaBIKT	Zodpovednosť sa chod projektu / implementáciu projektu		

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email
	CEO	Riadenie procesov		
	Development team lead	Zodpovednosť za implementáciu projektu		
	Data security officier	Informačná bezpečnosť a manažment bezpečnostných incidentov		
	Support team lead	Zodpovednosť za podporu chodu aplikácie a nastavenie procesov zákazníckej podpory		

Príloha č. 2 Bezpečnostné opatrenia v organizácii prevádzkovateľa základnej služby

Úvodné ustanovenia

„Bezpečnostná politika kybernetickej bezpečnosti“ rozpracováva strategické smerovanie riešenia kybernetickej bezpečnosti a stanovuje rámec systému riadenia bezpečnosti pre informačné a komunikačné systémy **Kancelárie Národnej rady Slovenskej republiky** so sídlom Námestie Alexandra Dubčeka 1, 812 80 Bratislava 1 (ďalej ako „Kancelária NR SR “).

Jednou z požiadaviek na aplikovanie bezpečnostných opatrení podľa Zákona č. 95/2019 o Vyhlášky č. 179/2020 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy a Zákona č. 69/2018 o kybernetickej bezpečnosti (ďalej len „zákon o KB a Vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení je vytvorenie požiadaviek na aplikovanie bezpečnostných opatrení pre tretie strany.

Vymedzenie Základných pojmov

1) Na účely tejto prílohy sa rozumie:
   a) **aktívum** – všetko, čo má pre Kanceláriu NR SR hodnotu (hardvérové komponenty, softvér, dáta, služby, ľudské zdroje, dobré meno Kancelárie NR SR a pod.),
   b) **analýza rizík** – proces identifikácie bezpečnostných rizík, určenie ich rozsahu a identifikácie oblastí, pre ktoré sú potrebné bezpečnostné opatrenia,
   c) **bezpečnostný incident** – udalosť, ktorej dôsledkom je narušenie bezpečnosti aktíva alebo porušenie bezpečnostnej politiky Kancelárie NR SR,
   d) **bezpečnostné opatrenie** – činnosť, zariadenie, procedúra alebo mechanizmus, ktorý eliminuje alebo minimalizuje možnosti vzniku, pôsobenia a následky bezpečnostného incidentu, hrozby alebo udalosti,
   e) **Bezpečnostná politika** – základný dokument systémového riešenia ochrany všetkých aktív spoločnosti pred možnými hrozbami a rizikami. Bezpečnostnou politikou sa vymedzujú bezpečnostné ciele, bezpečnostné požiadavky a zásady, základné organizačné opatrenia a zodpovednosť za jednotlivé bezpečnostné oblasti,
   f) **dostupnosť** – požiadavka, aby aktívum bolo na požiadavku oprávneného zamestnanca prístupné a schopné použitia,
   g) **dôvernosť** – umožnenie prístupu k IS a ním spracúvaným elektronickým informáciám iba pre určené subjekty,
   h) **Garant informačnej a kybernetickej bezpečnosti** (ďalej len „garant bezpečnosti“ alebo „garant informačnej bezpečnosti))– subjekt zodpovedný za presadzovanie, kontrolu a dodržiavanie celkovej bezpečnosti v Kancelárii NR SR, garant informačnej a kybernetickej bezpečnosti je zároveň manažérom kybernetickej bezpečnosti podľa Zákona o kybernetickej bezpečnosti a Vyhlášky š. 362/2018 §5 písm. a)

i) **Gestor IS** – organizačný útvar, ktorý predkladá požiadavku na verejné obstarávanie za účelom zabezpečenia svojich potrieb; ak je potrebný pre zabezpečenie činností viacerých organizačných útvarom, Gestorom je organizačný útvar, ktorý má najväčší finančný podiel na zákazke,

j) **incident** – akákoľvek udalosť, ktorá nie je súčasťou bežnej prevádzky IS/IKT služby a ktorá spôsobuje, prípadne môže spôsobiť prerušenie alebo pokles v kvalite danej služby,

k) **informačno-komunikačné technológie** (IKT) – integrovaný súbor technológií, používaných na manažovanie informácií, procesov a komunikácie v elektronickej podobe za účelom dosiahnutia účinných a efektívnych výsledkov optimalizovaním manažmentu zdrojov distribúcie informácií a vedomostí; ide napríklad o softvér, hardvér a metódy určené pre zber, spracovanie, prenos a úschovu informácií v dátovej (elektronickej) forme,

l) **informačná bezpečnosť** – súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných aktív,

m) **informačné aktívum** – aktívum v informačnom prostredí Kancelárie NR SR (znalosti a dáta/informácie, ktoré majú pre Kanceláriu NR SR hodnotu),

n) **integrita** – vlastnosť ochrany správnosti a úplnosti aktíva,

o) **informačný systém (IS)** – funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických a programových prostriedkov, ktoré sú súčasťou informačného systému; ide o súhrn prvkov hardvéru, softvéru, komunikačných a ďalších technológií, používaných pre záznam, uchovanie, prenos a využívanie informácií a dát,

p) **ISO** – International Standard Organization (medzinárodná štandardizačná organizácia),

q) **klasifikované informácie** – informácie, pri ktorých porušenie informačnej bezpečnosti predstavuje neakceptovateľné riziko pre organizáciu,

r) **kontinuita činností** – zabraňuje prerušeniam prevádzkových aktivít a chráni kritické procesy organizácie pred vplyvmi závažných zlyhaní alebo havárií informačných systémov a zabezpečuje ich včasnú obnovu,

s) **kybernetický bezpečnostný incident** - 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.

t) **médiá** – nosiče informácií listinného charakteru (papierové dokumenty, tlačové zostavy, systémová dokumentácia a pod.) a nelistinného charakteru (CD, DVD, USB disk, magnetická páska, disketa, vymeniteľný disk a pod.),

u) **ošetrenie rizík** – proces na úpravu rizík,
v) **riadenie rizík** – koordinované aktivity na riadenie organizácie s ohľadom na riziká,
w) **riešiteľ bezpečnostného incidentu** - poverený zamestnanec ktorý je oprávnený riešiť bezpečnostný incident, spravidla garant informačnej bezpečnosti alebo osoba poverená jeho zastupovaním (kapitola 8, odsek č. 3., 7., 9., 10., 11.)
x) **riziko** – miera ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
y) **zamestnanec** – je osoba, ktorá vykonáva prácu v prospech Kancelárie NR SR na základe pracovnoprávneho vzťahu.

Bezpečnosť prevádzky

1) Cieľom tejto oblasti je zabezpečenie správnej a bezpečnej prevádzky IS, predchádzanie narušeniu bezpečnosti pri práci s pamäťovými médiami, predchádzanie strate, modifikácii alebo zneužitiu informácií pri ich výmene s okolím Kancelárie NR SR. Ide o nasledovné oblasti:
   a) dokumentácia prevádzkových postupov,
   b) bezpečnosť prenositeľných médií,
   c) riadenie zmien,
   d) riadenie konfigurácií,
   e) riadenie kapacít,
   f) ochrana pred škodlivým softvérom,
   g) zálohovanie a archivácia,
   h) zaznamenávanie dát a monitorovanie,
   i) riadenie prevádzkového softvéru,
   j) riadenie technickej zraniteľnosti.
2) Na zaistenie správneho využívania bezpečnostných mechanizmov sa musí spôsob ich použitia zdokumentovať. Dokumentácia o kritických informačných systémoch Kancelárie NR SR obsahuje:
   a) Používateľskú dokumentáciu,
   b) Administrátorskú dokumentáciu,
   c) Prevádzkovú dokumentáciu.
3) Prevádzkové postupy a dokumentované postupy pre správu systémov sú spracované ako oficiálne dokumenty a ich zmeny autorizuje manažment.
4) Používanie prenosných médií musí byť formálne upravené a je povolené iba pre určené spôsoby použitia.

5) Pri zasielaní údajov mimo Kancelárie NR SR sa musia zohľadniť požiadavky aplikovateľnej legislatívy[1].
6) Zmeny informačných systémov musia byť riadené. Taktiež musí byť zavedený formálny postup schvaľovanie navrhovaných zmien.
7) Pri zmenách v prevádzkovom prostredí nesmie byť podstatným spôsobom narušená prevádzka ani znížená bezpečnosť.
8) Zmeny musia byť testované a musia byť zhodnotené vplyvy takýchto zmien na bezpečnosť IS.
9) Musia byť dostupné návratové a havarijné postupy vrátane postupov a zodpovedností za prerušenie, alebo predčasné ukončenie a obnovu z neúspešnej zmeny a nepredpokladaných udalostí.
10) Použitie prostriedkov musí byť monitorované a musia sa vykonávať odhady budúcich požiadaviek na kapacity, z dôvodu zabezpečenia dosiahnutia požadovanej výkonnosti systému.
11) Ochrana informačných systémov Kancelárie NR SR pred škodlivým softvérom je v rozsahu najmenej:
    a) kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
    b) detekcie prítomnosti škodlivého kódu na všetkých zariadeniach informačných systémov Kancelárie NR SR (pracovné stanice, notebooky, externé nosiče a pod.),
    c) kontroly súborov prijímaných zo siete Internet a odosielaných do tejto siete na prítomnosť škodlivého softvéru,
    d) detekcie prítomnosti škodlivého kódu na webových stránkach.
12) Pravidelne sa vytvárajú a testujú záložné kópie dôležitých informácií a softvéru.
13) Pre médiá obsahujúce záložné kópie sa musí zaistiť rovnaký stupeň bezpečnosti, ako je požadovaný pre údaje, ktoré sú na nich uložené. Tieto médiá sa musia zároveň uchovávať mimo priestorov s centrálnymi komponentmi IS tak, aby sa minimalizovalo riziko súčasného poškodenia originálnych aj záložných údajov.
14) Testovanie obnovy informačných systémov Kancelárie NR SR a údajov z prevádzkovej zálohy sa vykonáva najmenej 1x za rok. Testujú sa aj redundantné zapojenia zariadení.
15) Ako prevencia pred zlyhaním IS sa musí využívať monitorovanie v týchto oblastiach:
    a) záťaž kľúčových komponentov IS a komunikačnej infraštruktúry,
    b) kapacitné rezervy kľúčových komponentov IS (napr. voľné miesto na systémovom disku),
    c) výskyt chýb v IS.

[1] Napr. v súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov - ďalej v texte len „Nariadenie“) a so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, Výnosom MF SR č.55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov a pod.

16) Záznamy udalostí zaznamenávajúce aktivity používateľov, výnimky a udalosti informačnej bezpečnosti musia byť vytvárané, uchovávané a pravidelne preskúmavané.
17) Informácie obsiahnuté v záznamoch, ako aj prostriedky na ich tvorbu musia byť chránené pred neoprávnenými zásahmi a neautorizovaným prístupom.
18) Aktivity Správcu IS a operátora musia byť zaznamenávané. Záznamy musia byť chránené a pravidelne preskúmavané. Záznamy tretích strán musia byť ukladané na zariadeniach Kancelárie NR SR, ku ktorým musia mať umožnený prístup jej relevantní zamestnanci.
19) Hodiny na všetkých relevantných systémoch na spracúvanie informácií v rámci Kancelárie NR SR musia byť synchronizované prostredníctvom jediného presného časového zdroja.
20) Musia byť zavedené postupy na riadenie inštalovania softvéru na prevádzkových systémoch. Pre inštaláciu softvéru používateľmi musia byť vytvorené a zavedené prísne pravidlá.
21) Informácie o technickej zraniteľnosti využívaných informačných systémov musia byť zhromažďované a zhodnocovaná miera vystavenia sa zraniteľnosti. Následne sa musia zavádzať príslušné opatrenia na potlačenie týchto rizík.
22) Hodnotenie zraniteľností informačných systémov Kancelárie NR SR musí byť vykonávané s periodicitou najmenej raz ročne.
23) Používanie prenosných médií (napríklad USB diskov, USB kľúčov) na prenos informácií súvisiacich výhradne s plnením služobných alebo pracovných povinností je v kancelárii NR povolené.
24) Pri používaní prenosných médií musia používatelia zachovávať primerané bezpečnostné opatrenia, ktoré eliminujú riziko prezradenia, zneužitia alebo neautorizovaného prístupu k citlivým informáciám.
25) Bezpečnostnými opatreniami podľa odseku 24 sú najmä
    a) ochrana média pred stratou alebo krádežou jeho bezpečným skladovaním a prenášaním,
    b) externé prenosné médiá a informácie na nich uložené musia byť chránené šifrovaním s nastavením silného hesla minimálne desať alfanumerických znakov na otvorenie dokumentov, pričom pre šifrovanie sa používa asymetrické šifrovanie s minimálnou dĺžkou kľúča 2048kB,
    c) používanie prenosných médií iba na dôveryhodných počítačoch.
26) Za dodržiavanie bezpečnostných opatrení podľa odseku 25 ako aj za prípadné škody spôsobené zneužitím, prezradením, neautorizovaným prístupom k informáciám uloženým na prenosných médiách zodpovedá ich používateľ.
27) Všetky nepotrebné prenosné médiá vo vlastníctve úradu musia byť zlikvidované bezpečným spôsobom tak, aby nebolo možné z týchto médií extrahovať žiadne citlivé informácie.
28) Za likvidáciu nepotrebných médií podľa odseku 5 je zodpovedné oddelenie OIaKT.

29) Pri manipulácii a prenose informácií musia byť dodržané bezpečnostné opatrenia. Bezpečnostné opatrenia sú uplatňované najmä pri
    a) fyzickom prenose informácií (napríklad dokumentov),
    b) emailovej komunikácii vrátane zasielania príloh,
    c) elektronickom prenose,
    d) prenose, zobrazovaní informácií v informačnom systéme,
    e) používaní mobilných prostriedkov,
        a. telefonickej komunikácii, vrátane zasielania správ,
        b. faxovej komunikácii,
        c. zasielaní rýchlych správ (napríklad Instant Messaging, chat).
30) Pri výmene alebo prenose informácií medzi úradom a tretími stranami musí byť vykonaný odhad možných bezpečnostných rizík a určené bezpečnostné opatrenia na ochranu prenášaných informácií.
31) Správca informačného aktíva uzavrie s treťou stranou zmluvu o prenose informácií podľa požiadaviek Zákona o kybernetickej bezpečnosti, ktorá musí obsahovať aspoň ustanovenia o bezpečnostných opatreniach (technologických, procesných, personálnych), ktoré boli určené pre tento prenos ako aj zodpovednosť za ich dodržiavanie. Vlastník dotknutého informačného aktíva musí byť o uzavretí tejto zmluvy bezodkladne informovaný.

Bezpečnosť sieťovej komunikácie

1) Cieľom tejto oblasti bezpečnosti je predchádzať strate, neoprávnenej modifikácii alebo zneužitiu elektronických služieb a elektronických informácií v sieťach a v podporných zariadeniach, ktoré ich v sieti spracúvajú, ako aj ošetriť bezpečnosť prenášaných informácií v rámci organizácie a s ktoroukoľvek treťou stranou.
2) Vonkajšie aj vnútorné sieťové prostredie v Kancelárii NR SR je chránené prostredníctvom technologického riešenia na ochranu perimetra siete.
3) Na pripojenie zariadenia k bezdrôtovej sieti sa vzťahujú rovnaké bezpečnostné požiadavky ako na fyzické pripojenie zariadenia k zóne, ku ktorej je pripojená daná bezdrôtová sieť.
4) Auditné záznamy z aktívnych sieťových zariadení, príslušných serverov sa zaznamenávajú a ukladajú a zálohujú..
5) Kancelária NR SR vedie evidenciu o všetkých miestach prepojenia v sieti vrátane prepojení s externými sieťami.
6) Za účelom ochrany sieťovej infraštruktúry, prenášaných informácií a prepojených informačných systémov a služieb musia byť na úrade realizované bezpečnostné opatrenia.
7) Za realizáciu bezpečnostných opatrení sieťovej infraštruktúry úradu je zodpovedný odbor OIaKT.

8) Bezpečnostné opatrenia sú určené na základe posúdenia bezpečnostných rizík a to najmä ochrany:
    a) prenášaných informácií,
    b) uchovávaných informácií (napríklad dočasných súborov, obsahu uloženého do medzipamätí - cache),
    c) dizajnu sieťovej infraštruktúry,
    d) informácií o konfigurácii sietí, sieťových zariadení, definícií kontroly prístupu, oprávnení, správcovských hesiel a kryptografických kľúčov,
    e) sieťových ciest a trás,
    f) sieťových zdrojov (napríklad šírky pásma),
    g) hranice a obvodu siete,
    h) rozhrania informačného systému do sietí.
9) Konfigurácia sieťových zariadení musí byť zdokumentovaná. Zmeny konfigurácie sieťových zariadení, definícií kontroly prístupu, smerovania a prihlasovacích údajov musia byť zdokumentované a kontrolované.
10) Na sieťových zariadeniach musia byť použité aspoň tieto bezpečnostné opatrenia:
    a. všetky prístupy a konfiguračné zmeny sieťových zariadení musia byť logované,
    b. pre prístup musí byť použitý zabezpečený (šifrovaný) kanál, prípadne viacfaktorová autentifikácia,
    c. konfigurácie zariadení musia byť zálohované bezpečným spôsobom.
11) Ak sú na základe klasifikácie informačných aktív prenášané interné alebo chránené informácie, alebo na základe posúdenia rizík iné citlivé údaje je nutné použiť šifrovanie dát, správ, alebo trasy prenosu (SSH, SSL, TLS, VPN tunel a iné).
12) Pri používaní lokálnych bezdrôtových sietí (Wi-Fi sieť) musia byť použité aspoň tieto bezpečnostné opatrenia:
    a. silné šifrovanie minimálne WPA2, WPA3 alebo v poslednej aktuálnej verzii,
    b. silné heslo pre pripojenie (minimálne desať znakov),
    c. autentifikácia používateľov,
    d. pri spojení siete s lokálnou sieťou je nevyhnutné použiť zabezpečenie certifikátmi.
13) Ak sa poskytuje bezdrôtová sieť (Wi-Fi) externým subjektom (napríklad konferencie, návštevy), musí byť bezdrôtová sieť oddelená od lokálnej počítačovej siete, a to na úrovni fyzickej alebo logickej, s výnimkou kritických IS KNR SR a IS ktoré sú základnou službou v kategórii III, pričom tieto musia byť výlučne oddelené na fyzickej úrovni.
14) Na sieťových zariadeniach musí byť nastavené logovanie a monitorovanie všetkých dôležitých udalostí a to najmä
    a. sieťovej komunikácie odchádzajúcej mimo infraštruktúru úradu,

b. internej sieťovej komunikácie týkajúcej sa citlivých informácií a informačných systémov,
c. bezpečnostných incidentov na sieťových zariadeniach ako napríklad prihlásenie a zmena konfigurácie,
d. bezpečnostných udalostí na systémoch poskytujúcich autentifikačné a autorizačné služby v sieťovej infraštruktúre.

15) Aktivity v informačných systémoch a počítačových sieťach úradu musia byť za účelom odhalenia možného bezpečnostného incidentu monitorované, analyzované a vyhodnocované prostredníctvom ďalších bezpečnostných zariadení (NIDS – Network Intrusion Detection System, SIEM – Security Information and Event Management).
16) Za monitorovanie sieťovej infraštruktúry je zodpovedný odbor OIaKT.

Nákup, vývoj a údržba IS

1) Za účelom redukcie rizika neakceptovateľného výkonu, alebo zlyhania informačných systémov je potrebné monitorovať kapacitu jednotlivých informačných systémov, zisťovať súlad s požiadavkami na ich výkon, ich kapacitné limity a na tomto základe plánovať a optimalizovať kapacity v dostatočnom predstihu. Za plánovanie, monitorovanie a optimalizáciu kapacít je zodpovedný OIaKT.
2) Cieľom tejto oblasti bezpečnosti je zabezpečiť integráciu informačnej bezpečnosti do informačných systémov v celom ich životnom cykle a zaistiť, aby IT projekty prebiehali riadeným a bezpečným spôsobom.
3) Riešenie informačnej bezpečnosti Kancelárie NR SR je súčasťou celého životného cyklu IS počínajúc jeho obstarávaním.
4) Pre každý IT projekt, ktorý má byť prevádzkovaný v prostredí Kancelárie NR SR sú identifikované a špecifikované bezpečnostné požiadavky, ktoré sa stávajú súčasťou zadávacej dokumentácie k výberovému konaniu a následne sú premietnuté do zmluvy s dodávateľom.
5) V každom IT projekte je na strane dodávateľa aj na strane Kancelárie NR SR zriadená a obsadená rola zodpovedná za informačnú bezpečnosť. Na strane Kancelárie NR SR za informačnú bezpečnosť zodpovedá Garant bezpečnosti. Táto rola zabezpečuje (v rozsahu svojej pôsobnosti na strane Kancelárie NR SR a na strane dodávateľa):
   a) zohľadnenie právnych predpisov a technologických požiadaviek na bezpečnosť,
   b) integráciu bezpečnostných požiadaviek do IT projektu,
   c) vykonanie analýzy rizík,
   d) špecifikovanie bezpečnostných opatrení a dohľad nad ich implementáciou.
6) Súčasťou každého IT projektu je nevyhnutná analýza rizík a návrh opatrení na ich minimalizáciu, spracovaná vo forme bezpečnostného projektu alebo inej forme

bezpečnostnej dokumentácie zohľadňujúcej legislatívu aplikovateľnú na predmetný IS, jeho vývoj a údržbu.

7) Pred vývojom a implementáciou nových IS ovplyvňujúcich existujúce IS v prostredí Kancelárie NR SR musí byť ako súčasť analýzy rizík vykonaná aj analýza dopadov zmien na už prevádzkované IS a ich služby. V prípade identifikácie nepokrytých rizík musia byť navrhnuté a implementované dodatočné bezpečnostné opatrenia.
8) Súčasťou každého IT projektu je vytvorený návrh formy výkonu a rozsahu bezpečnostných testov.
9) V každom IT projekte sú určené a obsadené roly na strane Kancelárie NR SR, ktoré budú vykonávať správu a údržbu predmetu IT projektu po jeho zavedení do rutinnej prevádzky. Pokiaľ bude správu a údržbu vykonávať tretia strana, tak na strane Kancelárie NR SR je zriadená a obsadená rola vykonávajúca dohľad.
10) Pre každý nový informačný systém, alebo službu musia byť v návrhu a dokumentácii určené a dohodnuté kritériá pre jeho akceptáciu. Nový informačný systém musí byť testovaný podľa dohodnutých akceptačných kritérií skôr ako bude prijatý do prevádzky.
11) Súčasťou akceptačných kritérií musí byť aj preverenie implementácie dohodnutých bezpečnostných zásad a opatrení.
12) Pri definícií týchto rolí a ich následnom personálnom obsadzovaní musia byť určené a zohľadnené požiadavky na ich nezlučiteľnosť (nemožnosť kumulácie rolí v jednej osobe) a vzájomnú zastupiteľnosť.
13) Na zaistenie primeranej úrovne bezpečnosti je žiadúce v každom IT projekte vývojové a testovacie prostredie oddelené od produkčného prostredia, a v prípade kritických IS KNR SR a IS ktoré sú základnou službou v kategórii III je oddelenie prostredí nevyhnutné.
14) Pri testovaní vyvíjaných komponentov sa štandardne nesmú použiť údaje z produkčného prostredia. Ak pre testovacie prostredie budú vytvorené analogické bezpečnostné opatrenia ako pre produkčné prostredie a charakter testov to vyžaduje, je akceptovateľné ich dočasné použitie iba pre výkon testov .
15) Pokiaľ výkon testov vyžaduje použitie osobných údajov, musia byť pred použitím anonymizované.
16) Ku každého IT projektu prevádzkovanému v prostredí Kancelárie NR SR musí jeho dodávateľ zabezpečiť vypracovanie a dodanie príslušnej projektovej dokumentácie pred zavedením IS do produkčnej prevádzky – používateľskej, administrátorskej a prevádzkovej dokumentácie k IS.
17) Používateľská dokumentácia je manuál na ovládanie IS používateľmi a existuje v takom rozsahu, aby používateľ vedel použiť všetky ponúkané funkcie, vrátane správneho použitia bezpečnostných mechanizmov.
18) Administrátorská dokumentácia je návod na správu a prevádzku IS.
19) Obsahom prevádzkovej dokumentácie je najmä popis architektúry, konfigurácií, integračných väzieb a rozhraní.

20) Všetky zmeny sú formálne riadené, schvaľované a zohľadňujú bezpečnostné požiadavky. Pre výkon zmien v IS sú stanovené pravidlá zabezpečujúce trvalé udržanie úrovne bezpečnosti IS.
21) Zamestnanci Kancelárie NR SR a pracovníci dodávateľov môžu zasahovať do konfigurácie prevádzkovaných IS iba v rozsahu svojej pôsobnosti, na základe plnenia pracovnej úlohy resp. v súlade s ustanoveniami zmluvy/SLA. Všetky vykonané zmeny sú vopred komunikované s vlastníkom aj správcom dotknutého informačného aktíva/aktív a zdokumentované a schvaľované. Proces schvaľovania je definovaný v Smernici o riadení zmien.

Bezpečnosť v spolupráci s tretími stranami

1) Pred začatím spolupráce a umožnením prístupu dodávateľov k aktívam Kancelárie NR SR musia byť vždy identifikované bezpečnostné požiadavky na túto spoluprácu a navrhnuté opatrenia minimalizujúce riziká vyplývajúce z tejto spolupráce. Tretia strana musí byť pred začatím spolupráce poučená o týchto požiadavkách, ktoré sú na ňu kladené zo strany Kancelárie NR SR, vrátane spôsobov identifikácie, nahlasovania a zvládania bezpečnostných incidentov.
2) Tretia strana, ktorá bude mať prístup k aktívam Kancelárie NR SR, bude pre Kanceláriu NR SR dodávať alebo poskytovať IT infraštruktúru, jej komponenty alebo súvisiace služby, musí mať s Kanceláriou NR SR uzatvorenú zmluvu alebo musí mať vzťah s Kanceláriou NR SR upravený iným relevantným právnym spôsobom, v závislosti od typu tretej strany a charakteru spolupráce.
3) Zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s tretími stranami, servisnými a outsourcingovými partnermi sú explicitne vymedzené.
4) Tretia strana počas umožnenia prístupu k IS Kancelárie NR SR alebo údajom z IS Kancelárie NR SR, rešpektuje aplikovateľné ustanovenia bezpečnostnej politiky, interných dokumentov Kancelárie NR SR a relevantnej legislatívy.
5) Ak sa prevádzka časti IS alebo starostlivosť o niektoré aktíva IS prenáša na zmluvnú tretiu stranu (outsourcing), táto tretia strana má v zmluve vymedzenú zodpovednosť za ochranu aktív dotknutých outsourcingom. Tretia strana zabezpečuje výkon všetkých relevantných činností vyplývajúcich z bezpečnostnej politiky a súvisiacich predpisov.
6) V závislosti od charakteru služieb dodávaných treťou stranou sú zo strany Kancelárie NR SR priebežne monitorované a vyhodnocované s nimi súvisiace činnosti a parametre, najmä:
   a) využívanie vzdialených prístupov do siete Kancelárie NR SR,
   b) aktuálnosť prístupových oprávnení zamestnancov tretích strán,
   c) činnosti vykonávané na infraštruktúre a v aplikačnom vybavení,
   d) úroveň dodržiavania SLA parametrov dodávaných služieb.

7) Zodpovednosť za riadenie vzťahu s treťou stranou je na strane Kancelárie NR SR priradená konkrétnemu zamestnancovi alebo organizačnému útvaru.
8) Zástupcovia zodpovedného organizačného útvaru sú pri uzatváraní zmluvy s treťou stranou na dodávku informačného systému, alebo služby povinní do zmluvy zabezpečiť zapracovanie povinnosti dodržiavať túto prílohu a ďalšie interné predpisy týkajúce sa informačnej bezpečnosti, ako aj záväzky vyplývajúce z práv ochrany duševného vlastníctva pre všetkých zamestnancov tretej strany, ktorí budú pracovať s informačnými aktívami kancelárie NR.
9) Pred poskytnutím akýchkoľvek informácií týkajúcich sa informačného systému kancelárie NR vrátane žiadosti o návrh riešenia musí byť s treťou stranou uzavretá dohoda o mlčanlivosti, ak nejde o výkon auditu podľa všeobecne záväzných právnych predpisov.
10) Bez dohody o mlčanlivosti nesmú byť poskytnuté tretej strane žiadne informácie týkajúce sa informačného systému úradu, požadovaných riešení, alebo služieb. Výnimku tvoria všeobecne známe skutočnosti a informácie, ktoré nie sú predmetom mlčanlivosti.
11) Pri nákupe informačného systému, alebo dodávke informačného systému a služieb od tretích strán musia byť bezpečnostné požiadavky a opatrenia určené v príslušnej dokumentácii už pri špecifikovaní technických požiadaviek.
12) Informačné systémy a služby dodávané tretími stranami musia spĺňať všetky zásady a opatrenia ustanovené internými predpismi úradu pre oblasť informačnej bezpečnosti.
13) Zamestnanci tretej strany, ktorý pracujú s informačnými aktívami kancelárie NR musia byť rovnako preukázateľne oboznámení s platnými bezpečnostnými zásadami a opatreniami. Záznam o tomto oboznámení zamestnancov musí byť súčasťou dokumentácie dodávaného informačného systému alebo služby.
14) Za oboznamovanie tretích strán a ich zamestnancov s internými predpismi týkajúcimi sa informačnej bezpečnosti je zodpovedný vlastník informačného aktíva. Spôsob a formu oboznámenia určí garant informačnej bezpečnosti.
15) Dodávateľ alebo tretia strana musí prehlásiť znalosť a schopnosť implementovať bezpečnostné zásady a opatrenia ustanovené v interných predpisoch a v dokumentácii navrhovaného diela.
16) Výnimku z bezpečnostných požiadaviek a opatrení môže v odôvodnených prípadoch na žiadosť zadávateľa udeliť garant informačnej bezpečnosti. V prípade rozporu o udelenie výnimky rozhoduje komisia pre riadenie informačnej bezpečnosti.
17) Výnimka z bezpečnostných požiadaviek a opatrení podľa článku 17 môže byť udelená výhradne na dobu pokiaľ trvajú dôvody, pre ktoré je požadovaná. Po uplynutí dôvodu musí byť výnimka bezodkladne zrušená.
18) Udelenie výnimky podľa odseku 17 musí mať písomnú formu a byť súčasťou dokumentácie dodávaného diela alebo služby a musí obsahovať najmä
    a. popis výnimky s odkazom na ustanovenie tejto prílohy,
    b. dôvod, prečo je výnimka udelená,

c. časové ohraničenie trvania výnimky,
d. osobu zodpovednú za zrušenie výnimky po uplynutí dôvodu, pre ktorý bola udelená.

19) Zachovávanie bezpečnostných opatrení v informačných systémoch a službách dodaných tretími stranami musí byť priebežne monitorované a kontrolované tretími stranami ako aj úradom. Prípadné nedostatky musí tretia strana odstrániť v čo najkratšej dobe.
20) Ak sa identifikujú nové bezpečnostné riziká pri dodávke informačného systému tretími stranami, musia byť určené bezpečnostné opatrenia na ich elimináciu.
21) Bezpečnostné opatrenia informačných systémov a služieb dodaných tretími stranami musia byť prehodnotené aj v prípade ich významnej zmeny. V prípade vzniku bezpečnostného rizika pri zmene informačného systému, alebo služby musia byť treťou stranou dodatočne implementované bezpečnostné opatrenia eliminujúce zistené riziká.
22) Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia musí byť určená v zmluve s treťou stranou. Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia na ochranu osobných údajov úradu spravovaných treťou stranou (tzv. sprostredkovateľ) musí byť určená v zmluve s treťou stranou v samostatnej kapitole.

Príloha č. 3

Zoznam subdodávateľov

Dodávateľ vyhlasuje, že v súvislosti s plnením predmetu tejto Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 285/2024 nevyužije tretie osoby ako subdodávateľov.

.....
Peter Dzurjanin
konateľ spoločnosti
ForesServices, s.r.o.