Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzavretá podľa
§ 269 ods. 2 Zákona č. 513/1991 Z. z. Obchodný zákonník (ďalej len ako „**OBZ**"),
§ 19 a nasl. Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len ako „**zákon o kybernetickej bezpečnosti**"),
§ 8 a nasl. Vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len ako „**Vyhláška**") a Smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len ako „**smernica NIS**")
Č. Z/BTS/DTPR/186/2022
(ďalej len ako „**zmluva**")

medzi zmluvnými stranami:

Obchodné meno:	**Letisko M.R.Stefánika - Airport Bratislava, a.s. (BTS)**
Sídlo:	Letisko M.R. Štefánika,P.O.BOX 160, 823 11 Bratislava II
Právna forma:	akciová spoločnosť
IČO:	35 884 916
IČ DPH:	SK2021812683
Zastúpený:	Ing. Dušan Keketi, predseda predstavenstva a generálny riaditeľ Ing. Otto Szöke, člen predstavenstva
Zapísaný:	v Obchodnom registri Okresného súdu Bratislava I, oddiel: Sa, vložka č. 3327/B

(ďalej len ako „**Prevádzkovateľ základnej služby**" alebo ako „**BTS**")

a

Obchodné meno:	**SLOVAKODATA, a.s.**
Sídlo:	Kutlikova 17, P.O.BOX 134, 850 00 Bratislava
Právna forma:	akciová spoločnosť
IČO:	31367763
IČ DPH:	SK2020344128
Zastúpený:	Ing. Peter Maťašek, predseda predstavenstva
Zapísaný:	v Obchodnom registri Okresného súdu Bratislava I, oddiel: Sa, vložka č. 617/B(ďalej len ako „**Dodávateľ**")

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

Článok I.
ÚVODNÉ USTANOVENIA

1.1 Prevádzkovateľ je na základe rozhodnutia Národného bezpečnostného úradu Slovenskej republiky číslo 04107/2018/ORD-025 zaradený do registra prevádzkovateľov základných služieb.

1. 2 Zmluvné strany uzatvárajú túto zmluvu v zmysle § 19 ods. 2 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti (ďalej len „Zákon"). Účelom tejto Zmluvy je zabezpečiť plnenie bezpečnostných opatrení a notifikačných povinností podľa Zákona počas celej doby platnosti Zmluvy o poskytovaní podpory a rozvoji informačného systému SAP č. Z/BTS/DTPR/185/2022 (ďalej len „Zmluva o poskytovaní podpory"), pri plnení ktorej Dodávateľ vykonáva pre Prevádzkovateľa činnosti súvisiace s prevádzkou sietí a informačných systémov.

Článok II.
ZÁKLADNÉ POJMY

Na účely tejto zmluvy sa rozumie:

a) **sieťou elektronická komunikačná sieť podľa**
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) **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,

m) **prevádzkovateľom základnej služby** orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa § 3 písmena l) zákona o kybernetickej bezpečnosti, resp. podľa písmena k) tohto článku.

n) **digitálnou službou** služba, ktorej druh je uvedený prílohe č. 2 zákona o kybernetickej bezpečnosti,

o) **manažér kybernetickej bezpečnosti (MKB)** je osoba poverená riadením kybernetickej bezpečnosti,. Ide najmä o kontrolné činnosti, riešenie bezpečnostných a kybernetických incidentov, riadenie implementácie bezpečnostných opatrení, konzultačné a metodické činnosti pre oblasť kybernetickej bezpečnosti a ďalšie,

p) **riešením kybernetického bezpečnostného incidentu** všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

Článok III.
PREDMET ZMLUVY

1. Prevádzkovateľ základnej služby je povinný v zmysle § 19 ods. 2 Zákona uzatvoriť s Dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Obsah Zmluvy o zabezpečení kybernetickej bezpečnosti ustanovuje § 8 Vyhlášky.

2. V zmysle § 19 ods. 2 Zákona, a s ohľadom na hlavný zmluvný vzťah, je predmetom tejto zmluvy stanovenie práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

3. V rámci tejto zmluvy je potrebné stanoviť základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Prevádzkovateľa základnej služby a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany Prevádzkovateľa základnej služby (ďalej len **„ciele"**), a to aj v spolupráci s Dodávateľom.

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 zároveň povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby. 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. O takejto zmene Prevádzkovateľ upovedomí Dodávateľa.

5. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy.

6. Dodávateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto zmluvy.

7. 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 hlavného zmluvného vzťahu a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy od Prevádzkovateľa základnej služby nemá nárok.

Článok V.
BEZPEČNOSTNÉ OPATRENIA

1. Dodávateľ sa zaväzuje, že má zavedené a implementované bezpečnostné opatrenia v zmysle § 20 ods. 3 Zákona, a to minimálne v rozsahu:
   - organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
   - riadenia aktív, hrozieb a rizík 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 v zmysle § 20 ods. 4 Zákona zahŕňať najmenej:
   - 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 centrálneho systému včasného varovania.
   - 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

3. Bezpečnostné opatrenia Prevádzkovateľ základnej služby prijíma a realizuje 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 podľa § 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 hlavného zmluvného vzťahu 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. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí sa budú podieľať na plnení hlavného zmluvného vzťahu 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 podľa článku XII. bod 2. tejto zmluvy; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení podľa tohto bodu.

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

4. Dodávateľ sa zaväzuje prijať a dodržiavať všeobecné bezpečnostné opatrenia rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

5. Dodávateľ sa zaväzuje prijať a dodržiavať bezpečnostné opatrenia najmenej v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) Zákona v rozsahu podľa § 9, § 10, § 12, § 14 a § 15 Vyhlášky a v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

6. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

Článok VII.
POSTUP PRI RIEŠENÍ KYBERNETICKÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý incident a všetky skutočnosti majúce vplyv na zabezpečovanie kybernetickej bezpečnosti Prevádzkovateľovi základnej služby spôsobom určeným v článku XII. bod 1. tejto zmluvy, 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, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len „**reaktívne opatrenie**"). Pri riešení incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby, NBÚ a ďalším ústredným orgánom alebo iným orgánom štátnej správy určeným v § 4 zákona o kybernetickej bezpečnosti jednať, 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 sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby.

4. Dodávateľ sa zaväzuje oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.

5. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.

6. Po vyriešení incidentu je Dodávateľ na výzvu Prevádzkovateľa základnej služby v ním 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 lehote, ktorú určí Prevádzkovateľ základnej služby, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom základnej služby na jeho návrhu.

7. 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 všetkých skutočnostiach, ktoré sa dozvedel pri plnení povinností a ku ktorým sa zaviazal v súvislosti s plnením hlavného zmluvného vzťahu 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. Dodávateľ sa v rovnakom rozsahu zaväzuje zaviazať povinnosťou mlčanlivosti aj všetky ním poverené osoby, ktoré budú zúčastnené na predmete plnenia tejto Zmluvy o zabezpečení kybernetickej bezpečnosti (t. j. jeho zamestnanci, subdodávatelia a ich zamestnanci). Dodávateľ je povinný na požiadanie preukázať Prevádzkovateľovi splnenie tejto povinnosti. Povinnosť mlčanlivosti trvá aj po zániku ich pracovno-právneho vzťahu alebo obchodného vzťahu.

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

4. Po ukončení tejto zmluvy je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tohto zmluvného vzťahu prístup, resp. tieto podľa pokynu Prevádzkovateľa základnej služby zničiť.

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

6. Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa zákona o kybernetickej bezpečnosti nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

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 v článku XII. tejto zmluvy, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

2. Dodávateľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.

3. Kontaktné osoby podľa prílohy č. 1 tejto zmluvy môže Dodávateľ zmeniť, ak oznámi novú kontaktnú osobu Prevádzkovateľovi základnej služby v písomnej forme poštou na adresu sídla Prevádzkovateľa základnej služby; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve.

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 NBÚ v oblasti kybernetickej bezpečnosti.

2. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto zmluvy v súlade so sektorovými bezpečnostnými opatreniami, ktoré vydáva Ministerstvo hospodárstva Slovenskej republiky v spolupráci s NBÚ.

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, dôvernosť, 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 dôvernosť, 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 zapojenia ďalšieho dodávateľa (ďalej len ako „**subdodávateľ**“) 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. Dodávateľ zodpovedá za konanie prípadných subdodávateľov tak, ako keby konal sám.

8. 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.

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.

2. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní od vykonania auditu Prevádzkovateľom základnej služby. O náprave takýchto nedostatkov a o spôsobe ich nápravy Dodávateľ upovedomí Prevádzkovateľa základnej služby vo vyššie uvedenej lehote, a to v písomnej forme na adresu sídla Prevádzkovateľa základnej služby uvedenú v záhlaví tejto zmluvy.

3. 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.

4. 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.

5. 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.

6. 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.

7. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej desať 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.

8. Dodávateľ sa zaväzuje informovať Prevádzkovateľa základnej služby spôsobom podľa článku XII. bod 3. o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.

9. 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. tejto zmluvy sa uplatňujú primerane.

10. 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 ako „**BOZP**") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len ako „**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.

HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV A INÝCH INFORMÁCIÍ

1. Dodávateľ je podľa článku VII. bod 1. tejto zmluvy povinný bezodkladne informovať Prevádzkovateľa základnej služby o kybernetickom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti. Formulár na hlásenie kybernetických incidentov sa nachádza v prílohe č. 4, pričom Dodávateľ nahlasuje Prevádzkovateľovi bezpečnostné incidenty prostredníctvom e-mailu.
2. Dodávateľ je taktiež podľa článku VI. bod 2. tejto zmluvy povinný nahlásiť Prevádzkovateľovi každú zmenu v personálnom obsadení, ktorá by mala vplyv na zoznam pracovných rolí Dodávateľa, a to bezodkladne po uskutočnení takejto zmeny. Dodávateľ informuje Prevádzkovateľa základnej služby o tejto zmene elektronicky alebo písomne poštou na adresu sídla Prevádzkovateľa základnej služby uvedenú v záhlaví tejto zmluvy.
3. Dodávateľ je povinný hlásiť všetky ďalšie informácie požadované Prevádzkovateľom základnej služby, ktoré sú vymedzené v tejto zmluve a informácie potrebné na plnenie jeho povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti, a to elektronicky alebo písomne poštou na adresu sídla Prevádzkovateľa základnej služby uvedenú v záhlaví tejto zmluvy.
4. Dodávateľ je povinný nahlásiť Prevádzkovateľovi aj všetky ostatné informácie, ktoré by

mohli mať vplyv na zmluvu, a to bezodkladne po uskutočnení takejto zmeny elektronicky alebo doporučene na adresu sídla Prevádzkovateľa základnej služby uvedenú v záhlaví tejto zmluvy.

Článok XIII.
SANKCIE

1. V prípade porušenia akejkoľvek povinnosti, záväzku alebo vyhlásenia Dodávateľa uvedených v tejto zmluve o zabezpečení kybernetickej bezpečnosti, vrátane porušenia povinnosti mlčanlivosti, je Prevádzkovateľ oprávnený požadovať od Dodávateľa zmluvnú pokutu vo výške 5 000 EUR za každý jednotlivý prípad, a to aj opakovane. Zaplatením zmluvnej pokuty nie je dotknutý nárok Prevádzkovateľa na náhradu škody podľa príslušných právnych predpisov.
2. 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. OBZ. Pre odstránenie právnych pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.
3. V prípade, ak orgán príslušný konať vo veciach kybernetickej bezpečnosti uloží Prevádzkovateľovi základnej služby v dôsledku porušenia akejkoľvek povinnosti, záväzku alebo vyhlásenia Dodávateľa vyplývajúcich z tejto zmluvy o zabezpečení kybernetickej bezpečnosti pokutu, alebo inú sankciu, Dodávateľ je povinný nahradiť túto Prevádzkovateľovi základnej služby v plnej výške a to do 30 dní odo dňa doručenia výzvy Prevádzkovateľa základnej služby na jej náhradu.
4. Zaplatenie zmluvnej pokuty nezbavuje Dodávateľa povinnosti splniť záväzok zabezpečený zmluvnou pokutou.

Článok XIV.
ZÁVEREČNÉ USTANOVENIA

1. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania hlavného zmluvného vzťahu.

2. Táto Zmluva je uzavretá dňom jej podpísania obidvoma Zmluvnými stranami a právne účinky nadobúda v zmysle ustanovenia § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a súvisiacich platných právnych predpisov nasledujúci deň po dni jej zverejnenia v centrálnom registri zmlúv vedenom Úradom vlády SR.

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.

4. Za podstatné porušenie zmluvy sa považuje:
   a) porušenie povinností uvedených v čl. IV ods. 1, čl. VI. ods. 3, 4, čl. VII a čl. VIII tejto zmluvy;
   b) ak Dodávateľ vedel v čase uzavretia zmluvy alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola zmluva uzavretá, že Prevádzkovateľ základnej služby nebude mať záujem na plnení povinností pri takom porušení zmluvy;
   c) Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto zmluvy.

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 po mesiaci, v ktorom bola výpoveď Dodávateľovi doručená.

6. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán.

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. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na Prevádzkovateľa základnej služby. Tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu a to najmenej po dobu piatich rokov po ukončení tejto zmluvy.

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

10. 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 všeobecné súdy Slovenskej republiky.

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

12. 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.

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

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

15. Táto zmluva bola vyhotovená v štyroch rovnopisoch, po dvoch pre každú zmluvnú stranu.

16. 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 – Formulár na hlásenie incidentov

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

V Bratislave dňa 21 NOV. 2022

Prevádzkovateľ základnej služby:

[redacted]

Ing. Ing. Dušan Keketi
predseda predstavenstva
a generálny riaditeľ
Letisko M. R. Štefánika – Airport Bratislava, a.s. (BTS)

[redacted]

Ing. Ing. Otto Szőke
Člen predstavenstva
Letisko M. R. Štefánika – Airport Bratislava, a.s. (BTS)

V Bratislave dňa 23. 11. 2022

Dodávateľ:

[redacted]

Ing. Peter Maťašek
SLOVAKODATA, a. s.

27

bts.aero BRATISLAVA AIRPORT
Letisko M. R. Štefánika – Airport Bratislava, a. s. (BTS)
P. O. Box 160, 823 11 Bratislava 216

Príloha 1
Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa - VZOR

Prevádzkovateľ základnej služby:

Rola	Proces súvisiaci s prevádzkou ZS	Email
MKB	Manažér kybernetickej bezpečnosti	[redacted]

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email
Ing. Karol Haják	riaditeľ úseku realizácie		[redacted]	[redacted]

Príloha č. 2
Bezpečnostné opatrenia v organizácii Prevádzkovateľa základnej služby, ktoré sa vzťahujú na Dodávateľa

I. Riadenie dodávky služieb poskytovaných tretími stranami

1. Informačné systémy a služby dodávané tretími stranami musia spĺňať politiku kybernetickej bezpečnosti.

2. Pred poskytnutím informácií týkajúcich sa informačného systému BTS vrátane žiadosti o návrh riešenia musí byť s treťou stranou uzavretá dohoda o mlčanlivosti, ak nejde o výkon auditu podľa všeobecne záväzných právnych predpisov.

3. Bez dohody o mlčanlivosti nesmú byť poskytnuté tretej strane žiadne informácie týkajúce sa informačného systému BTS, požadovaných riešení, alebo služieb. Výnimku tvoria všeobecne známe skutočnosti a informácie, ktoré nie sú predmetom mlčanlivosti.

4. 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.

5. Zamestnanci tretej strany, ktorý pracujú s informačnými aktívami BTS musia byť rovnako preukázateľne oboznámení s pravidlami pre oblasť kybernetickej bezpečnosti.

6. Za oboznamovanie tretích strán a ich zamestnancov s internými predpismi týkajúcimi sa kybernetickej bezpečnosti je zodpovedný vlastník informačného aktíva. Spôsob a formu oboznámenia určí manažér kybernetickej bezpečnosti.

7. Dodávateľ alebo tretia strana musí prehlásiť znalosť a schopnosť implementovať bezpečnostné opatrenia ustanovené v interných predpisoch BTS a v dokumentácii navrhovaného diela.

8. Výnimku z bezpečnostných požiadaviek a opatrení môže v odôvodnených prípadoch na žiadosť zadávateľa udeliť manažér kybernetickej bezpečnosti. V prípade rozporu o udelenie výnimky rozhoduje bezpečnostný výbor.

9. Zachovávanie bezpečnostných opatrení v informačných systémoch a službách dodaných tretími stranami musí byť priebežne monitorované a kontrolované tretími stranami ako aj BTS. Prípadné nedostatky musí tretia strana odstrániť v čo najkratšej dobe.

10. Ak sa identifikujú nové bezpečnostné riziká pri dodávke informačného systému tretími stranami, musia byť určené bezpečnostné opatrenia na ich elimináciu.

11. 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.

12. Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia musí byť určená v zmluve s treťou stranou.

II. Bezpečnostné požiadavky na informačné systémy

1. Pri akvizícii, vývoji, alebo údržbe informačných systémov a služieb musí byť pri ich plánovaní ako aj v procese realizácie vykonaný odhad, alebo analýza bezpečnostných rizík, ktorých účelom je identifikovať bezpečnostné riziká a určiť bezpečnostné opatrenia na ich elimináciu.

2. Za koordináciu identifikácie rizík, určenie a schválenie bezpečnostných opatrení pri akvizícii, vývoji a údržbe informačného systému je zodpovedný manažér kybernetickej bezpečnosti BTS.

3. Bezpečnostné opatrenia vo forme bezpečnostných požiadaviek musia byť zapracované do projektovej dokumentácie, alebo zadania tretej strane a musia byť súčasťou akceptačného testovania informačného systému alebo služby. Za zapracovanie bezpečnostných požiadaviek je zodpovedný vlastník informačného aktíva.

4. Interná štruktúra spracovania, vstupné a výstupné funkcie aplikácií, informačných systémov a služieb BTS musia byť navrhnuté a vytvorené tak, aby bol proces spracovania informácií v týchto systémoch bezpečný a aby sa vylúčilo riziko
a) chybného spracovania,
b) prerušenia prevádzky,
c) neoprávneného prístupu,
d) zneužitia a úniku informácií, alebo
e) inej kompromitácie systému.

5. Zmeny vykonávané na informačných systémoch a službách BTS musia byť vykonávané na základe formálneho postupu, ktorý okrem dokumentácie zmeny musí vyžadovať odhad, alebo analýzu bezpečnostných rizík a schválenie zmeny manažérom kybernetickej bezpečnosti.

6. Za účelom odstránenia zraniteľností musia byť na všetkých informačných systémoch vrátane pracovných staníc BTS aplikované bezpečnostné záplaty publikované výrobcom. Za aplikáciu bezpečnostných záplat zodpovedajú správcovia jednotlivých informačných systémov.

III. Riadenie incidentov kybernetickej bezpečnosti

1. Zamestnanci BTS, ako aj zamestnanci tretích strán, ktorí pri svojej činnosti vytvárajú, spravujú, alebo inak využívajú informačné systémy a služby BTS sú povinní hlásiť všetky bezpečnostné incidenty, podozrenia, alebo bezpečnostne relevantné udalosti, ktoré môžu byť príčinou bezpečnostného incidentu, o ktorých sa dozvedeli pri svojej pracovnej alebo inej činnosti.

2. O tom, či udalosť je kybernetický bezpečnostný incident, rozhoduje manažér kybernetickej bezpečnosti BTS a v prípade rozporu bezpečnostný výbor BTS.

3. Kybernetický bezpečnostný incident je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia politiky kybernetickej bezpečnosti negatívny vplyv na bezpečnosť, alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo ohrozenie bezpečnosti informácií.

4. Manažér kybernetickej bezpečnosti na základe zistených následkov alebo predpokladaných následkov, rozsahu alebo spôsobu vykonania určí závažnosť kybernetického bezpečnostného incidentu.

5. Na základe zistených následkov manažér kybernetickej bezpečnosti môže počas riešenia bezpečnostného incidentu zmeniť kybernetický bezpečnostný incident na závažný kybernetický bezpečnostný incident. Zmenu závažného kybernetického bezpečnostného incidentu na kybernetický bezpečnostný incident môže manažér kybernetickej bezpečnosti vykonať len na základe schválenia bezpečnostným výborom.

IV. Vznik a hlásenie kybernetického bezpečnostného incidentu

1. Zdrojom udalostí pre identifikáciu kybernetického bezpečnostného incidentu sú:
a) hlásenie používateľa BTS,
b) hlásenie používateľa tretej strany,
c) výstup z bezpečnostného monitoringu informačno-komunikačných technológií,
d) výstup z bezpečnostných technológií,
e) výsledok z kontrolnej činnosti (audit, penetračný test, test zraniteľnosti a pod.),
f) informácia z externého zdroja (internet, médiá a pod.),
g) podnet priamo od manažér kybernetickej bezpečnosti,

2. Používateľ BTS, ako aj používateľ tretej strany, ktorý pri svojej činnosti používa, vytvára, spravuje alebo inak využíva informačný systém alebo službu BTS je povinný hlásiť každý bezpečnostný incident alebo podozrenie, ktoré môže neplánovane znepristupniť službu a/alebo spustiť bezpečnostný. Za bezpečnostný incident sa považuje aj porušenie ochrany osobných údajov.

3. Používateľ BTS hlási incident priamo na ServiceDesk, používatelia riadiacich systémov nahlasujú incidenty na Hotline RS.

4. Používateľ tretej strany nahlasuje bezpečnostný incident zamestnancovi BTS, ktorý je zodpovedný za koordináciu nimi dodávaného informačného systému alebo služby.

5. Zamestnanec ServiceDesk, resp. Hotline RS eskaluje bezpečnostný incident na manažéra kybernetickej bezpečnosti. Manažér kybernetickej bezpečnosti prijaté informácie preverí a rozhodne o ďalšom riešení incidentu. V prípade, že sa jedná o incident týkajúci sa porušenia ochrany osobných údajov v automatizovanej forme, zamestnanec ServiceDesk, resp. Hotline RS kontaktuje zodpovednú osobu na ochranu osobných údajov.

6. Po vzniku bezpečnostného incidentu je zakázané vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov bezpečnostného incidentu (poradiť sa s administrátorom príslušného informačného systému, v prípade nájdenia citlivého dokumentu nachádzajúceho sa na chodbe, zamedziť jeho ďalšiemu šíreniu tým, že ho zamestnanec uchová u seba a následne odovzdá manažérovi kybernetickej bezpečnosti, a pod.).

7. Manažér kybernetickej bezpečnosti bezodkladne vykoná všetky nevyhnutné opatrenia, ktoré sú potrebné, aby sa predišlo rozšíreniu následkov kybernetického bezpečnostného incidentu.

8. Manažér kybernetickej bezpečnosti v prípade, že aktivity používateľa spôsobili kybernetický bezpečnostný incident o tejto skutočnosti informuje daného používateľa a ak je to potrebné aj jeho nadriadeného zamestnanca.

V. Riadenie privilegovaného prístupu tretej strany do informačných systémov BTS

1. Tretej strane sa môže privilegované prístupové oprávnenie prideliť len na dobu nevyhnutnú na realizáciu požadovaného zásahu, maximálne po dobu platného zmluvného vzťahu. Po tejto dobe musí byť prístupový účet deaktivovaný. Výnimky z uvedeného postupu schvaľuje manažér kybernetickej bezpečnosti.

2. Žiadosť o pridelenie privilegovaného prístupového oprávnenia pre pracovníka tretej strany do informačného systému spoločnosti BTS zabezpečuje vlastník informačného systému.

3. Pre proces prideľovania a zmeny privilegovaného prístupového oprávnenia zamestnancovi tretej strany sa použijú ustanovenia uvedené v čl. 7.

4. Zriadenie privilegovaného prístupového oprávnenia tretej strane do informačného systému alebo infraštruktúry BTS je umožnené len za predpokladu identifikácie a minimalizácie rizík, ktoré z toho vyplývajú.

5. Zrušenie privilegovaného prístupového oprávnenia pre zamestnanca tretej strany je realizované:

a) po uplynutí lehoty, na ktorú bolo privilegované prístupové oprávnenie udelené,
b) po ukončení zmluvy s treťou stranou,
c) na pokyn manažéra kybernetickej bezpečnosti, vedúceho odboru AICT vedúceho oddelenia HSE a QPR alebo vedúceho oddelenia RS,
d) po ukončení pracovného pomeru pracovníka tretej strany s treťou stranou.

VI. Činnosti realizované treťou stranou

1. Jednotlivé činnosti týkajúce sa správy, prevádzky, údržby alebo podpory informačného systému a komponentov infraštruktúry BTS môžu byť vykonávané treťou stranou na základe zmluvného vzťahu.

2. Každá zmluva s treťou stranou, ktorá zabezpečuje správu, prevádzku, údržbu alebo podporu informačného systému alebo služieb BTS musí obsahovať:
   a) požiadavky na úroveň poskytovaných služieb,
   b) ustanovenia týkajúce sa mlčanlivosti a ochrany informácií spojených s poskytovanými činnosťami,
   c) určenie osoby tretej strany zodpovednej za informačnú bezpečnosť,
   d) povinnosť zamestnancov tretej strany dodržiavať pri práci s prvkami infraštruktúry BTS všetky interné predpisy a všeobecne záväzné právne predpisy, ktoré sa týkajú kybernetickej bezpečnosti,
   e) možnosť vykonania bezpečnostného auditu a testovania dodávaného informačného systému alebo služby,

3. V rámci dohody o úrovni poskytovaných služieb musia byť stanovené najmä:
   a) cieľová úroveň služby a akceptovateľná úroveň služby, bezpečnostné požiadavky na služby,
   b) ak ide o servisnú zmluvu, maximálna doba začiatku, prípadne ukončenia zásahu od nahlásenia poruchy,
   c) doba poskytovanej podpory (5 dní x 8 hodín denne,...) a úroveň poskytovanej podpory a to v pracovnom čase a mimo pracovného času,
   d) zodpovednosť dodávateľa za poskytovanú službu.

4. Za stanovenie požiadaviek v dohode o úrovni poskytovaných služieb zodpovedá vlastník informačného systému v súčinnosti s prevádzkovateľom informačného systému v BTS.

5. Vlastník informačného systému je zodpovedný za vykonávanie kontroly plnenia požiadaviek stanovených v dohode o úrovni poskytovaných služieb.

Príloha č. 3

Formulár na hlásenie kybernetických incidentov

Záznam o kybernetickom bezpečnostnom incidente (KBI)					
Názov KBI :				Číslo KBI:	
Dátum a čas vzniku KBI:			Dátum a čas hlásenia KBI:		
Nahlásil:				Funkcia a osobné číslo:	
Útvar		Telefónny kontakt:		Email:	
KBI zaevidoval:				Funkcia a osobné číslo:	
Popis incidentu:					
Dotknutý útvar:			Odhadovaný dopad:	Malý ☐ Stredný ☐ Veľký ☐	
Druh KBI:	Závažný ☐	Vstup/Spôsob hlásenia:			
Popis a vyčíslenie možného dopadu:					
Popis vyšetrovania KBI:					
Kategória KBI:	Útok, ☐ Zneužitie, ☐ Odcudzenie , ☐ Zlyhanie ľudského faktora, ☐ Vplyv zmien, ☐ Prerušenie prevádzky IS/SW, ☐ Nesprávna konfigurácia zariadení, ☐ Iné (uviesť):		Typ KBI:	Neautorizované činnosti v IKT ☐ Infiltrácia, alebo poku o zavedenie škodlivého kódu, ☐ Neoprávnený fyzický prístup, ☐ Zneužitie prístupových práv, ☐ Únik informácií, ☐	

			Neautorizované externé čin. voči IKT, ☐ Iné (uviesť):

Popis prijatých/navrhovaných opatrení:			
Opatrenie:	Popis opatrenia:	Útvar/osoba zodpovedná za riešenie:	Termín splnenia:

Poznámky:	
Zoznam príloh:	
Podpisy zodpovedných osôb:	Hlásenie o KBI podal: Hlásenie o KBI prijal: Navrhované opatrenia schválil: