

Číslo zmluvy:

**Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností**  
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších  
predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení  
niektorých zákonov v znení neskorších predpisov  
(ďalej len „Zmluva KB“)

medzi zmluvnými stranami:

Prevádzkovateľ základnej služby:

Sídlo:

IČO:

Zastúpený:

(ďalej len „Objednávateľ“)

a

Poskytovateľ/Zhotoviteľ: **Skupina dodávateľov IS – Industry Solutions, a.s. a Teco ZA, s.r.o.**

Hlavný člen skupiny dodávateľov:

Názov: **IS – Industry Solutions, a.s.**

Sídlo: M.R. Štefánika 129, 010 01 Žilina

IČO: 47 373 288

IČ DPH: SK2023844801

Zastúpený: Ing. Jozef Mihalčin, predseda predstavenstva

Ing. Tibor Baranec, člen predstavenstva

Zapísaný: v OR Okresného súdu Žilina, Oddiel: Sa, Vložka č.: 10805/L

a

Člen skupiny dodávateľov:

Názov: **Teco ZA, s.r.o.**

Sídlo: Vysokoškolákov 8421/41, 010 08 Žilina

IČO: 36 369 403

IČ DPH: SK2020100929

Zastúpený: Ing. Ján Králik, konateľ

Zapísaný: v OR Okresného súdu Žilina, Oddiel: Sro, Vložka č.: 10134/L

(ďalej len „Poskytovateľ/Zhotoviteľ“)

(Prevádzkovateľ základnej služby a Poskytovateľ/Zhotoviteľ spolu ďalej len „zmluvné strany“)

## Článok I.

### ÚVODNÉ USTANOVENIA

1. **Národná diaľničná spoločnosť, a. s.** je podľa § 3 písm. m) 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“) Objednávateľom podľa § 3 písm. l) zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Objednávateľa ako prevádzkovateľa kritickej základnej služby.



2. Poskytovateľ/Zhotoviteľ uzatvára s Objednávateľom ..... „.....“ (ďalej len „**hlavná zmluva**“), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v ZoKB pre Objednávateľa (ďalej aj ako „**hlavný zmluvný vzťah**“). Konkrétny rozsah činností Poskytovateľa/Zhotoviteľa je identifikovaný v hlavnej zmluve.
3. Plnenie povinností podľa tejto Zmluvy KB sa vyžaduje počas celej doby trvania hlavného zmluvného vzťahu medzi Poskytovateľom/Zhotoviteľom a Objednávateľom, pričom táto Zmluva KB trvá najneskôr dovtedy, pokiaľ bude trvať hlavný zmluvný vzťah medzi Poskytovateľom/Zhotoviteľom a Objednávateľom.
4. V súlade s ustanovením § 19 ods. 2 ZoKB je Prevádzkovateľ základnej služby povinný pri uzatvorení zmluvy s Poskytovateľom/Zhotoviteľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Objednávateľa uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti hlavnej zmluvy.

## Článok II. ZÁKLADNÉ POJMY

1. Na účely tejto Zmluvy KB sa rozumie:
  - a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,
  - b) kybernetickým priestorom globálny, dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktívované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,
  - c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
  - d) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
  - e) 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,
  - f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
  - g) 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,
  - h) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
  - i) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
  - j) 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
    - i. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,



- ii. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
  - iii. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
  - iv. ohrozenie bezpečnosti informácií,
- k) základnou službou služba, ktorá je zaradená v zozname základných služieb a
- i. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 ZoKB,
  - ii. je informačným systémom verejnej správy, alebo
  - iii. je prvkom kritickej infraštruktúry,
- l) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k) tohto bodu Zmluvy KB,
- m) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2 ZoKB,
- n) manažér informačnej a kybernetickej bezpečnosti (ďalej len „**MIKB**“) je osoba poverená riadením informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti definované v Politike informačnej a kybernetickej bezpečnosti a ďalších smerniciach Objednávateľa. Ide najmä o kontrolné činnosti, riešenie kybernetických bezpečnostných incidentov, riadenie implementácie bezpečnostných opatrení, konzultačné a metodické činnosti pre oblasť informačnej a kybernetickej bezpečnosti a ďalšie,
- o) 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. V zmysle § 19 ods. 2 ZoKB a s ohľadom na hlavnú zmluvu, je predmetom tejto Zmluvy KB úprava práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti hlavnej zmluvy.
2. Prevádzkovateľ základnej služby je povinný v zmysle § 19 ods. 2 ZoKB uzatvoriť s Poskytovateľom/Zhotoviteľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Obsah zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností definuje a ustanovuje § 9 ods. 2 Vyhlášky č. 362/2018 Z.z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej aj „**Vyhláška NBÚ**“).
3. V rámci tejto Zmluvy KB je potrebné stanoviť základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Objednávateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Objednávateľa a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany Objednávateľa (ďalej len „**ciele**“), a to aj v spolupráci s Poskytovateľom/Zhotoviteľom.
4. Prevádzkovateľ základnej služby a Poskytovateľ/Zhotoviteľ pri riešení incidentov podľa článku VI., bod 1 tejto Zmluvy KB a implementácií reaktívnych opatrení podľa článku VI., bod 2 tejto Zmluvy KB a ochranných opatrení podľa článku VI., bod 6 tejto Zmluvy KB budú postupovať podľa usmernení vládnej jednotky pre riešenie počítačových incidentov, so zreteľom na oznámenia a varovania špecifikované na web stránkach [www.csirt.gov.sk](http://www.csirt.gov.sk), [www.nbu.gov.sk](http://www.nbu.gov.sk), [www.sk-cert.sk](http://www.sk-cert.sk).



#### Článok IV.

#### PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN

1. Poskytovateľ/Zhotoviteľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Objednávateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve KB tak, aby boli naplnené ciele tejto Zmluvy KB. Zoznam bezpečnostných opatrení Objednávateľa a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v prílohe č. 2 tejto Zmluvy KB.
2. Poskytovateľ/Zhotoviteľ je povinný dodržiavať bezpečnostné opatrenia z bezpečnostných politík Objednávateľa (Príloha č. 2 tejto Zmluvy KB), ktoré sa týkajú poskytovania služby podľa hlavnej zmluvy a poskytovania služby podľa hlavnej zmluvy, s ktorými ho Prevádzkovateľ základnej služby preukázateľne písomne oboznámil, a to v rozsahu v akom súvisia s prevádzkovaním základnej služby Objednávateľom, a zároveň v akom ich je možné aplikovať na služby uvedené v článku I. bod 2 Zmluvy
3. Poskytovateľ/Zhotoviteľ berie na vedomie, že bezpečnostné požiadavky a politiky Objednávateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Objednávateľa a aktuálnym hrozbám dotýkajúcim sa Poskytovateľa/Zhotoviteľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa. Prevádzkovateľ základnej služby sa zaväzuje o takýchto plánovaných zmenách Poskytovateľa/Zhotoviteľa informovať najneskôr 30 (tridsať) dní pred ich implementovaním.
4. Poskytovateľ/Zhotoviteľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve KB tak, aby boli naplnené ciele tejto Zmluvy KB. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto Zmluvy KB.
5. Poskytovateľ/Zhotoviteľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy KB, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto Zmluvy KB pre identifikáciu prípadne pre opravu poruchy/incidentu a zabezpečenie bezpečnej prevádzky IS.
6. Odplata za plnenie povinností Poskytovateľa/Zhotoviteľa podľa tejto Zmluvy KB a náhrada všetkých nákladov vynaložených Poskytovateľom/Zhotoviteľom v súvislosti s plnením povinností Poskytovateľa/Zhotoviteľa podľa tejto Zmluvy KB sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Objednávateľom Poskytovateľovi/Zhotoviteľovi podľa hlavnej zmluvy.
7. Prevádzkovateľ základnej služby a Poskytovateľ/Zhotoviteľ sa dohodli, že Poskytovateľ/Zhotoviteľ je oprávnený podľa vlastného uváženia a na vlastnú zodpovednosť zapojiť ďalšieho zmluvného partnera (ďalej len „**subdodávateľ**“) úplne alebo čiastočne zabezpečujúceho alebo akýmkoľvek spôsobom sa podieľajúceho na službách pre Objednávateľa namiesto Poskytovateľa/Zhotoviteľa alebo spolu s Poskytovateľom/Zhotoviteľom. Poskytovateľ/Zhotoviteľ sa zaväzuje, že nezapojí ďalšieho subdodávateľa predtým, než dostane písomný súhlas Objednávateľa.
8. Zoznam subdodávateľov tvorí prílohu hlavnej zmluvy. Poskytovateľ/Zhotoviteľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Poskytovateľa/Zhotoviteľa uvedené v tejto Zmluve KB. Poskytovateľ/Zhotoviteľ je plne zodpovedný voči Objednávateľovi za plnenie povinností subdodávateľa.
9. Poskytovateľ/Zhotoviteľ sa zaväzuje, počas trvania hlavnej zmluvy, najneskôr do troch (3) dní od zmeny údajov, Objednávateľovi odovzdať v zalepenej zapečatenej obálke všetky prihlasovacie údaje (administrátorské užívateľské meno a heslo) do príslušného informačného systému na ich správu, prístupové licenčné kľúče, overovacie kľúče, prístupové master kódy do všetkých technických objektov a HW zariadení, zoznamy prístupových kariet, zoznamy pridelených RFID k zariadeniam z RFID čipom, zoznamy pridelených kľúčov od miestností vo vlastníctve NDS, a.s.



ako aj všetky ďalšie súvisiace prístupy. Zoznamy budú v tlačenej alebo elektronickej forme, ku každému prístupu bude uvedené okrem identifikácie prístupu aj meno prideleného, pracovné zaradenie, kontakt (mobil/e-mail), užívateľské meno, heslo. Prevádzkovateľ sa zaväzuje, že dané údaje budú uložené na bezpečnom mieste u MIKB, a budú využité výhradne v krízovej situácii po písomnom informovaní Poskytovateľa/Zhotoviteľa Objednávateľom.

10. Poskytovateľ/Zhotoviteľ sa zaväzuje, po skončení trvania hlavnej zmluvy, najneskôr do troch (3) dní Objednávateľovi odovzdať všetky prihlasovacie údaje (administrátorské užívateľské meno a heslo) do príslušného informačného systému na ich správu, prístupové licenčné kľúče, overovacie kľúče, prístupové master kódy do všetkých technických objektov a HW zariadení, pridelené prístupové karty, zariadenia s RFID čipom, kľúče od miestností vo vlastníctve NDS, ako aj všetky ďalšie súvisiace prístupy pre zabezpečenie funkčného a bezproblémového prevzatia systémov a zachovania kontinuity činnosti.

#### Článok V. POŽADOVANÝ ROZSAH ČINNOSTÍ DODÁVATEĽA

1. Poskytovateľ/Zhotoviteľ je povinný v rámci zabezpečenia bezpečného fungovania základnej služby Objednávateľa a predchádzaniu kybernetickým bezpečnostným incidentom, ktoré by mohli mať potenciálne nepriaznivý vplyv na základnú službu Objednávateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa v súvislosti s poskytovaním služby podľa hlavnej zmluvy (ďalej len „**incidenty**“ v príslušnom gramatickom tvare):
  - a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Poskytovateľa/Zhotoviteľa nebolo možné zasiahnuť siete a informačné systémy Objednávateľa,
  - b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy KB alebo budú mať prístup k informáciám Objednávateľa,
  - c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
  - d) sledovať hrozby, dotýkajúce sa Poskytovateľa/Zhotoviteľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa,
  - e) predchádzať vzniku incidentov,
  - f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
  - g) prijímať od Objednávateľa varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa,
  - h) spolupracovať s Objednávateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa.
2. Poskytovateľ/Zhotoviteľ je povinný stanoviť postupy plnenia svojich povinností podľa Zmluvy KB vo vlastnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; dokumentáciu je na odôvodnené požiadanie povinný predložiť Objednávateľovi na nahliadnutie.
3. Poskytovateľ/Zhotoviteľ je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 v aktuálne platnej verzii (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom v prílohe č. 2 tejto Zmluvy KB.
4. Poskytovateľ/Zhotoviteľ je povinný prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v Prílohe č. 2 tejto Zmluvy KB.



5. Poskytovateľ/Zhotoviteľ je povinný písomne informovať Objednávateľa o každej jemu preukázateľne známej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Poskytovateľ/Zhotoviteľ alebo o všetkých jemu preukázateľne známych skutočnostiach, majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti; tým nie sú dotknuté povinnosti a zodpovednosť Objednávateľa v zmysle ZoKB, osobitných predpisov a/alebo ich vykonávacích predpisov.
6. Zoznam pracovných rolí Poskytovateľa/Zhotoviteľa a zoznam jeho zamestnancov a zamestnancov subdodávateľov, ktorí sa budú podieľať na plnení hlavnej zmluvy a tejto Zmluvy KB a/alebo budú mať prístup k informáciám a údajom Objednávateľa, je uvedený v prílohe č. 1 tejto Zmluvy KB. Poskytovateľ/Zhotoviteľ je povinný bezodkladne písomne oznámiť Objednávateľovi každú zmenu v personálnom obsadení; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB. Poskytovateľ/Zhotoviteľ je povinný zaviazat povinnosťou mlčanlivosti podľa ZoKB osoby, ktoré sa budú podieľať na plnení podľa tohto bodu Zmluvy KB.

#### Článok VI.

#### POSTUP PRI RIEŠENÍ KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Poskytovateľ/Zhotoviteľ sa zaväzuje bezodkladne hlásiť každé podozrenie na kybernetický bezpečnostný incident, ako aj všetky ďalšie informácie požadované Objednávateľom na plnenie jeho povinností vyplývajúcich zo ZoKB a informácie majúce vplyv na Zmluvu KB ako aj hlavnú zmluvu Objednávateľovi spôsobom určeným Objednávateľom, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov. Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, Poskytovateľ/Zhotoviteľ sa zaväzuje odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Poskytovateľ/Zhotoviteľ sa po detekcii kybernetického bezpečnostného incidentu zaväzuje poskytnúť súčinnosť a spoločne s Objednávateľom riešiť kybernetické bezpečnostné incidenty najmä odozvou alebo inou reakciou na kybernetický bezpečnostný incident, ohraňovaním kybernetického bezpečnostného incidentu a jeho dopadov, nápravou následkov kybernetického bezpečnostného incidentu, asistenciou pri riešení kybernetického bezpečnostného incidentu na mieste, reakciou na kybernetický bezpečnostný incident a podporou reakcií na kybernetický bezpečnostný incident (ďalej len „reaktívne opatrenie“). Pri riešení kybernetických bezpečnostných incidentov je Poskytovateľ/Zhotoviteľ povinný na žiadosť Objednávateľa spolupracovať s Objednávateľom, Národným bezpečnostným úradom a ďalším ústredným orgánom alebo iným orgánom štátnej správy určeným v § 4 ZoKB jednať, a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy KB alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického bezpečnostného incidentu.
3. Poskytovateľ/Zhotoviteľ sa zaväzuje v čase detekcie kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Objednávateľovi.
4. Poskytovateľ/Zhotoviteľ sa zaväzuje bezodkladne, ale najneskôr do 24 (dvadsaťštyri) hodín po detekcii kybernetického bezpečnostného incidentu oznámiť Objednávateľovi skutočnosť, že v súvislosti s kybernetickým bezpečnostným incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Poskytovateľ/Zhotoviteľ sa zaväzuje bezodkladne, najneskôr však do 24 (dvadsaťštyri) hodín po nasadení reaktívnych opatrení v zmysle bodu 2 tohto článku Zmluvy KB, oznámiť a preukázať Objednávateľovi vykonanie reaktívneho opatrenia v súlade § 27 ods. 4 ZoKB vo formulári, ktorého vzor tvorí prílohu č. 4 tejto Zmluvy KB.



6. Po vyriešení kybernetického bezpečnostného incidentu je Poskytovateľ/Zhotoviteľ na výzvu Objednávateľa povinný predložiť Objednávateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenia“) na schválenie. Ak Poskytovateľ/Zhotoviteľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Poskytovateľ/Zhotoviteľ povinný spolupracovať s Objednávateľom na jeho návrhu.
7. Po schválení ochranného opatrenia Objednávateľom, je Poskytovateľ/Zhotoviteľ povinný ochranné opatrenie bez zbytočného odkladu, najneskôr však v lehote vyplývajúcej z opatrení schválených príslušným odborom gestora IS, vykonať. Po vykonaní ochranného opatrenia Poskytovateľom/Zhotoviteľom, je Poskytovateľ/Zhotoviteľ povinný za prítomnosti MIKB Objednávateľa preveriť jeho efektívnu účinnosť. Zmluvné strany sa dohodli, že účinnosť ochranných opatrení bude podmienená výkonom simulovaných útokov, pričom záver takýchto simulovaných útokov bude vyhodnotený na základe protokolu o efektívnom účinku ochranného opatrenia za Objednávateľa signovanom MIKB a za Poskytovateľa/Zhotoviteľa signovanom osobou.

## Článok VII. ZÁVÄZOK MLČANLIVOSTI

1. Poskytovateľ/Zhotoviteľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením hlavnej zmluvy a tejto Zmluvy KB, 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. Poskytovateľ/Zhotoviteľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základnú službu Objednávateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa. Poskytovateľ/Zhotoviteľ je zároveň povinný chrániť všetky informácie poskytnuté Objednávateľom Poskytovateľovi/Zhotoviteľovi.
2. Poskytovateľ/Zhotoviteľ sa v rovnakom rozsahu zaväzuje zaviazat povinnosťou mlčanlivosti aj všetky ním poverené osoby, ktoré budú zúčastnené na predmete plnenia tejto Zmluvy KB (t. j. jeho zamestnanci, subdodávateľa a ich zamestnanci). Poskytovateľ/Zhotoviteľ je povinný na požiadanie preukázať Objednávateľovi splnenie tejto povinnosti. Povinnosť mlčanlivosti trvá aj po zániku ich pracovno-právneho vzťahu alebo obchodného vzťahu. Povinnosť zachovávať mlčanlivosť podľa tohto článku Zmluvy KB trvá aj po skončení tejto Zmluvy KB resp. hlavnej zmluvy. Mlčanlivosť sa vzťahuje na všetkých zástupcov Poskytovateľa/Zhotoviteľa ako aj jeho Subdodávateľov.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje ZoKB.
4. Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa ZoKB nie je dotknutá povinnosť mlčanlivosti alebo zachovania obchodného tajomstva podľa osobitných predpisov.

## Článok VIII. POVINNOSTI PO SKONČENÍ ZMLUVY

1. Po ukončení tejto Zmluvy KB je Poskytovateľ/Zhotoviteľ povinný vrátiť alebo previesť na Objednávateľa všetky informácie, ku ktorým mal počas trvania tejto Zmluvy KB prístup, resp. podľa písomného pokynu Objednávateľa zabezpečiť preukázateľné zničenie akýchkoľvek nosičov elektronickej informácie certifikovanou organizáciu, a doložením protokolu s podpismi oprávnených osôb Poskytovateľa/Zhotoviteľa a objednávateľa.
2. Zmluvné strany berú na vedomie, že predmetom plnenia hlavnej zmluvy môže byť autorské dielo podľa zákona č. 185/2015 Z. z. Autorský zákon v platnom znení, ktorého súčasťou môže byť:



- a) softvér, ktorý bol vytvorený Poskytovateľom/Zhotoviteľom predovšetkým pre podmienky a potreby Objednávateľa;
  - b) softvér Poskytovateľa/Zhotoviteľa, ktorý má všeobecný charakter;
  - c) softvér tretích osôb; alebo
  - d) Open Source softvér, ktorý je podriadený príslušnej licencií slobodného softvéru.
3. Zmluvné strany berú ďalej na vedomie, že predmetom plnenia hlavnej zmluvy môže byť aj vytvorenie alebo poskytnutie iných predmetov duševného vlastníctva, ako sú napr. technická a užívateľská dokumentácia, prevádzkový manuál, návrh riešenia k Softvéru alebo k Balíkovému softvéru alebo konkrétne digitálne dizajny, vrátane grafického užívateľského rozhrania (GUI), jednotlivých ikon či symbolov, prípadne konkrétne know-how Poskytovateľa/Zhotoviteľa.
  4. S ohľadom na body 1, 2 a 3 tohto článku Zmluvy KB, zmluvné strany berú na vedomie, že Poskytovateľ/Zhotoviteľ je v zmysle § 9 ods. 2 písm. p) Vyhlášky NBÚ povinný po zániku hlavnej zmluvy umožniť Objednávateľovi zabezpečiť kontinuitu prevádzkovej základnej služby vo vzťahu k službám, ktoré priamo súvisia s prevádzkou tejto základnej služby v rámci sietí a informačných systémov Objednávateľa.
  5. Ustanovenie bodov 1 až 3 tohto článku Zmluvy KB sa uplatňuje pre dodávku autorského diela v opačnom prípade sa neaplikuje.

#### Článok IX. ZODPOVEDNOSŤ ZA ŠKODU

1. Zmluvná strana zodpovedá za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinnosti zmluvnej strany stanovenej ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvou KB.
2. V prípade, ak v dôsledku porušenia ZoKB alebo preukázateľného porušenia povinností vyplývajúcich z tejto Zmluvy KB na strane Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov vznikne Objednávateľovi ujma alebo finančná sankcia, Poskytovateľ/Zhotoviteľ zodpovedá za spôsobenú škodu podľa ustanovení ZoKB. V prípade sankcie uloženej Národným bezpečnostným úradom, túto znáša v plnom rozsahu Poskytovateľ/Zhotoviteľ.
3. V prípade, že zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvy KB (ďalej ako „**porušujúca zmluvná strana**“) a v dôsledku tohto konania alebo opomenutia konania porušujúcej zmluvnej strany preukázateľne dôjde k vzniku škody na strane druhej zmluvnej strany (ďalej ako „**poškodená zmluvná strana**“), zaväzuje sa porušujúca zmluvná strana túto škodu vzniknutú poškodenej zmluvnej strane nahradiť.
4. Vznik zodpovednosti porušujúcej zmluvnej strany za škodu vzniknutú poškodenej zmluvnej strane je však podmienená povinnosťou poškodenej zmluvnej strany preukázať porušujúcej zmluvnej strane existenciu príčinnej súvislosti medzi porušením povinnosti podľa Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy na strane porušujúcej zmluvnej strany a vznikom škody. Príчинná súvislosť je okrem iného daná aj vtedy, ak porušujúca zmluvná strana nespĺnila svoju všeobecnú preventívnu povinnosť počínať si tak, aby nedochádzalo ku vzniku škôd. Počínaním podľa predchádzajúcej vety sa rozumie najmä akýkoľvek postup zmluvnej strany, na ktorý je v zmysle Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy oprávnená a prostredníctvom ktorého mohlo byť vzniku škody zabránené.
5. V prípade preukázania existencie príčinnej súvislosti podľa tohto článku Zmluvy KB je porušujúca zmluvná strana povinná uhradiť poškodenej zmluvnej strane vzniknutú škodu, a to v lehote do 10 (desať) dní odo dňa doručenia písomnej výzvy porušujúcej zmluvnej strane na adresu



uvedenú v záhlaví tejto Zmluvy KB. V prípade potreby vzniknutú škodu posúdi nezávislá tretia strana, ktorú zabezpečí Prevádzkovateľ základnej služby.

6. Zánikom tejto Zmluvy KB nie sú dotknuté tie ustanovenia, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zániku tejto Zmluvy KB a záväzky na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy KB.

#### Článok X.

#### KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Poskytovateľ/Zhotoviteľ sa zaväzuje komunikovať pri plnení povinností podľa tejto Zmluvy KB s Objednávateľom spôsobom určeným Objednávateľom, t.j. v zmysle komunikačnej matice, pričom Poskytovateľ/Zhotoviteľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií (napr. PGP šifrovanie).
2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Poskytovateľom/Zhotoviteľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.
3. Poskytovateľ/Zhotoviteľ určuje kontaktné osoby pre komunikáciu s Objednávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.
4. Kontaktné osoby podľa prílohy č. 1 tejto Zmluvy KB 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 KB. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia Zmluvy KB o doručovaní.

#### Článok XI.

#### SPOLOČNÉ USTANOVENIA

1. Poskytovateľ/Zhotoviteľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB v súlade so ZoKB a jeho vykonávacími predpismi ostatnej platnej legislatívy, 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. Poskytovateľ/Zhotoviteľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Objednávateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Poskytovateľ/Zhotoviteľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy KB na zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
4. Poskytovateľ/Zhotoviteľ sa zaväzuje dokumentovať svoju činnosť podľa tejto Zmluvy KB.
5. Poskytovateľ/Zhotoviteľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB bezodkladne od účinnosti hlavnej zmluvy a odo dňa prebratia diela k plneniu predmetu hlavnej zmluvy, pokiaľ to nie je v tejto Zmluve KB alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
6. V prípade, ak Poskytovateľ/Zhotoviteľ plní Zmluvu KB prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Objednávateľa, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Objednávateľa, Poskytovateľ/Zhotoviteľ sa zaväzuje



zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto Zmluvy KB aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto Zmluvy KB. Poskytovateľ/Zhotoviteľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto Zmluvy KB aj u týchto subdodávateľov.

7. Objednávateľ služby je oprávnený, na základe identifikácie, určiť, že Poskytovateľa/Zhotoviteľa má významný vplyv na zabezpečenie kybernetickej bezpečnosti kritickej základnej služby.
8. V prípade, že analýza rizík Objednávateľa služby potvrdí významný vplyv Poskytovateľa/Zhotoviteľa na zabezpečenie kybernetickej bezpečnosti kritickej základnej služby Objednávateľa, je Objednávateľ povinný túto skutočnosť nahlásiť Národnému bezpečnostnému úradu (ďalej len „NBÚ“).
9. NBÚ následne podnet posúdi a v súlade s § 17 ods. 1 písm. i) a ods. 3 ZoKB Poskytovateľa/Zhotoviteľa do registra prevádzkovateľov základnej služby.
10. Poskytovateľ/Zhotoviteľ je povinný poskytnúť Objednávateľ všetku potrebnú súčinnosť pri plnení povinností vyplývajúcich z tohto článku.

## Článok XII.

### VYŠŠIA MOC

1. Vyššia moc znamená mimoriadnu udalosť alebo okolnosť, ktorú nemohla žiadna zo zmluvných strán pred uzatvorením Zmluvy KB predvídať, ktorá je mimo kontroly ktorejkoľvek zo zmluvných strán a nebola spôsobená úmyselne alebo z nedbanlivosti konaním alebo opomenutím ktorejkoľvek zmluvnej strany a ktorá podstatným spôsobom sťažuje alebo znemožňuje plnenie povinností podľa Zmluvy KB ktoroukoľvek zo zmluvných strán. Takýmito udalosťami alebo okolnosťami sú najmä živelné pohromy alebo prírodné katastrofy. Výslovne sa stanovuje, že vyššou mocou nie je štrajk personálu Poskytovateľa/Zhotoviteľa ani hospodárske pomery zmluvných strán.
2. Ak niekto zmluvných strán bráni alebo bude brániť v plnení niektorej jej povinnosti podľa Zmluvy KB vyššia moc, potom písomne oznámi druhej zmluvnej strane udalosť alebo okolnosť, ktoré predstavujú vyššiu moc, uvedie povinnosti, v ktorých plnení jej vyššia moc bráni alebo bude brániť a predpokladané trvanie takej okolnosti predstavujúcej vyššiu moc. Oznámenie musí byť urobené bezodkladne, najneskôr však v lehote 15 (pätnásť) dní potom, čo sa zmluvná strana dozvedela alebo sa pri vynaložení riadnej odbornej starostlivosti mala a mohla dozvedieť o príslušnej udalosti alebo okolnostiach predstavujúcich dôvod vyššej moci. Ak je to možné, pri vynaložení riadnej odbornej starostlivosti, musí uvedené oznámenie obsahovať návrh opatrení vedúcich k zmierneniu alebo vylúčeniu dôsledkov okolností predstavujúcich vyššiu moc. V ostatných prípadoch bude oznámenie obsahovať iba najbližší možný termín, do ktorého môže byť návrh opatrenia poskytnutý pri vynaložení primeraného úsilia. Ak návrh opatrenia druhá zmluvná strana schváli, na čo má lehotu 15 (pätnásť) dní, postupuje zmluvná strana dotknutá vyššou mocou podľa neho až do ukončenia okolností vyššej moci.
3. Po uskutočnení tohto oznámenia príslušnou zmluvnou stranou, nebude táto zmluvná strana zodpovedná za príslušné porušenie povinností po dobu, dokiaľ jej vyššia moc bráni alebo bude brániť v ich plnení.
4. Zmluvnú stranu nezbavuje zodpovednosti za porušenie povinnosti vyššia moc, ktorá nastala až v čase, kedy bola povinná zmluvná strana v omeškaní s plnením povinnosti. Účinky vylúčenia zodpovednosti sú obmedzené iba na dobu, dokiaľ trvá vyššia moc.
5. Každá zmluvná strana vždy vyvinie všetko úsilie potrebné k tomu, aby minimalizovala omeškanie pri plnení svojich povinností podľa Zmluvy KB, ktoré vzniklo v dôsledku vyššej moci, najmä plniť



návrh opatrenia, ak je tento schválený druhou zmluvnou stranou.

6. Príslušná zmluvná strana oznámi druhej zmluvnej strane okamih ukončenia pôsobenia vyššej moci v rovnakej lehote ako pri oznámení o jej vzniku podľa bodu 2 tohto článku tejto Zmluvy KB.
7. Ak je z dôvodu okolností vylučujúcej zodpovednosť alebo prípadu vyššej moci plnenie Zmluvy KB jednej zo zmluvných strán ovplyvnené len čiastočne, takáto zmluvná strana zostáva zodpovedná za plnenie tých záväzkov, ktoré okolnosťou vylučujúcou zodpovednosť alebo vyššou mocou nie sú dotknuté.
8. Ak má niektorý zo subdodávateľov podľa akejkoľvek zmluvy či dohody týkajúcej sa poskytovania služby podľa tejto Zmluvy KB širšie definovaný nárok na omeškanie v dôsledku pôsobenia vyššej moci, okolností vylučujúcich zodpovednosť alebo iného obdobného právneho inštitútu, než ako je definovaná vyššia moc podľa tejto Zmluvy KB, takéto širšie definované udalosti alebo okolnosti neospravedlňujú porušenie povinností podľa Zmluvy KB s Poskytovateľom/Zhotoviteľom ani mu nezakladajú nároky podľa tohto článku Zmluvy KB.

### Článok XIII

#### AUDIT KYBERNETICKEJ BEZPEČNOSTI/AUDIT BEZOEČNOSTI

1. Prevádzkovateľ základnej služby je oprávnený vykonať v rozsahu predmetu hlavnej zmluvy voči Poskytovateľovi/Zhotoviteľovi ako aj u jeho subdodávateľom audit zameraný na overenie plnenia povinností Poskytovateľa/Zhotoviteľa a subdodávateľov podľa tejto Zmluvy KB a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Poskytovateľa/Zhotoviteľa a subdodávateľov na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Poskytovateľa/Zhotoviteľa a subdodávateľov pre plnenie cieľov tejto Zmluvy KB.
2. Prípadné nedostatky zistené auditom sú Poskytovateľ/Zhotoviteľ a subdodávateľia povinní odstrániť bez zbytočného odkladu, ak to je procesne a finančne toho času možné. V prípade, že tieto nedostatky nebudú v lehote 60 (šesťdesiat) dní od zistenia na základe auditu odstránené, považuje sa to za podstatné porušenie Zmluvy KB zo strany Poskytovateľa/Zhotoviteľa.
3. Prevádzkovateľ základnej služby môže audit u Poskytovateľa/Zhotoviteľa a subdodávateľov realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Objednávateľa pri výkone auditu realizuje Objednávateľom poverená tretia osoba.
4. Poskytovateľ/Zhotoviteľ sa zaväzuje za seba ako aj za subdodávateľov pri audite spolupracovať s Objednávateľom a sprístupniť mu svoje priestory ak spadajú do predmetu plnenia hlavnej zmluvy, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
5. Prevádzkovateľ základnej služby, prípade ním oprávnené tretie osoby sú v rámci auditu oprávnení klásť otázky zamestnancom Poskytovateľa/Zhotoviteľa a subdodávateľom, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB.
6. V rámci auditu sú Poskytovateľ/Zhotoviteľ a subdodávateľia povinní preukázať Objednávateľovi súlad s touto Zmluvou KB, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzkov a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto Zmluvy KB a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Poskytovateľovi/Zhotoviteľovi najmenej 15 (pätnásť) pracovných dní vopred svoj zámer realizovať u Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov audit. Vykonanie alebo nevykonanie auditu Objednávateľom nezbavuje Poskytovateľa/Zhotoviteľa zodpovednosti za plnenie povinností Poskytovateľa/Zhotoviteľa vyplývajúcich z tejto Zmluvy KB. Ak Poskytovateľ/Zhotoviteľ alebo jeho subdodávateľ neumožní



vykonanie auditu, považuje sa to za podstatné porušenie Zmluvy KB a Prevádzkovateľ základnej služby je oprávnený vyvodiť voči Poskytovateľ/Zhotoviteľ zmluvné sankcie.

8. Poskytovateľ/Zhotoviteľ sa zaväzuje písomne informovať Objednávateľa v zmysle komunikačnej matice o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Poskytovateľom/Zhotoviteľom.
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 VII. ods. 2, 3 a 4 tejto Zmluvy KB sa uplatňujú primerane.
10. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov v rámci výkonu auditu musia dodržiavať pokyny Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „BOZP“) a ochrany pred požiarom na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO“), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Poskytovateľ/Zhotoviteľ. Poskytovateľ/Zhotoviteľ sa zaväzuje pred vykonaním auditu v priestoroch Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov písomne informovať zamestnancov Objednávateľa o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Poskytovateľ/Zhotoviteľ alebo jeho subdodávateľia na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia, vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov.
11. Pre vylúčenie akýchkoľvek pochybností sa Poskytovateľ/Zhotoviteľ zaväzuje zabezpečiť Objednávateľovi vykonanie auditu v zmysle tohto článku tejto Zmluvy KB aj u svojich subdodávateľov.

#### Článok XIV.

#### SANKCIE

1. Zmluvné strany sa dohodli, že v prípade porušenia ktorejkoľvek povinnosti Poskytovateľa uvedenej v bode 1 až 12 prílohy č. 2 tejto Zmluvy je Objednávateľ oprávnený uložiť Poskytovateľovi zmluvnú pokutu vo výške 500 EUR (slovom: päťsto eur) za každý, aj začatý deň trvania porušenia povinnosti, až do vykonania nápravy, a to aj opakovane a za každé jednotlivé porušenie povinnosti samostatne.
2. V prípade, ak Poskytovateľ/Zhotoviteľ spôsobí Objednávateľovi porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo Zmluvy KB akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. Pre odstránenie právnych pochybností, zodpovednosť Poskytovateľa/Zhotoviteľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Poskytovateľ/Zhotoviteľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Objednávateľovi tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Poskytovateľom/Zhotoviteľom.
3. Zmluvné strany sa dohodli, že uplatnením sankcií v zmysle tohto článku Zmluvy KB nie je dotknutý nárok Objednávateľa na náhradu škody, ktorá mu vznikla porušením povinností Poskytovateľa/Zhotoviteľa.



4. Zaplataenie zmluvnej pokuty nezavuje Poskytovateľa/Zhotoviteľa povinnosti splniť záväzok zabezpečený zmluvnou pokutou.

#### **Článok XV. TRVANIE ZMLUVY**

1. Táto Zmluva KB sa uzatvára na dobu určitú, a to na dobu trvania hlavnej zmluvy. Táto Zmluva KB môže byť ukončená v prípadoch ustanovených v Zmluve KB alebo na základe zákona.
2. Za podstatné porušenie Zmluvy KB sa považuje:
  - a) porušenie ktorejkoľvek povinnosti uvedenej v tejto Zmluve KB;
  - b) ak Poskytovateľ/Zhotoviteľ, ako strana porušujúca Zmluvu KB, vedel v čase uzavretia Zmluvy KB alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel Zmluvy KB, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola Zmluva KB uzavretá, že Prevádzkovateľ základnej služby nebude mať záujem na plnení povinností pri takom porušení Zmluvy KB;
  - c) Poskytovateľ/Zhotoviteľ neposkytne potrebnú súčinnosť v zmysle tejto Zmluvy KB.
3. Odstúpením/okamžitým odstúpením od hlavnej zmluvy Zmluva KB zaniká.
4. Túto Zmluvu KB nie je možné vypovedať Poskytovateľom/Zhotoviteľom ani Objednávateľom, a je viazaná na účinnosť hlavnej zmluvy.
5. Po zániku tejto Zmluvy KB je Poskytovateľ/Zhotoviteľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Objednávateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Objednávateľom. Licenčné podmienky sa riadia hlavnou zmluvou.

#### **Článok XVI. ZÁVEREČNÉ USTANOVENIA**

1. Táto Zmluva KB sa spravuje zákonmi Slovenskej republiky. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
2. Prípadné spory vyplývajúce z tejto Zmluvy KB budú riešené predovšetkým mimosúdne. Podpisom tejto Zmluvy KB zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto Zmluvy KB sú príslušné súdy Slovenskej republiky.
3. Táto Zmluva KB sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo Zmluvy KB nevyplýva niečo iné.
4. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto Zmluvy KB na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
5. V prípade, ak niektoré z ustanovení Zmluvy KB je alebo sa stane neúplným, neplatným, neúčinným a/alebo nevykonateľným, nie sú tým dotknuté ostatné ustanovenia Zmluvy KB, pokiaľ z jeho povahy, obsahu alebo okolností, za ktorých bolo dojednané nevyplýva, že ho nie je možné oddeliť od ostatného obsahu Zmluvy KB. Zmluvné strany sa zaväzujú bez zbytočného odkladu nahradiť takéto neúplné, neplatné, neúčinné a/alebo nevykonateľné ustanovenie, takým úplným, platným, účinným a/alebo vykonateľným ustanovením, ktoré svojím obsahom najviac zodpovedá nahrádzanému ustanoveniu.
6. Táto Zmluva KB predstavuje úplnú dohodu zmluvných strán o jej obsahu. Podpisom tejto Zmluvy KB zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto Zmluvy KB a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto Zmluve KB neuvedených, ústnych alebo písomných dojednaní a dohôd.



7. Táto Zmluva KB bola vyhotovená v **(4) štyroch** rovnopisoch, po (2) dvoch pre každú zmluvnú stranu.
8. 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.
9. Táto Zmluva KB nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv.
10. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
  - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Objednávateľa a Poskytovateľa/Zhotoviteľa, **(nezverejňuje sa v CRZ, GDPR)**
  - Príloha č. 2 - Špecifikácia a rozsah bezpečnostných opatrení - Bezpečnostné opatrenia v organizácii Objednávateľa, ktoré sa vzťahujú na Poskytovateľa/Zhotoviteľa (vyplývajúce z Bezpečnostných smerníc Objednávateľa), **(nezverejňuje sa v CRZ)**
  - Príloha č. 3 – Vzor - Záznam o kybernetickom bezpečnostnom incidente
11. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu KB neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy KB dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

**Prevádzkovateľ základnej služby:**

**Poskytovateľ/Zhotoviteľ:**

V Bratislave dňa.....

V Žiline dňa 14.02.2025

\_\_\_\_\_  
(obchodné meno)  
(titul, meno, priezvisko  
štatutára)  
(funkcia)

\_\_\_\_\_  
IS – Industry Solutions, a.s.  
Ing. Jozef Mihalčin  
predseda predstavenstva

\_\_\_\_\_  
IS – Industry Solutions, a.s.  
~~Ing. Jozef Mihalčin~~ Ing. Tibor Baranec  
predseda predstavenstva  
8/en



**Príloha č. 1: Zoznam pracovných rolí a kontaktov Objednávateľa a Poskytovateľa/Zhotoviteľa (nezverejňuje sa v CRZ,GDPR)**

Prevádzkovateľ základnej služby:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email

Poskytovateľ/Zhotoviteľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email



## Príloha č. 2

## Špecifikácia a rozsah bezpečnostných opatrení

1. Informovať NDS o všetkých skutočnostiach majúcich vplyv na túto zmluvu a o jeho povinnostiach vyplývajúcich z tejto zmluvy alebo zo zákona vzhľadom na ustanovenia tejto zmluvy a zabezpečenie požiadaviek zákona č. 69/2018 Z. z..
2. Poskytovateľa je povinný zaviazat svojich zamestnancov týmito povinnosťami:
  - zamestnancovi sa zakazuje zverejňovať alebo inej osobe vyzradiť svoje autentizačné údaje (heslá), taktiež sa zakazuje držanie záznamu hesiel (napr. na papieri, v softvérovom súbore, na prenosnom zariadení a pod),
  - zamestnanec je povinný chrániť pridelený autentizačný prostriedok pred odcudzením a zničením a nesmie ho prenechať inej osobe,
  - zamestnancovi sa zakazuje pristupovať k IT aktívam, ktoré nie sú predmetom zmluvného vzťahu a vykonávať na nich akúkoľvek činnosť,
  - zamestnancovi sa zakazuje vykonávať činnosti, ktoré nie sú predmetom zmluvného vzťahu.
3. Chrániť všetky informácie poskytnuté NDS pred ich únikom a zneužitím,
4. Zapojiť do činností vykonávaných v zmysle tejto zmluvy len také tretie strany, ktoré bude NDS akceptovať a ktoré budú schopné splniť požiadavky uvedené v tejto zmluve tak, ako by ich plnil Poskytovateľ.
5. **Bezpečnostné opatrenia- riadenia prístupu**
  - Riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa.
  - Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
  - Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
  - Privilegované prístupové práva do informačných systémov technologického vybavenia súvisiacich s predmetom rámcovej dohody sa prideľujú len na dobu nevyhnutnú na realizáciu požadovaného servisného zásahu, maximálne však na šesť mesiacov za čo zodpovedá správca dotknutého informačného systému. Po tejto dobe musí byť prístupový účet deaktivovaný, alebo opätovne reaktivovaný.
6. **Bezpečnostné opatrenia - technické zraniteľnosti systémov a zariadení**
  - sledovať hrozby voči technologickému vybaveniu, ktoré by mohli mať potenciálny nepriaznivý vplyv na kritickú základnú službu NDS,
  - využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov. V prípade CVSS skóre nad 9.0 je Poskytovateľ povinný postupovať v zmysle odporúčaní výrobcu.
7. **Bezpečnostné opatrenia – ochrana proti škodlivému kódu**
  - Inštalovať a aktualizovať antivírusový softvér na všetkých zariadeniach, ktoré to umožňujú.
  - určiť zodpovednosti používateľov technológie za prevenciu pred škodlivým kódom,
  - Je povolené vyberať len overené a spoľahlivé antivírusové a antimalware programy od renomovaných výrobcov.
  - Poskytovateľ je povinný zabezpečiť, aby antivírusový a antimalware softvér bol vždy aktuálny.



- Kontrolovať funkčnosť a prevádzku predmetu rámcovej dohody

#### 8. Bezpečnostné opatrenia- riadenia sieťovej a komunikačnej bezpečnosti

- Pripojenie do siete a informačného systému a využitie vzdialený prístup, musí byť zabezpečené napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov a musí byť schválené NDS.
- Zamestnanci Poskytovateľa sú povinní pred prihlásením k aktívu NDS o tejto skutočnosti informovať kontaktnú osobu NDS buď prostredníctvom mailu alebo telefonicky. Na základe tohto oznámenia im bude povolené pripojenie. Po skončení údržby alebo inej činnosti zamestnancom Poskytovateľa sa im zruší možnosť pripojenia, prípadne so ohľadom na okolnosti stanovisko môže byť vydané súbežne so schválením plánovaného servisného zásahu.
- Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
- Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
- Poskytovateľ musí zabezpečiť, že všetky zariadenia, ktoré používa na vzdialené prihlasovanie sa do siete NDS, sú pravidelne aktualizované a udržiavané v bezpečnom stave. To zahŕňa pravidelné nainštalovanie bezpečnostných aktualizácií, opráv a záplat od výrobcov zariadení a dodávateľov softvéru. Okrem toho musí dodávateľ implementovať a dodržiavať bezpečnostné postupy a štandardy, aby sa minimalizovalo riziko zneužitia alebo kompromitácie týchto zariadení a zabezpečilo sa, že ich použitie neohrozí bezpečnosť našej siete.
- Zákaz používania neoverených pripojení: Servisná organizácia musí mať povolenie používať iba overené a dôveryhodné pripojenia na internet. Používanie hot spot pripojení by malo byť povolené iba v prípadoch, keď nie je k dispozícii iná možnosť pripojenia a iba po predchádzajúcom schválení NDS a zástupcov Odboru riadenia bezpečnosti NDS.
- Zákaz používania externých médií. Servisný technici Poskytovateľa nemajú povolené používať USB alebo externé pevné disky na prenášanie údajov, pokiaľ to nie je výslovne schválené a správne dokumentované v procese servisných činností.
- Poskytovateľ je povinný poskytnúť objednávateľovi bezpečnostnú dokumentáciu nastavenia a konfigurácie sieťovej komunikácie dotknutého informačného systému v rámci predmetu rámcovej dohody.
- Poskytovateľ je povinný poskytnúť objednávateľovi aktualizovanú bezpečnostnú dokumentáciu nastavenia a konfigurácie sieťovej komunikácie dotknutého informačného systému v rámci predmetu tejto rámcovej dohody pri akejkoľvek významnej zmene informačných systémov technologického vybavenia podľa čl. 1 bodu 1.1 rámcovej dohody, ktorá má vplyv na kybernetickú bezpečnosť týchto informačných systémov technologického vybavenia systému.

#### 9. Bezpečnostné opatrenia – zaznamenávanie udalosti a monitorovania

- Poskytovateľ je povinný vytvárať prevádzkové záznamy a zaznamenávať najmenej
  - aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií ( ak sú takéto informácie spracúvané technológiou v zmysle predmetu zákazky) a údajov alebo ďalších informačných aktív s nimi spojených,
  - iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,



- pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla,
- automatické varovné alebo chybové hlásenia systémov,
- detegované podozrivé alebo škodlivé aktivity.
- Prevádzkové záznamy sú zabezpečené najmenej tak, že
  - sú čitateľné výlučne osobám povereným ich analýzou,
  - zamedzujú možnosti prepísania alebo vymazania záznamu,
  - záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete,
  - sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

#### 10. Bezpečnostné opatrenia – riešenie kybernetických bezpečnostných incidentov ( prevenčné opatrenia v čase plnenia predmetu zákazky) (ďalej len „KBI“).

- Oboznámenie sa s postupmi NDS pri riešení KBI.
- Predchádzať vzniku incidentov dodržiavaním opatrení definovaných v tejto prílohe,
- Informovať NDS o každom podozrení na kybernetický bezpečnostný incident a o kybernetickom bezpečnostnom incidente ak bude mať o ňom vedomosť a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.
- V prípade výskytu podozrivých udalostí v čase plnenia mimoriadneho servisných činností, požaduje NDS analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb NDS.
- Poskytovateľ je povinný v čase prípadného incidentu v čase poskytovania predmetu rámcovej zmluvy poskytnúť súčinnosť pri zabezpečovaní dôkazov, ktoré budú slúžiť na objasnenie vzniku a riešenia kybernetického bezpečnostného incidentu. Poskytovateľ je povinný oznámiť NDS skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
- Pri riešení incidentu je Poskytovateľ povinný spolupracovať s NDS, Národným bezpečnostným úradom a na tento účel im poskytnúť potrebnú súčinnosť a všetky získané informácie, ktoré by mohli byť dôležité pre riešenie incidentu.

#### 11. Spôsob hlásenia bezpečnostného incidentu

- Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v prílohe č. 1 tejto Zmluvy a postupom a cez kontakty uvedené v prílohe č. 4 „Poriadku o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“, ktorý bude Poskytovateľovi Objednávateľom poskytnutý.
- Samotný spôsob a forma hlásenia bezpečnostného incidentu sa bude riadiť platným predpisom NDS – „Poriadok o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“.

#### 12. Bezpečnostné opatrenia- všeobecné

- Poskytovateľ/Zhotoviteľ je povinný poskytnúť súčinnosť Objednávateľa pri zabezpečovaní opatrení pre oblasť riadenia rizík a aktív, a to:
  - Odovzdanie evidencie aktív a komponentov vo formáte určenom Objednávateľom,
  - Poskytnutie súčinnosti pri technickom vykonávaní kompletnej inventarizácie všetkých aktív v čase prevádzky systému Poskytovateľom/Zhotoviteľom pre Objednávateľa,



- Zabezpečiť pravidelnú údržbu a aktualizácie technických zariadení a softvérov v zmysle hlavného zmluvného vzťahu,
- Poskytovateľ/Zhotoviteľ musí prispôbiť opatrenia na základe spätnej väzby od Objednávateľa a výsledkov hodnotení rizík v súlade s postupmi pre zmenové požiadavky definovanými hlavnou zmluvou,
- Objednávateľ s Poskytovateľom/Zhotoviteľom musí pravidelne revidovať a aktualizovať opatrenia na riadenie rizík a ochranu aktív v súlade so zmenami v prostredí a novými hrozbami.



Výkon servisnej činnosti a opráv technologického vybavenia rýchlostnej cesty v úsekoch R2 Žiar nad Hronom – obchvat, R2 Zvolen, východ – Pstruša a R2 Pstruša - Kriváň

**Príloha č. 3:**

**Záznam o kybernetickom bezpečnostnom incidente**

Záznam o kybernetickom bezpečnostnom incidente				
Názov bezpečnostného incidentu:				Číslo bezpečnostného incidentu: (Vyplní NDS)
Dátum a čas vzniku bezpečnostného incidentu:	Dátum a čas hlásenia bezpečnostného incidentu:			
Bezpečnostný incident nahlásil:	Funkcia a osobné číslo:			
Útvar/úsek/spoločnosť:	Telefonický kontakt:	Email:		
Bezpečnostný incident zaevidoval:	Funkcia a osobné číslo:			
Dotknutá základná služba(príp. objekt) :				
Dotknuté IS a riadiace systémy:				
Popis incidentu:				
Dotknutý útvar:	Odhadovaný dopad: (Vyplní NDS)		Vyberte položku.	
Kategória bezpečnostného incidentu: (Vyplní NDS)	Vyberte položku.	Vstup/Spôsob hlásenia:		
Hlásenie incidentu do JISKB NBÚ SR (Vyplní NDS)	Číslo: Forma hlásenia (rozhranie JISKB, email): Popis dotknutej základnej služby:			



Výkon servisnej činnosti a opráv technologického vybavenia rýchlostnej cesty v úsekoch R2 Žiar nad Hronom – obchvat, R2 Zvolen, východ – Pstruša a R2 Pstruša - Kriváň

Popis a vyčíslenie možného dopadu: <b>(Vyplní NDS)</b>			
Popis vyšetrovania incidentu: <b>(Vyplní dodávateľ aj NDS)</b>			
Druh bezpečnostného incidentu:	Vyberte položku.  Iné (uviesť):	Typ bezpečnostného incidentu:	Vyberte položku.  Iné (uviesť):
Popis prijatých/navrhovaných opatrení: <b>(Vyplní dodávateľ aj NDS)</b>			
Opatrenie:	Popis opatrenia:	Útvar/osoba zodpovedná za riešenie:	Termín splnenia:
Poznámky:			
Zoznam príloh:			



Výkon servisnej činnosti a opráv technologického vybavenia rýchlostnej cesty v úsekoch R2 Žiar nad Hronom – obchvat, R2 Zvolen, východ – Pstruša a R2 Pstruša - Kriváň

<b>Podpisy zodpovedných osôb:</b>	<b>Hlásenie o KBI podal:</b>  <b>Hlásenie o KBI prijal:</b>  <b>Navrhované opatrenia schválil:</b>
-----------------------------------	--