Rámcová zmluva o poskytovaní služieb

uzatvorená podľa ust. § 269 ods. 2 zákona č. 513/1991 Zb.
Obchodný zákonník v znení neskorších predpisov
(ďalej len „**Zmluva**“)

Číslo zmluvy:

Železničná spoločnosť Cargo Slovakia, a.s. Sídlo: Tomášikova 28B, 821 01 Bratislava, Slovenská republika IČO: 35 914 921 DIČ: 2021920065 IČ DPH: IBAN: BIC: Zápis v OR: Mestský súd Bratislava III, oddiel: Sa, vložka číslo: 3496/B konajúca prostredníctvom: Ing. Jaroslav Daniška - predseda predstavenstva a generálny riaditeľ a Mgr. Matej Hambálek, MBA - podpredseda predstavenstva a riaditeľ úseku služieb (ďalej len „**ZSSK CARGO**“)	**..** Sídlo: .... IČO: .... DIČ: .... IČ DPH: .... IBAN: .... BIC: .... Zápis v OR: .... súd ...., oddiel: ...., vložka číslo: .... konajúca prostredníctvom: .... - .... (ďalej len „**Poskytovateľ**“)
Predmet Zmluvy: Predmetom tejto Zmluvy je záväzok Poskytovateľa poskytovať ZSSK CARGO na základe písomných objednávok služby spočívajúce v Business Impact Analysis (BIA) a Business Continuity Management (BCM) (ďalej len „**Služba/Služby**“) a záväzok ZSSK CARGO zaplatiť Poskytovateľovi za riadne poskytnuté služby dohodnutú odmenu (cenu). Detailná špecifikácia Služieb s uvedením cien je uvedená v prílohe č. 2 tejto Zmluvy.	**Celkový finančný objem: ....,- EUR bez DPH** (cenník služieb s uvedením jednotkových cien za jednotlivé plnenia je obsiahnutý v prílohe č. 2 tejto Zmluvy) **Termín/lehota poskytnutia Služby:** v zmysle Objednávky **Miesto poskytovania Služby:** Železničná spoločnosť Cargo Slovakia, a. s. Tomášikova 28B 821 01 Bratislava
Kontaktná osoba ZSSK CARGO: Ing. Juraj Ďuriš - Riaditeľ sekcie ICT tel: e-mail:	**Kontaktná osoba Poskytovateľa** (v rozsahu meno, priezvisko, funkcia, tel. číslo, e-mail):

Táto Zmluva sa uzatvára na dobu určitú, a to na dobu 12 mesiacov odo dňa nadobudnutia platnosti tejto Zmluvy.

Táto Zmluva nadobúda platnosť dňom jej podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR v zmysle ust. §47a ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov v spojení s ust. § 5a ods. 2 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Táto Zmluva sa riadi Všeobecnými obchodnými podmienkami spoločnosti Železničná spoločnosť Cargo Slovakia, a.s. pre Rámcové zmluvy o poskytovaní služieb (ďalej len „**VOP**“), ktoré tvoria prílohu č. 1 tejto Zmluvy, a ktoré sú zverejnené na webovom sídle Kupujúceho a to na *https://www.zscargo.sk/o-nas/obstaravanie-a-nakup*. Poskytovateľ podpisom tejto Zmluvy vyhlasuje, že s obsahom VOP sa pri podpise tejto Zmluvy riadne oboznámil a s úpravou práv a povinností z nich vyplývajúcou v celom rozsahu súhlasí, čo podpisom tejto Zmluvy potvrdzuje.

Neoddeliteľnou súčasťou tejto Zmluvy je *Špecifikácia Služby/Služieb* s uvedením jednotkových cien za jednotlivé plnenia v rámci poskytovania Služby/Služieb a určením lehôt/termínov na poskytnutie Služby/Služieb, ktorá tvorí prílohu č. 2 tejto Zmluvy.

Neoddeliteľnou súčasťou tejto Zmluvy je *Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností*, ktorá tvorí prílohu č. 3 tejto Zmluvy.

Zmluvné strany podpisom tejto Zmluvy vyhlasujú, že si ju spolu s jej prílohami pred podpisom riadne prečítali, jej obsahu porozumeli a na dôkaz súhlasu s obsahom práv a povinností z nej vyplývajúcich (vrátane všetkých jej príloh) ju prostredníctvom osôb oprávnených konať v ich mene podpísali. Zmluvné strany svojim podpisom zároveň potvrdzujú, že táto Zmluva bola dojednaná v súlade so zásadami poctivého obchodného styku.

Táto Zmluva je vyhotovená v dvoch vyhotoveniach, pričom každá zo Zmluvných strán obdrží jedno vyhotovenie.

Železničná spoločnosť Cargo Slovakia, a.s. V Bratislave, dňa:		**...........................** V ...., dňa:
.... **Ing. Jaroslav Daniška** predseda predstavenstva a generálny riaditeľ	.... **Mgr. Matej Hambálek, MBA** podpredseda predstavenstva a riaditeľ úseku služieb	.... Meno a funkcia:

Príloha č. 2 Rámcovej zmluvy o poskytovaní služieb č. .... – Špecifikácia Služby):

Predmetom zmluvy je komplexná analýza vplyvov na prevádzku (Business Impact Analysis - BIA) a návrh a vypracovanie plánov riadenia kontinuity prevádzky (Business Continuity Management - BCM).

ZSSK CARGO je prevádzkovateľom základnej služby (PZS) v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov (ZoKB) a subjektom hospodárskej mobilizácie. ZSSK CARGO je v registri vedenom Národným bezpečnostným úradom zapísaný prevádzkovateľ kritickej základnej služby nie je kritickým subjektom podľa zákona č. 367/2024 Z. z. o kritickej infraštruktúre. Toto zaradenie je záväzné pre celý rozsah plnenia, pretože od neho závisia identifikačné kritériá závažného narušenia fungovania (30 minút, resp. 60 minút pre prevádzkovateľa kritickej základnej služby oproti 60 minútam, resp. 180 minútam pre prevádzkovateľa základnej služby podľa prílohy č. 1 k vyhláške č. 226/2025 Z. z.) aj relevancia jednotlivých bezpečnostných opatrení podľa prílohy č. 1 k vyhláške č. 227/2025 Z. z.

2. Hlavné ciele projektu

a) Identifikácia a kategorizácia kritických procesov prevádzky, podporných procesov a ich závislostí.

b) Zosúladenie s legislatívnymi požiadavkami na kontinuitu činností v zmysle zákona č. 69/2018 Z. z. a vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach.

c) Stanovenie striktných parametrov obnovy (RTO, RPO, MTPD) - v zákonnej terminológii cieľovej doby obnovy a cieľového bodu obnovy podľa § 5 ods. 2 vyhlášky č. 227/2025 Z. z. - s ohľadom na bezpečnosť prevádzky (Safety) a kybernetickú bezpečnosť (Security).

d) Vytvorenie auditovateľného a testovateľného BCM rámca vrátane havarijných plánov (DRP) a plánov kontinuity (BCP) pre scenáre kybernetických útokov, výpadkov kritických technológií, energetického blackoutu či fyzickej sabotáže.

e) Zosúladenie výstupov s bezpečnostným plánom podľa zákona č. 367/2024 Z. z. o kritickej infraštruktúre a s krízovým plánom hospodárskej mobilizácie podľa § 5 písm. a) zákona č. 179/2011 Z. z. tak, aby nevznikli paralelné a vzájomne nekonzistentné krízové dokumenty.

3. Legislatívny, normatívny a sektorový rámec

Poskytovateľ je povinný pri realizácii plne rešpektovať a do výstupov implementovať požiadavky nasledujúcich predpisov a noriem:

3.1 Slovenská legislatíva a sektorové predpisy

a) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ZoKB), ktorého transpozičná novela č. 366/2024 Z. z. (smernica NIS2) nadobudla účinnosť 1. 1. 2025 a ktorý bol následne ďalej novelizovaný (naposledy zákonom č. 67/2026 Z. z.); uchádzač vychádza zo znenia účinného ku dňu vyhlásenia tejto zákazky - primárne § 20 (Bezpečnostné opatrenia), § 24 (hlásenia), § 29 (audit kybernetickej bezpečnosti) a § 3 (vymedzenie pojmov) a súvisiace prílohy.

b) Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach - so špecifickým zameraním na opatrenia pre riadenie kontinuity činností a na zvládanie kybernetických bezpečnostných incidentov (príloha č. 1 k vyhláške, podľa § 20 ods. 2 zákona). Táto vyhláška nahradila pôvodnú vyhlášku č. 362/2018 Z. z. Príloha č. 1 rozlišuje relevanciu jednotlivých opatrení pre prevádzkovateľa základnej služby a pre prevádzkovateľa kritickej základnej služby, a to samostatne pre informačné a komunikačné technológie a pre operačné technológie; Poskytovateľ je povinný pracovať s tým stĺpcom relevancie, ktorý zodpovedá zaradeniu ZSSK CARGO.

c) Vyhláška NBÚ č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach - identifikačné kritériá závažného narušenia fungovania prevádzkovateľa základnej služby (príloha č. 1) a náležitosti hlásenia závažného kybernetického bezpečnostného incidentu podľa § 24 zákona. Táto vyhláška nahradila pôvodnú vyhlášku č. 165/2018 Z. z.

d) Zákon č. 513/2009 Z. z. o dráhach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákon č. 514/2009 Z. z. o doprave na dráhach v znení neskorších predpisov.

e) Zákon č. 179/2011 Z. z. o hospodárskej mobilizácii a o zmene a doplnení zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov (postavenie ZSSK CARGO ako subjektu hospodárskej mobilizácie).

f) Bezpečnostné smernice a predpisy podľa presnej špecifikácie V ZSSK CARGO.

g) Zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov (transpozícia smernice (EÚ) 2022/2557), účinný od 1. 1. 2025, ktorý zrušil zákon č. 45/2011 Z. z. - najmä povinnosti kritického subjektu pri zabezpečovaní odolnosti a kontinuity poskytovania základnej služby, bezpečnostný plán a oznamovanie incidentov ústrednému orgánu. ZSSK CARGO pred vyhlásením zákazky doplní aktuálny stav svojho určenia ako kritického subjektu a lehoty, ktoré z tohto určenia plynú.

h) Zákon Národnej rady SR č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení neskorších predpisov, zákon č. 129/2002 Z. z. o integrovanom záchrannom systéme v znení neskorších predpisov a zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov.

i) Predpisy o bezpečnosti železničnej dopravy, najmä smernica (EÚ) 2016/798 o bezpečnosti železníc
a nariadenie Komisie (EÚ) 2018/762, ktorým sa stanovujú spoločné bezpečnostné metódy týkajúce sa požiadaviek na systém riadenia bezpečnosti; BIA musí mať definované rozhranie na existujúci systém riadenia bezpečnosti ZSSK CARGO. Aplikovateľnosť týchto predpisov ZSSK CARGO potvrdí pred vyhlásením zákazky.

3.2 Európska legislatíva

a) Smernica (EÚ) 2022/2555 (NIS2) - transponovaná do národnej legislatívy zákonom č. 366/2024 Z. z., najmä v oblasti riadenia rizík dodávateľského reťazca a hlásenia incidentov.

b) Smernica (EÚ) 2022/2557 (CER) o odolnosti kritických subjektov (sektor dopravy) - transponovaná zákonom č. 367/2024 Z. z.

c) Nariadenie (EÚ) 2016/679 (GDPR) - v kontexte dostupnosti osobných údajov zamestnancov a zákazníkov pri krízovom režime; v národnej úprave zákon č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

3.3 Medzinárodné normy a best practices

a) ISO 22301 - Security and resilience - Business continuity management systems - Requirements.

b) ISO/IEC 27001 a ISO/IEC 27002 - Riadenie informačnej a kybernetickej bezpečnosti.

c) ISO 22317 (analýza vplyvov na činnosť organizácie), ISO 22313 (návod na uplatňovanie ISO 22301), ISO/IEC 27031 (pripravenosť IKT na kontinuitu činností) a ISO 22398 (cvičenia).

d) IEC 62443 - bezpečnosť priemyselných automatizačných a riadiacich systémov, pre prostredie operačných technológií.

4. Rozsah požadovaných prác pre Business Impact Analysis (BIA)

Poskytovateľ navrhne metodiku a zrealizuje BIA, ktorá musí explicitne pokrývať špecifické prostredie prevádzkovateľa základnej služby (PZS). BIA sa na účely tejto zákazky považuje za analýzu funkčného vplyvu podľa § 5 ods. 2 vyhlášky č. 227/2025 Z. z., ktorá je súčasťou riadenia rizík; jej výstupy musia byť použiteľné ako súčasť bezpečnostnej dokumentácie podľa § 4 tej istej vyhlášky.

4.1 Procesná analýza a mapovanie závislostí

a) Identifikácia a kategorizácia kritických prevádzkových procesov.

b) Mapovanie závislostí kritických procesov na podporných systémoch a aktívach:

1. Informačné systémy (IT).
2. Ľudské zdroje: kritické roly a ich zastupiteľnosť.
3. Tretie strany: externí dodávatelia údržby, telekomunikační operátori, dodávatelia energií.
4. Operačné technológie (OT): so zaradením komponentov do vrstiev 0 až 5 podľa vysvetliviek
k prílohe č. 1 vyhlášky č. 227/2025 Z. z. (dispečerské riadenie a zber dát a rozhranie človek-stroj sú vrstvou 2, programovateľné logické automaty vrstvou 1), keďže časť bezpečnostných opatrení je relevantná len pre vrstvu 3 a vyššiu.

4.2 Analýza vplyvov a stanovenie kritických parametrov

Vyhodnotenie dopadov prerušenia činností v čase. Okrem štandardných finančných a právnych dopadov sa vyžaduje prioritné vyhodnotenie:

a) Dopad na bezpečnosť (Safety): riziko ohrozenia života a zdravia zamestnancov a tretích osôb v dôsledku zlyhania technológií.

b) Dopad na kontinuitu kritickej infraštruktúry štátu: paralyzovanie logistických reťazcov, dopad na medzinárodné koridory.

c) Regulačný dopad v zmysle ZoKB: pokuty za porušenie povinností PZS, povinnosť hlásenia závažných kybernetických bezpečnostných incidentov podľa § 24 ZoKB a vyhlášky č. 226/2025 Z. z.

d) Kvantifikácia parametrov: stanovenie RTO (Recovery Time Objective), RPO (Recovery Point Objective), MTPD (Maximum Tolerable Period of Disruption) a MBCO (Minimum Business Continuity Objective) pre každú základnú službu a kritický proces. RTO a RPO sa v dokumentácii označia aj zákonnými pojmami cieľová doba obnovy a cieľový bod obnovy podľa § 5 ods. 2 vyhlášky č. 227/2025 Z. z.; MTPD a MBCO sú pojmy normy ISO 22301 bez zákonného ekvivalentu a použijú sa ako doplňujúce parametre.

e) Stanovené hodnoty MTPD a RTO nesmú byť v rozpore s identifikačnými kritériami závažného narušenia fungovania podľa prílohy č. 1 k vyhláške č. 226/2025 Z. z. pre kategóriu, do ktorej je ZSSK CARGO zaradený.

4.3 Požadované výstupy BIA

a) Metodika BIA prispôsobená pre sektor dopravy, schválená Manažérom kybernetickej bezpečnosti ZSSK CARGO; metodika musí obsahovať preukázateľné mapovanie na úrovne rizika podľa bezpečnostnej metodiky zverejnenej na webovom sídle Národného bezpečnostného úradu (§ 5 ods. 1 písm. c) vyhlášky č. 227/2025 Z. z.).

b) Katalóg procesov a služieb s priradenou úrovňou kritickosti; úrovne kritickosti musia byť mapované na klasifikačnú schému podľa prílohy č. 2 k vyhláške č. 227/2025 Z. z..

c) Komplexná mapa závislostí (proces → aplikácia → OT technológia → infraštruktúra → Poskytovateľ)
s uvedením vrstvy operačných technológií (0 - 5) pre každý komponent a s väzbou na evidenciu aktív podľa § 6 vyhlášky č. 227/2025 Z. z. (primárne a podporné aktíva, vlastníci aktív).

d) BIA Záverečná správa (BIA Report) pripravená na predloženie pre účely auditu kybernetickej bezpečnosti podľa § 29 ZoKB.

5. Rozsah požadovaných prác pre BCM

5.1 Návrh BCM rámca a riadenia (governance)

a) Vypracovanie Politiky riadenia kontinuity činností v plnom súlade s požiadavkami na riadenie kontinuity činností podľa vyhlášky NBÚ č. 227/2025 Z. z. (príloha č. 1, podľa § 20 ods. 2 zákona).

b) Definovanie organizačnej štruktúry krízového riadenia (Krízový štáb, BCM tím, tím na manažment incidentov) vrátane presných rolí, zodpovedností a zastupiteľnosti.

c) Návrh eskalačných procedúr v prípade kybernetického útoku (prepojenie na ústredný orgán a národnú jednotku CSIRT - Národné centrum kybernetickej bezpečnosti SK-CERT). Hlásenie závažného kybernetického bezpečnostného incidentu sa podľa § 24 ZoKB podáva Národnému bezpečnostnému úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, a to vo viacstupňovom režime (včasné varovanie, hlásenie incidentu, záverečná správa); konkrétne lehoty Poskytovateľ prevezme z aktuálneho znenia § 24 ZoKB a náležitosti z príloh č. 2 a č. 3 vyhlášky č. 226/2025 Z. z. Eskalačné procedúry musia zohľadniť aj paralelnú oznamovaciu povinnosť podľa zákona č. 367/2024 Z. z., ak je ZSSK CARGO kritickým subjektom.

d) Zosúladenie BCM rámca s bezpečnostným plánom podľa zákona č. 367/2024 Z. z. a s krízovým plánom hospodárskej mobilizácie podľa § 5 písm. a) zákona č. 179/2011 Z. z. vrátane väzby na jednotný informačný systém hospodárskej mobilizácie; duplicitné alebo protichodné postupy sú neprípustné.

5.2 Strategický návrh kontinuity a scenáre obnovy

Návrh stratégií obnovy a obchádzkových riešení (workarounds) pre špecifické krízové scenáre:

a) Scenár „Kybernetický útok“: ransomvérový útok ochromujúci IT systémy.

b) Scenár „Blackout“: dlhodobý výpadok dodávky elektrickej energie.

c) Scenár „Výpadok kľúčového dodávateľa“: výpadok údržby a podpory pre kritické systémy.

d) Scenár „Kombinované ohrozenie“: kybernetický útok vedený súbežne s fyzickou sabotážou, prípadne v období krízovej situácie podľa zákona č. 179/2011 Z. z.

5.3 Vypracovanie havarijných plánov a plánov obnovy

a) Plány kontinuity činností (BCP): návody pre business zložky, ako prevádzkovať nákladnú železničnú dopravu v obmedzenom/manuálnom režime (degradovaný mód) pri výpadku systémov.

b) Plány obnovy po havárii (DRP): technické postupy pre personál na obnovu integrity systémov, sietí a dát zo záloh po kybernetickom incidente.

c) Plány krízovej komunikácie: postupy pre informovanie verejnosti, štátnych orgánov (ústredný orgán, Národné centrum kybernetickej bezpečnosti SK-CERT, CSIRT.SK, MINDOP), zamestnancov a zložiek Integrovaného záchranného systému.

5.4 Návrh testovania, vzdelávania a cvičení

a) Vytvorenie Ročného plánu testovania BCM (plán musí pokrývať najmenej tie testy, ktoré príloha č. 1 k vyhláške č. 227/2025 Z. z. vyžaduje vykonávať aspoň raz ročne so záznamom, najmä plánovanie a testovanie riešenia kybernetických bezpečnostných incidentov podľa položky 20, testovanie pravidiel izolácie kritických komponentov podľa položky 26, testovanie záložných kópií dát, softvéru a konfigurácií podľa položky 28 a pri operačných technológiách prevádzkovateľa kritickej základnej služby kontrolu funkčnosti záloh aspoň dvoch rôznych systémov podľa položky 34. O každom teste sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia. Testovanie plánov kontinuity ako takých vychádza z položky 27 prílohy č. 1 a z normy ISO 22301, ktorá frekvenciu neurčuje číselne).

b) Príprava a realizácia Tabletop cvičenia (simulácia ransomvérového útoku a výpadku kritického IT systému); súčasťou plnenia je vyhodnotenie cvičenia a preukázateľné zapracovanie zistení do BCP a DRP.

6. Požiadavky na spôsob spracovania a metodiku

6.1 Metodické a procesné požiadavky

a) Auditovateľnosť a trasovateľnosť: všetky závery v BIA a BCM musia byť preukázateľne podložené (napr. záznamom z workshopu, konkrétnou legislatívnou požiadavkou). Výstupy budú slúžiť ako kľúčový dôkazový materiál pri audite kybernetickej bezpečnosti.

b) Eliminácia prevádzkovej slepoty: Poskytovateľ musí viesť workshopy tak, aby identifikoval reálne (nie len teoretické) riziká a závislosti, so zreteľom na kombinované riziká (napr. kybernetický útok vedený súbežne s fyzickou sabotážou).

c) Jednotná terminológia: dôsledné uplatňovanie pojmov definovaných v § 3 zákona č. 69/2018 Z. z. a v § 2 a § 5 vyhlášky č. 227/2025 Z. z. (najmä aktívum, primárne aktívum, podporné aktívum, analýza funkčného vplyvu, cieľová doba obnovy, cieľový bod obnovy) a norme ISO 22301.

6.2 Požiadavky na dokumentáciu

a) Všetky dokumenty musia byť dodané v slovenskom jazyku, v editovateľnej podobe (MS Office - DOCX, XLSX) a finálne verzie v PDF.

b) Procesné mapy a diagramy závislostí musia byť dodané vo formáte MS Visio (VSDX) alebo ekvivalentnom vektorovom formáte.

c) Dokumentácia musí podliehať prísnemu riadeniu verzií (version control) s jasným sledovaním zmien, autorstva a schvaľovateľov.

7. Bezpečnostné požiadavky na Poskytovateľa (NDA)

Vzhľadom na to, že Poskytovateľ príde do styku s informáciami o kritickej infraštruktúre štátu a detailnou architektúrou informačných a riadiacich systémov PZS, platia tieto podmienky:

a) Dohoda o mlčanlivosti (NDA): podpísanie prísnej NDA pred začatím akýchkoľvek prác, a to na úrovni spoločnosti aj jednotlivých členov tímu; dohody o mlčanlivosti sa preskúmavajú a podpisujú najmenej raz za dva roky v súlade s položkou 71 prílohy č. 1 k vyhláške č. 227/2025 Z. z..

b) Bezúhonnosť: ZSSK CARGO si vyhradzuje právo požadovať výpis z registra trestov (nie starší ako 3 mesiace) pre všetkých členov realizačného tímu.

c) Bezpečnostná previerka (AK RELEVANTNÉ): ZSSK CARGO si vyhradzuje právo požadovať, aby vybraní experti boli oprávnenými osobami na oboznamovanie sa s utajovanými skutočnosťami v zmysle zákona č. 215/2004 Z. z. v znení neskorších predpisov, a to pre stupeň utajenia „Vyhradené“ na základe určenia vedúcim po vyhodnotení bezpečnostnej previerky I. stupňa podľa § 31 tohto zákona (pre tento stupeň Národný bezpečnostný úrad osvedčenie nevydáva), alebo pre stupeň utajenia „Dôverné“ a vyšší na základe platného osvedčenia Národného bezpečnostného úradu. Ak by Poskytovateľ ako právnická osoba mal prijímať, vytvárať alebo uchovávať utajované skutočnosti, vyžaduje sa aj platné potvrdenie o priemyselnej bezpečnosti; s ohľadom na lehoty jeho získania ZSSK CARGO pred vyhlásením zákazky posúdi, či je možné utajované skutočnosti z rozsahu plnenia vylúčiť.

d) Bezpečné nakladanie s dátami: Poskytovateľ nesmie ukladať dáta a dokumentáciu ZSSK CARGO na neschválené cloudové úložiská. Výmena súborov bude prebiehať výhradne cez zabezpečený kanál definovaný ZSSK CARGO (napr. šifrovaná VPN, dedikované on-premise úložisko). Po ukončení projektu je Poskytovateľ povinný vykonať bezpečný skart/výmaz všetkých kópií dát.

e) Zmluva podľa § 19 ods. 2 ZoKB: Poskytovateľ sa na účely tejto zákazky považuje za tretiu stranu s významným vplyvom, preto sa okrem NDA uzatvára zmluva podľa § 19 ods. 2 ZoKB s povinným obsahom podľa § 7 ods. 2 vyhlášky č. 227/2025 Z. z. (záväzok dodržiavať bezpečnostné politiky ZSSK CARGO, súhlas s nimi, rozsah a spôsob vykonávania kontrolných činností a auditu u tretej strany, povinnosť informovať o kybernetickom bezpečnostnom incidente a poskytnúť súčinnosť pri jeho riešení). Uzatvoreniu zmluvy predchádza analýza rizík dodávateľských služieb podľa položiek 145 až 148 prílohy č. 1 k tej istej vyhláške. ZSSK CARGO môže vychádzať zo vzoru zmluvy zverejneného na webovom sídle Národného bezpečnostného úradu.

f) Nezávislosť a konflikt záujmov: Poskytovateľ ani osoby patriace do tej istej hospodárskej skupiny nesmú u ZSSK CARGO vykonávať audit kybernetickej bezpečnosti podľa § 29 ZoKB, ktorého predmetom by boli výstupy tejto zákazky, a to po dobu 24 mesiacov od odovzdania diela.

8. Akceptačné kritériá výstupov

Každý odovzdaný dokument/výstup bude posudzovaný Akceptačnou komisiou ZSSK CARGO (vrátane Manažéra kybernetickej bezpečnosti). Výstupy budú akceptované, len ak splnia:

1. Úplnosť a súlad: plný súlad s požiadavkami na riadenie kontinuity činností podľa vyhlášky NBÚ č. 227/2025 Z. z. a normy ISO 22301, pričom výstup obsahuje maticu súladu s uvedením konkrétnych položiek prílohy č. 1 k vyhláške a príslušného stĺpca relevancie (PZS/PKZS, IKT/OT), ktoré daný výstup pokrýva.

2. Uplatniteľnosť v praxi: odmietnuté budú čisto teoretické alebo generické texty (tzv. „vzorové šablóny“), ktoré nereflektujú reálny stav a technológie ZSSK CARGO.

3. Technická obhájiteľnosť: hodnoty RTO a RPO uvedené v BCM plánoch musia byť technicky realizovateľné vzhľadom na stav infraštruktúry (overené IT/OT expertom); ak požadované hodnoty nie sú pri súčasnom stave infraštruktúry dosiahnuteľné, výstup musí obsahovať gap analýzu a plán opatrení na ich dosiahnutie vrátane odhadu náročnosti a priorít.

4. Úspešné pripomienkové konanie: zapracovanie všetkých opodstatnených pripomienok ZSSK CARGO v stanovenom termíne.

Cenník

P. č.	**Pomenovanie**	**MJ**	**Počet v MJ**	**Cena za MJ v EUR bez DPH**
1.	Business Impact Analysis (BIA) a Business Continuity Management (BCM)	služba	1	
Cena celkom				

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená podľa § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov medzi

1./	**Železničná spoločnosť Cargo Slovakia, a.s.**
Sídlo:	Tomášikova 28B, 821 01 Bratislava
Zapísaná:	Obchodný register Mestského súdu Bratislava III oddiel: Sro, vložka č. 3496/B
IČO:	35 914 921
DIČ:	
IČ DPH:	
Konajúca:	Ing. Jaroslav Daniška – predseda predstavenstva Mgr. Matej Hambálek, MBA – podpredseda predstavenstva

(ďalej len **„ZSSK CARGO“**)

a

2./	
Sídlo:	
Zapísaná:	
IČO:	
DIČ:	
IČ DPH:	
Konajúca:	

(ďalej len **„Partner“**)

(ZSSK CARGO a Partner ďalej spoločne ako **„Zmluvné strany“** alebo jednotlivo ako **„Zmluvná strana“**)

Článok I
Predmet Zmluvy

Predmetom tejto Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len **„Zmluva“**) je úprava podmienok a spôsobu zabezpečenia plnenia bezpečnostných opatrení podľa § 20 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“**), úprava povinností Zmluvných strán pri plnení notifikačných povinností stanovených Zákonom o kybernetickej bezpečnosti a vymedzenie ostatných práv a povinností Zmluvných strán s ohľadom na hlásenie a riešenie kybernetických bezpečnostných incidentov.

Článok II
Rozsah činnosti Partnera

(1) Partner ako dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou informačných systémov poskytuje ZSSK CARGO ako prevádzkovateľovi kritickej základnej služby činnosti súvisiace s Business Impact Analysis (BIA) a Business Continuity Management (BCM), a to na základe Rámcovej zmluvy o poskytovní služieb č. xxxxxxxxxxxxxxxxxxxx (ďalej len ako „Hlavná zmluva“).

(2) Špecifikácia bezpečnostných opatrení Partnera podľa tejto Zmluvy je špecifikovaná v Prílohe č. 1 k tejto Zmluve.

Článok III
Povinnosti Zmluvných strán

(1) ZSSK CARGO je povinná:

a) dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení prijatých ZSSK CARGO,

b) dodržiavať príslušné sektorové bezpečnostné opatrenia, ak sú prijaté,

c) dňom prevádzkovania novej základnej služby o tejto skutočnosti informovať Partnera a podnik na poskytovanie elektronických komunikačných služieb alebo sietí podľa zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov ku ktorému je sieť alebo informačný systém novej základnej služby pripojená,

d) informovať v nevyhnutnom rozsahu Partnera o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie tejto Zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak,

e) riešiť kybernetický bezpečnostný incident v súlade s príslušnými všeobecne záväznými právnymi predpismi,

f) bezodkladne oznámiť závažný kybernetický bezpečnostný incident v spôsobe a rozsahu stanovenými príslušnými všeobecne záväznými právnymi predpismi,

g) spolupracovať s Národným bezpečnostným úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

h) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,

i) oznámiť orgánom činným v trestnom konaní skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

j) prijímať a realizovať bezpečnostné opatrenia na základe schválenej bezpečnostnej dokumentácie,

k) vypracovať a aktualizovať bezpečnostnú dokumentáciu v súlade so Zákonom o kybernetickej bezpečnosti, oboznámiť Partnera s jej obsahom v rozsahu nevyhnutnom pre riadne plnenie jeho záväzkov vyplývajúcich z tejto Zmluvy a zabezpečiť, aby bezpečnostná dokumentácia bola počas celej doby trvania tejto Zmluvy aktuálna a zodpovedala reálnemu stavu,

l) hlásiť prostredníctvom jednotného informačného systému kybernetickej bezpečnosti každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov,

m) 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 a to len ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky,

n) poskytovať súčinnosť Národnému bezpečnostnému úradu a jednotke CSIRT pri riešení kybernetického incidentu,

o) bezodkladne oznámiť a preukázať Národnému bezpečnostnému úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok,

p) prijímať ochranné opatrenie na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu vypracovanej jednotkou CSIRT,

q) na výzvu Národného bezpečnostného úradu v určenej lehote predložiť navrhované ochranné opatrenie na schválenie,

r) preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom o kybernetickej bezpečnosti vykonaním auditu kybernetickej bezpečnosti podľa Zákona o kybernetickej bezpečnosti,

s) poskytovať súčinnosť Partnerovi pri plnení záväzkov vyplývajúcich z tejto Zmluvy,

t) zabezpečiť, aby všetky zmluvy uzatvorené s Partnerom, bez ohľadu na to, kedy boli uzatvorené, tvorili súčasť bezpečnostnej dokumentácie ZSSK CARGO,

u) plniť ďalšie povinnosti stanovené touto Zmluvou, Zákonom o kybernetickej bezpečnosti a osobitnými všeobecne záväznými právnymi predpismi príslušnými v oblasti kybernetickej bezpečnosti.

(2) Partner je povinný:

a) pri činnostiach, vykonávaných pre ZSSK CARGO podľa tejto Zmluvy a podľa Hlavnej zmluvy, dodržiavať bezpečnostné politiky ZSSK CARGO s ktorými bol Partner ku dňu podpisu tejto Zmluvy oboznámený a s ktorými podpisom tejto Zmluvy vyjadruje súhlas a plniť povinnosti vyplývajúce aj z bezpečnostnej dokumentácie ZSSK CARGO, s ktorou bol ku dňu podpisu tejto Zmluvy oboznámený; zoznam dokumentov tejto bezpečnostnej dokumentácie, s ktorou bol Partner oboznámený a zoznam dokumentov obsahujúcich špecifikáciu bezpečnostných politík, s ktorými bol Partner oboznámený, je uvedený v Prílohe č.2 k tejto Zmluve,

b) chrániť všetky informácie poskytnuté spoločnosťou ZSSK CARGO v súvislosti s plnením tejto Zmluvy, najmä, ale nie výlučne, informácie týkajúce sa bezpečnostnej politiky ZSSK CARGO a neposkytovať ich tretím stranám; Partner je oprávnený poskytnúť tieto informácie príslušným kontaktným osobám Partnera uvedeným v článku X ods. 1 tejto Zmluvy len na základe princípu *need-to-know*, t.j. v nevyhnutnom rozsahu,

c) prijímať a dodržiavať bezpečnostné opatrenia a plniť ostatné s tým súvisiace povinnosti podľa príslušných ustanovení článku V tejto Zmluvy,

d) bezodkladne informovať ZSSK CARGO o kybernetickom bezpečnostnom incidente v zmysle článku VII tejto Zmluvy a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a zároveň vykonať všetky opatrenia, ktorých účelom je zamedziť rozširovaniu kybernetického bezpečnostného incidentu a jeho následkov a informovať o týchto opatreniach ZSSK CARGO,
e) v prípade kybernetického bezpečnostného incidentu poskytovať súčinnosť ZSSK CARGO a to aj podľa pokynov Národného bezpečnostného úradu, ak takéto pokyny boli Národným bezpečnostným úradom udelené a podieľať sa na riešení bezpečnostného incidentu podľa bezpečnostných politík ZSSK CARGO a ostatných pokynov ZSSK CARGO,
f) po ukončení trvania tejto Zmluvy vrátiť ZSSK CARGO, previesť na ZSSK CARGO alebo zničiť všetky podklady a informácie, ku ktorým mal Partner počas trvania tejto Zmluvy prístup podľa odseku 3 tohto článku Zmluvy,
g) poskytnúť Národnému bezpečnostnému úradu na základe jeho žiadosti za účelom plnenia jeho úloh pri riešení kybernetického bezpečnostného incidentu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu,
h) poskytnúť ZSSK CARGO bezodkladne všetky podklady a informácie a súčinnosť nevyhnutnú k tomu, aby si ZSSK CARGO mohla riadne a včas plniť všetky povinnosti podľa odseku 1 tohto článku Zmluvy,
i) poskytnúť ZSSK CARGO potrebnú súčinnosť pri automatizovanom vyhodnocovaní výskytu kybernetického bezpečnostného incidentu a nahlasovaní kybernetického bezpečnostného incidentu, ak je takáto povinnosť uložená ZSSK CARGO Národným bezpečnostným úradom,
j) odstrániť všetky nedostatky určené Národným bezpečnostným úradom v zmysle § 27a Zákona v lehote určenej Národným bezpečnostným úradom,
k) plniť ďalšie povinnosti stanovené touto Zmluvou, Zákonom o kybernetickej bezpečnosti a príslušnými osobitnými všeobecne záväznými právnymi predpismi v oblasti kybernetickej bezpečnosti.
l) Partner súhlasí s tým, že bezpečnostná politika ZSSK CARGO sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov ZSSK CARGO a aktuálnym bezpečnostným rizikám a hrozbám týkajúcim sa Parrnera, ktoré by mohli mať potenciálny nepriaznivý vplyv na kvalitu, dostupnosť a bezpečnosť základnej služby ZSSK CARGO. ZSSK CARGO je povinné bezodkladne oboznámiť Partnera s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené
m) Partner vyhlasuje, že má potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role, opatrenia a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie účelu tejto zmluvy.
n) Partner je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť ZSSK CARGO v určenej lehote.
o) Zoznam zamestnancov Partnera, subdodávateľa Partnera a tretích osôb, ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa tejto zmluvy a ktorí

budú mať prístup k informáciám ZSSK CARGO (ďalej len „zoznam osôb“) sú uvedení v článku X Kontaktné osoby a droučovanie. Partner je povinný oznámiť ZSSK CARGO každú zmenu v zozname osôb podľa tohto bodu bezodkladne na mailovú adresu kontaktnej osoby ZSSK CARGO.

p) Partner je povinný písomne informovať ZSSK CARGO o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Partnerom na účely plnenia tejto zmluvy.

(3) Bezodkladne po ukončení tejto Zmluvy, najneskôr však do 5 pracovných dní, Partner predloží ZSSK CARGO sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča dát, ktoré s prihliadnutím na povahu informácií priamo alebo nepriamo súvisia s povinnosťami vyplývajúcich z tejto Zmluvy, zo Zákona o kybernetickej bezpečnosti alebo z osobitného všeobecne záväzného právneho predpisu v oblasti kybernetickej bezpečnosti a ktoré sa týkajú ZSSK CARGO. ZSSK CARGO na základe sumarizácie podľa predchádzajúcej vety písomne informuje Partnera o tom, ktoré podklady a informácie má Partner vrátiť ZSSK CARGO, previesť na ZSSK CARGO a ktoré má zničiť. Partner je povinný splniť si povinnosť podľa predchádzajúcej vety najneskôr do 5 pracovných dní odo dňa, kedy ZSSK CARGO informovala Partnera o spôsobe naloženia s týmito podkladmi a informáciami.

(4) Zmluvné strany sú povinné vzájomne si bezodkladne písomne oznámiť každú skutočnosť, ktorá má alebo môže mať vplyv na plnenie záväzkov podľa tejto Zmluvy, povinností podľa Zákona o kybernetickej bezpečnosti alebo osobitných všeobecne záväzných právnych predpisov v oblasti kybernetickej bezpečnosti alebo ktorá s nimi súvisí a to na všetky e-mailové adresy príslušnej Zmluvnej strany uvedené v článku X tejto Zmluvy.

Článok IV
Bezpečnostné opatrenia Zmluvných strán

(1) Zmluvné strany sa na základe vyhotovenej analýzy rizík dohodli, že príjmu bezpečnostné opatrenia, ktoré sú špecifikované v prílohe č. 1 tejto Zmluvy najneskôr do 15 dní po nadobudnutí účinnosti zmluvy.

(2) Zmluvné strany sa pri plnení záväzkov podľa odseku 1 tohto článku Zmluvy zaväzujú poskytovať si navzájom všetku potrebnú súčinnosť. V prípade, že niektorá zo Zmluvných strán nebude schopná všetky bezpečnostné opatrenia prijať najneskôr do termínu stanoveného v ods. 1 tohto článku Zmluvy, bude o tom bez zbytočného odkladu informovať druhú Zmluvnú stranu s uvedením termínu/lehoty dokedy tieto opatrenia prijme. V prípade nemožnosti alebo nehospodárnosti prijatia bezpečnostných opatrení v zmysle prílohy č. 1 tejto Zmluvy sa Zmluvné strany písomne dohodnú na prijatí náhradných riešení, ktoré svojim účelom a povahou čo najlepšie nahradia príslušné bezpečnostné opatrenia.

(3) Zmluvné strany berú na vedomie, že obsah bezpečnostných opatrení podľa tohto článku Zmluvy je ustanovený Vyhláškou NBÚ č. 362/2018 Z. z.

(4) ZSSK CARGO podpisom tejto Zmluvy vyhlasuje, že ku dňu podpisu tejto Zmluvy oboznámila Partnera s bezpečnostnou politikou ZSSK CARGO a bezpečnostnou dokumentáciou ZSSK CARGO a Partner podpisom tejto Zmluvy vyhlasuje, že sa s bezpečnostou politkou ZSSK CARGO a bezpečnostnou dokumentáciou ZSSK CARGO ku dňu podpisu tejto Zmluvy oboznámil. Zoznam dokumentov tejto bezpečnostnej dokumentácie, s ktorou bol Partner oboznámený a zoznam dokumentov obsahujúcich špecifikáciu bezpečnostných politík, s ktorými bol Partner oboznámený, je uvedený v Prílohe č.2 k tejto Zmluve.

Článok V
Špecifikácia a rozsah bezpečnostných opatrení Zmluvných strán

(1) Špecifikácia a rozsah bezpečnostných opatrení Zmluvných strán tvorí Prílohu č. 1 tejto Zmluvy.

(2) ZSSK CARGO je ako prevádzkovateľ základnej služby povinná najmä:

a) mať vypracovanú a schválenú bezpečnostnú dokumentáciu v súlade s príslušnými ustanoveniami Zákona o kybernetickej bezpečnosti a v súlade s príslušnými ustanoveniami Vyhlášky NBÚ č. 362/2018 Z. z. a zároveň je povinná ju v prípade potreby náležite aktualizovať tak, aby zodpovedala reálnemu stavu;
b) dodržiavať a prijať bezpečnostné opatrenia v zmysle B. časti Prílohy č. 1 tejto Zmluvy;
c) bezodkladne písomne informovať Partnera o akýchkoľvek zmenách bezpečnostných politík relevantných pre plnenia záväzkov Partnera a o ich obsahu;
d) bezodkladne písomne informovať Partnera o akýchkoľvek zmenách v rozsahu a špecifikácií ňou prijatých bezpečnostných opatrení.

(3) Partner je vo vzťahu k činnostiam, ktoré zabezpečuje pre ZSSK CARGO podľa Hlavnej zmluvy a tejto Zmluvy, povinný najmä:

a) dodržiavať bezpečnostnú politiku ZSSK CARGO, s ktorou bol pri podpise tejto Zmluvy oboznámený a o ktorej zmenách ho bude ZSSK CARGO informovať,
b) dodržiavať a prijať bezpečnostné opatrenia v špecifikácii a rozsahu stanovenom v časti A. Prílohy č. 1 k tejto Zmluve a tieto priebežne podľa potreby alebo písomných pokynov ZSSK CARGO aktualizovať alebo dopĺňať,
c) bezodkladne písomne oznámiť ZSSK CARGO zmenu v špecifikácií a rozsahu ním prijatých bezpečnostných opatrení týkajúcich sa výlučne činností pre ZSSKC CARGO podľa tejto Zmluvy a podľa Hlavnej zmluvy,
d) dodržiavať písomné pokyny ZSSK CARGO pri uplatňovaní bezpečnostných opatrení Partnera a bezpečnostných politík ZSSK CARGO a v prípade potreby (s ohľadom na povahu týchto pokynov) implementovať príslušné opatrenia alebo zmeny v existujúcich opatreniach vo svojej organizácii, a to v lehotách písomne dohodnutých s ZSSK CARGO.

(4) ZSSK CARGO je oprávnená:

a) dávať Partnerovi písomné pokyny týkajúce sa uplatňovania bezpečnostných opatrení Partnera podľa tejto Zmluvy a uplatňovania bezpečnostných politík ZSSK CARGO,
b) kontrolovať plnenie záväzkov Partnera podľa tejto Zmluvy a vykonať u Partnera bezpečnostný audit v oblasti plnenia zmluvných záväzkov vyplývajúcich z tejto Zmluvy v oblasti kybernetickej bezpečnosti vo vzťahu k informačným aktívam ZSSK CARGO podľa článku VIII tejto Zmluvy.

(5) Zmluvné strany berú na vedomie, že ZSSK CARGO je podľa Zákona o kybernetickej bezpečnosti povinná podrobovať sa auditu kybernetickej bezpečnosti a predložiť Národnému bezpečnostnému úradu záverečnú správu o výsledkoch tohto auditu. Partner sa v tejto súvislosti zaväzuje poskytnúť ZSSK CARGO všetku nevyhnutnú súčinnosť, ktorá bude z jeho strany potrebná pre riadne vykonanie auditu, a to podľa písomných požiadaviek ZSSK CARGO. V prípade, že sa na základe výsledkov auditu ukážu niektoré bezpečnostné opatrenia Zmluvných strán vyplývajúce z tejto Zmluvy ako nedostatočné alebo z výsledkov auditu vyplynú iné nedostatky, ktoré sa dotýkajú bezpečnostných opatrení na zabezpečenie činností podľa tejto Zmluvy, zaväzujú sa Zmluvné strany vo vzájomnej súčinnosti prijať a implementovať všetky nevyhnutné aktualizácie prijatých opatrení alebo doplniť bezpečnostné opatrenia v súlade so závermi obsiahnutými v záverečnej správe o výsledkoch auditu, a to na základe písomnej požiadavky ZSSK CARGO v lehotách písomne odsúhlasených oboma Zmluvnými stranami rešpektujúc lehoty stanovené NBÚ, príp. uzatvoriť dodatok k tejto Zmluve, ktorým sa príslušným spôsobom upraví / zmení /doplní úprava práv a povinností Zmluvných strán. Náklady na audit kybernetickej bezpečnosti znáša ZSSK CARGO v celom rozsahu, pokiaľ tieto náklady neznáša Národný bezpečnostný úrad. Ustanovenie tohto článku sa uplatňuje rovnako aj v prípade, ak bude v ZSSK CARGO vykonaný audit Národným bezpečnostným úradom alebo nariadený audit kybernetickej bezpečnosti zo strany Národného bezpečnostného úradu podľa § 29 ods. 6 Zákona o kybernetickej bezpečnosti.

(6) V prípade akýchkoľvek zmien v špecifikácii a rozsahu bezpečnostných opatrení podľa tohto článku Zmluvy, na ktorých sa Zmluvné strany dohodli, sa Zmluvné strany zaväzujú tieto zmeny reflektovať vo forme písomného dodatku k tejto Zmluve, ktorý Zmluvné strany uzatvoria najneskôr do 10 pracovných dní odo dňa doručenia oznámenia o návrhu zmien v špecifikácií a rozsahu bezpečnostných opatrení, ak sa Zmluvné strany písomne nedohodnú na inej lehote.

Článok VI
Zapojenie ďalšieho dodávateľa

(1) Partner je oprávnený zapojiť ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie podľa Hlavnej zmluvy pre ZSSK CARGO len na základe predchádzajúceho písomného súhlasu ZSSK CARGO.

(2) Partner je povinný informovať ZSSK CARGO o akýchkoľvek zamýšľaných zmenách v súvislosti s pridaním alebo nahradením ďalších dodávateľov, čím sa ZSSK CARGO dáva možnosť namietať voči takýmto zmenám. V prípade, ak ZSSK CARGO do 5 pracovných dní nenamietne voči osobe ďalšieho dodávateľa, Partner je oprávnený takého ďalšieho dodávateľa zapojiť za účelom zabezpečenia plnenia podľa Hlavnej zmluvy pre ZSSK CARGO, v opačnom prípade tak nie je oprávnený urobiť.

(3) Ak Partner zapojí ďalšieho dodávateľa zabezpečujúceho plnenie podľa Hlavnej zmluvy v mene Partnera, tomuto ďalšiemu dodávateľovi v zmluve alebo inom právnom úkone je povinný uložiť rovnaké povinnosti týkajúce sa zabezpečovania predmetu plnenia podľa príslušnej Hlavnej zmluvy tak, ako sú ustanovené v tejto Zmluve pre Partnera.

(4) Ak ďalší dodávateľ poverený Partnerom nesplní svoje povinnosti týkajúce plnenia podľa príslušnej Hlavnej zmluvy a/alebo povinnosti podľa odseku 3 tohto článku Zmluvy, nesie zodpovednosť voči ZSSK CARGO v plnej miere Partner.

Článok VII
Oznámenie o kybernetických bezpečnostných incidentoch

(1) Zmluvné strany sú povinné bezodkladne vzájomne si oznámiť každý kybernetický bezpečnostný incident, ktorý súvisí s Partnerom prevádzkovaným informačným systémom a o ktorom sa hodnoverne dozvedia, prostredníctvom k tomu poverených zamestnancov a to na kontaktné údaje uvedené v článku X tejto Zmluvy.

(2) V oznámení podľa odseku 1 tohto článku Zmluvy príslušná Zmluvná strana uvedie:
- a) službu podľa Hlavnej zmluvy zasiahnutú kybernetickým bezpečnostným incidentom,
- b) vplyv kybernetického bezpečnostného incidentu na poskytovanú službu,
- c) časové údaje priebehu kybernetického bezpečnostného incidentu,
- d) detailný opis priebehu kybernetického bezpečnostného incidentu,
- e) rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu alebo rozsah predpokladaných škôd z dôvodu kybernetického bezpečnostného incidentu,
- f) popis následkov kybernetického bezpečnostného incidentu alebo popis očakávaných následkov kybernetického bezpečnostného incidentu,
- g) riešenie kybernetického bezpečnostného incidentu,
- h) stav riešenia kybernetického bezpečnostného incidentu,
- i) vykonané nápravné opatrenia, ak boli vykonané.

Článok VIII
Vykonávanie auditu u Partnera

(1) ZSSK CARGO je oprávnená po predchádzajúcom písomnom oznámení adresovanom Partnerovi najneskôr 7 pracovných dní pred termínom auditu vykonať u Partnera audit v oblasti plnenia zmluvných záväzkov vyplývajúcich z tejto Zmluvy v oblasti kybernetickej

bezpečnosti vo vzťahu k informačným aktívam ZSSK CARGO, za účelom preverenia účinnosti Partnerom prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom o kybernetickej bezpečnosti a ostatných príslušných všeobecne záväzných právnych predpisov v oblasti kybernetickej bezpečnosti.

(2) ZSSK CARGO v písomnom oznámení podľa odseku 1 tohto článku Zmluvy uvedie dátum a čas vykonania auditu a mená a priezviská zamestnancov ZSSK CARGO, ktorí audit u Partnera vykonajú. V prípade, že Partnerovi dátum a čas vykonania auditu nevyhovuje, má právo žiadať o určenie iného, neskoršieho temínu auditu, čomu je ZSSK CARGO povinné vyhovieť, ak je takáto žiadosť doručená ZSSK CARGO najneskôr 3 pracovné dni pred termínom auditu určenom v písomnom oznámení podľa odseku 1 tohto článku Zmluvy. Neskorší termín auditu nemôže byť určený Partnerom viac ako 7 pracovných dní odo ňa termínu určeného ZSSK CARGO v písomnom oznámení podľa odseku 1 tohto článku Zmluvy, pričom Partner je povinný v tomto termíne audit vykonať a nie je oprávnený určiť ďalší neskorší termín.

(3) Partner je povinný poskytnúť ZSSK CARGO všetku súčinnosť potrebnú k riadnemu vykonaniu tohto auditu, poskytnúť ZSSK CARGO informácie potrebné na preukázanie splnenia jeho povinností podľa Zákona o kybernetickej bezpečnosti a podľa tejto Zmluvy a zabezpečiť prítomnosť zamestnancov Partnera alebo Partnerom poverených osôb, ktoré v rámci organizačnej štruktúry Partnera zodpovedné za plnenie povinností v oblasti kybernetickej bezpečnosti.

(4) ZSSK CARGO predloží Partnerovi do 30 dní od ukončenia auditu záverečnú správu o výsledkoch auditu spolu s návrhom opatrení a lehôt na ich zapracovanie. Následne sa zmluvné strany do 10 pracovných dní od predloženia záverečnej správy zo strany ZSSK CARGO dohodnú na spôsobe zapracovania navrhovaných opatrení a na záväzných termínoch na ich zapracovanie.

(5) V prípade, ak Partner nezapracuje navrhnuté opatrenia vyplývajúce z opatrení na nápravu spôsobom a v lehotách dohodnutých zmluvnými stranami podľa odseku 4 tohto článku Zmluvy, ZSSK CARGO má právo odstúpiť od tejto Zmluvy; tým nie je dotknutý nárok ZSSK CARGO na zmluvnú pokutu a ani zodpovednosť Partnera za škodu, ktorá prípadne ZSSK CARGO vznikla v dôsledku neprijatia opatrení na nápravu.

Článok IX
Sankcie

(1) V prípade, že si Partner ani napriek písomnej výzve ZSSK CARGO nesplní ktorúkoľvek povinnosť (záväzok) stanovenú touto Zmluvou v dodatočnej primeranej lehote poskytnutej mu zo strany ZSSK CARGO vo výzve na dodatočné plnenie, je ZSSK CARGO oprávnená uplatniť si voči Partnerovi nárok na zmluvnú pokutu vo výške 0,03 % z celkovej ročnej sumy odplaty, ktorú ZSSK CARGO vyplatila Partnerovi za plnenie záväzkov Partnera podľa Hlavnej zmluvy v kalendárnom roku predchádzajúcom kalendárnemu roku, kedy

k porušeniu zabezpečenej povinnosti Partnera došlo, a to za každý aj začatý deň omeškania s plnením príslušnej povinnosti (záväzku) Partnera, maximálne však do výšky 3 % z celkovej ročnej sumy odplaty, ktorú ZSSK CARGO vyplatila Partnerovi za plnenie záväzkov Partnera podľa Hlavnej zmluvy v kalendárnom roku predchádzajúcom kalendárnemu roku, kedy k porušeniu zabezpečenej povinnosti Partnera došlo. V prípade porušenia povinnosti Partnera, ktoré podľa povahy porušenej povinnosti nemožno dodatočne splniť/napraviť alebo zvrátiť, je ZSSK CARGO oprávnená uplatniť si voči Partnerovi nárok na zmluvnú pokutu vo výške 3 % z celkovej ročnej sumy odplaty, ktorú ZSSK CARGO vyplatila Partnerovi za plnenie záväzkov Partnera podľa Hlavnej zmluvy v kalendárnom roku predchádzajúcom kalendárnemu roku, kedy k porušeniu zabezpečenej povinnosti Partnera došlo.

(2) V prípade, ak Partner neodstráni akékoľvek nedostatky identifikované Národným bezpečnostným úradom podľa § 27a Zákona o kybernetickej bezpečnosti, ktoré majú priamu alebo nepriamu súvislosť s plnením Hlavnej zmluvy v lehote určenej Národným bezpečnostným úradom, v dôsledku čoho Národný bezpečnostný úrad rozhodne o zakázaní alebo obmedzení používania produktu, procesu alebo služby, ktoré pre ZSSK CARGO zabezpečuje Partner, alebo ak Národný bezpečnostný úrad zakáže alebo obmedzí činnosti Partnera, v dôsledku čoho si Partner nebude môcť plniť povinnosti voči ZSSK CARGO, ZSSK CARGO je oprávnená uplatniť si voči Partnerovi nárok na zmluvnú pokutu vo výške 10 % z celkovej ročnej sumy odplaty, ktorú ZSSK CARGO vyplatila Partnerovi za plnenie záväzkov Partnera podľa Hlavnej zmluvy v kalendárnom roku predchádzajúcom kalendárnemu roku, kedy bolo rozhodnutie Národného bezpečnostného úradu vyhlásené v Zbierke zákonov Slovenskej republiky. Uplatnením alebo zaplatením zmluvnej pokuty podľa tohto ustanovenia Zmluvy nie je dotknutý nárok ZSSK CARGO na náhradu škody v rozsahu prevyšujúcom zmluvnú pokutu.

(3) Partner má nárok na náhradu akýchkoľvek preukázaných sankcií, ktoré mu budú uložené z dôvodu porušenia povinností stanovených touto Zmluvou zo strany ZSSK CARGO. V prípade, ak dôjde k uloženiu pokuty z dôvodov porušenia povinností stanovených touto Zmluvou zo strany oboch Zmluvných strán, má Partner nárok na náhradu sankcie len v pomernom rozsahu, v ktorom možno pričítať uloženie príslušnej sankcie ZSSK CARGO.

(4) Partner je povinný ZSSK CARGO nahradiť sumu pokuty, ktorá bola ZSSK CARGO právoplatne uložená Národným bezpečnostným úradom alebo iným príslušným orgánom verejnej správy a neprebieha ani konanie o jej zrušenie na príslušnom (správnom) súde, ak pokuta bola ZSSK CARGO uložená z dôvodu porušenia povinnosti Partnera podľa tejto Zmluvy a/alebo podľa Zákona o kybernetickej bezpečnosti v oblasti kybernetickej bezpečnosti vo vzťahu k informačným aktívam ZSSK CARGO. Náhradou podľa predchádzajúcej vety nie je dotknuté právo ZSSK CARGO na nárok na náhradu skutočnej škody (mimo ušlého zisku a súvisiacich vynaložených nákladov) spôsobenej porušením povinnosti Partnera, pre ktorú bola ZSSK CARGO pokuta uložená. ZSSK CARGO je povinné v konaní o uloženie pokuty či náhradu škody alebo jemu predchádzajúcom konaní vykonať všetky primerané opatrenia a uplatniť všetky prostriedky a spôsoby obrany voči hroziacej pokute a uplatnenej škode a informovať o konaniach Partnera v rozsahu, aby mohol zaujať stanovisko; ak hroziaca pokuta či uplatnená škoda mali byť spôsobené aj

porušením povinností Partnerom, ZSSK CARGO nesmie hroziacu pokutu či uplatnenú škodu uznať bez súhlasu Partnera. Pre porušenie povinností podľa predchádzajúcej vety zo strany ZSSK CARGO nie je Partner povinný nahradiť pokutu či škodu v rozsahu, v akom malo toto porušenie vplyv na výšku uloženej pokuty či priznanej náhrady škody. Náhrada spôsobenej škody, za ktorú sa považuje aj pokuta uložená ZSSK CARGO podľa tohto bodu, sa riadi bodom 5.1 Hlavnej zmluvy. V prípade, ak dôjde k uloženiu pokuty z dôvodov porušenia povinností stanovených touto Zmluvou zo strany oboch Zmluvných strán, resp. z dôvodov porušenia povinnosti v oblasti kybernetickej bezpečnosti zo strany iných dodávateľov ZSSK Cargo, má ZSSK CARGO nárok na náhradu pokuty len v pomernom rozsahu, v ktorom možno pričítať uloženie príslušnej pokuty Partnerovi; ak sa Zmluvné strany nedohodnú na rozsahu zodpovednosti, tento rozsah môže určiť príslušný znalec, pričom každá Zmluvná strana môže požiadať o toto určenie aj súd.

Článok X
Kontaktné osoby a doručovanie

(1) Zoznam a kontaktné údaje zamestnancov Partnera a/alebo osôb poverených Partnerom pre oblasť kybernetickej bezpečnosti, ktoré majú prístup k informáciám a údajom ZSSK CARGO v oblasti bezpečnostných politík ZSSK CARGO a iných skutočností dôležitých pre kybernetickú bezpečnosť ZSSK CARGO:

Meno a priezvisko	**Označenie role:**	**E-mail:**	**Tel. číslo:**

(2) Zoznam a kontaktné údaje zamestnancov ZSSK CARGO pre oblasť kybernetickej bezpečnosti:

Meno a priezvisko	**Označenie role:**	**E-mail:**	**Tel. číslo:**
Rastislav Koňakovský	Vedúci tímu bezpečnosti a správy IT		
Lubomír Kopáček	Manažér KB		

(3) Zmluvné strany sú povinné vzájomne sa bezodkladne písomne informovať o každej zmene údajov v odseku 1 a 2 tohto článku Zmluvy, pričom o vykonaní tejto zmeny nie je potrebné uzatvoriť písomný dodatok podľa článku XIII ods. 3 tejto Zmluvy.

(4) Všetky písomnosti podľa tejto Zmluvy, s výnimkou písomností týkajúcej sa samotnej Zmluvy, odosielajúca Zmluvná strana posiela elektronicky druhej Zmluvnej strane na všetky e-mailové adresy druhej Zmluvnej strany uvedené v tomto článku Zmluvy.

(5) Všetky písomnosti týkajúce sa samotnej Zmluvy si Zmluvné strany posielajú na adresu sídla príslušnej Zmluvnej strany uvedenej v záhlaví tejto Zmluvy.

Článok XI
Mlčanlivosť a ochrana osobných údajov

(1) Za dôverné informácie sa na účely tejto zmluvy považujú najmä informácie týkajúce sa (i) plnenia tejto Zmluvy, (ii) IT infraštruktúry ZSSK CARGO, (iii) a informačných systémov, ktoré sú predmetom Hlavnej zmluvy, vrátane ich zabezpečenia, (iv) detaily týkajúce sa technických a organizačných opatrení na zabezpečenie integrity a prevádzkyschopnosti sietí a informačných systémov vrátane bezpečnostných politík Zmluvných strán, (v) osobné údaje, ktoré si Zmluvné strany na základe tejto Zmluvy a v súvislosti s jej plnením poskytnú, (vi) údaje a informácie o Zmluvných stranách a ich činnosti, ktoré nie sú verejne dostupné a (vii) iné údaje a informácie poskytované druhej Zmluvnej strane, ktoré poskytujúca Zmluvná strana výslovne za dôverné označí (ďalej len „**Dôverné informácie**“).

(2) Dôverné informácie poskytnuté, odovzdané, oznámené, sprístupnené a/alebo akýmkoľvek iným spôsobom získané jednou Zmluvnou stranou od druhej Zmluvnej strany na základe a/alebo v akejkoľvek súvislosti s touto Zmluvou môžu byť použité výhradne na účely plnenia predmetu tejto Zmluvy. Zmluvné strany sa zaväzujú udržiavať vyššie uvedené dôverné informácie v prísnej tajnosti, zachovávať o nich mlčanlivosť a chrániť ich pred zneužitím, poškodením, zničením, znehodnotením, stratou a odcudzením, a to i po ukončení platnosti a účinnosti tejto Zmluvy.

(3) Zmluvná strana nie je oprávnená bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany Dôverné informácie poskytnúť, odovzdať, oznámiť, sprístupniť, zverejniť, publikovať, rozširovať, vyzradiť ani použiť inak než na účely plnenia predmetu tejto Zmluvy, a to ani po ukončení platnosti a účinnosti tejto Zmluvy, s výnimkou prípadu ich poskytnutia/ odovzdania/ oznámenia/ sprístupnenia odborným poradcom Zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov, alebo audítorov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti stanovenou alebo uloženou zákonom alebo sú povinní zachovávať mlčanlivosť na základe písomnej dohody so Zmluvnou stranou.

(4) Povinnosť Zmluvných strán zachovávať mlčanlivosť o Dôverných informáciách sa nevzťahuje na informácie, ktoré:

(a) boli zverejnené už pred podpisom tejto Zmluvy, čo musí byť preukázateľné na základe poskytnutých podkladov, ktoré túto skutočnosť dokazujú;

(b) majú byť sprístupnené na základe povinnosti stanovenej zákonom, rozhodnutím súdu, prokuratúry alebo iného oprávneného orgánu verejnej moci, pričom v tomto prípade Zmluvná strana, ktorá je povinná informácie sprístupniť, bezodkladne informuje o sprístupnení informácií druhú Zmluvnú stranu.

(5) Zmluvné strany sú povinné zabezpečiť riadne a včasné utajenie Dôverných informácií a zachovávanie povinnosti mlčanlivosti o Dôverných informáciách podľa všeobecne platných, zaužívaných a zachovávaných pravidiel, zásad a zvyklostí pre utajovanie a zachovávanie povinnosti mlčanlivosti o takýchto informáciách.

(6) Zmluvné strany sú povinné zabezpečiť riadne a včasné utajenie Dôverných informácií a zachovávanie povinnosti mlčanlivosti o Dôverných informáciách aj u svojich zamestnancov, štatutárnych orgánov, členov štatutárnych orgánov, dozorných orgánov, členov dozorných orgánov, zástupcov, splnomocnencov, subdodávateľov ako i iných spolupracujúcich tretích osôb, pokiaľ im takéto Dôverné informácie boli poskytnuté, odovzdané, oznámené a/alebo sprístupnené v súlade s touto Zmluvou.

(7) Zmluvné strany sa navzájom zaväzujú zachovávať všetky platnými právnymi predpismi stanovené povinnosti vo vzťahu k spracúvaniu a ochrane osobných údajov, ktoré získajú a budú na základe tejto Zmluvy alebo v súvislosti s jej plnením spracúvať. Zmluvné strany sa zaväzujú oznamovať si navzájom zmeny všetkých osobných údajov, ktoré si na základe tejto Zmluvy, resp. v súvislosti s jej plnením poskytli tak, aby spracúvali vždy len správne a aktuálne osobné údaje. Zmluvné strany sa zaväzujú najmä zachovávať zásadu minimalizácie spracúvaných osobných údajov tak, aby spracúvali vždy len tie osobné údaje, ktoré sú potrebné na účely daného spracúvania, resp. na účely plnenia tejto Zmluvy. Informácie o ochrane osobných údajov v ZSSK CARGO určené zmluvným partnerom spoločnosti, ich zamestnancom a zástupcom sú dostupné na webovej adrese: https://www.zscargo.sk/oou, o čom je Partner povinný informovať dotknuté osoby. Zmluvné strany zároveň vyhlasujú, že žiadna z nich nebude na základe tejto Zmluvy spracúvať osobné údaje v mene druhej Zmluvnej strany.

Článok XII
Trvanie zmluvy

(1) Táto Zmluva sa uzatvára na dobu neurčitú, počas trvania Hlavnej zmluvy.

(2) Táto Zmluva zaniká:
a) písomnou dohodou Zmluvných strán v deň tam uvedený;
b) nadobudnutím účinnosti písomného odstúpenia od tejto Zmluvy jednou zo Zmluvných strán v súlade s odsekom 3 tohto článku Zmluvy;
c) zánikom Hlavnej zmluvy.

(3) Odstúpiť od tejto Zmluvy môže ktorákoľvek zo Zmluvných strán v prípadoch výslovne stanovených touto Zmluvou a tiež v prípade akéhokoľvek porušenia zmluvných povinností druhou Zmluvnou stranou, ak povinná Zmluvná strana nevykoná nápravu ani napriek

písomnému upozorneniu oprávnenej Zmluvnej strany v primeranej dodatočnej lehote poskytnutej jej k tomu oprávnenou Zmluvnou stranou alebo ak opätovne poruší tú istú povinnosť, na ktorej porušenie bola povinná Zmluvná strana v priebehu trvania tejto Zmluvy už raz upozornená. Písomné odstúpenie od Zmluvy nadobúda platnosť a účinnosť dňom jeho doručenia druhej Zmluvnej strane s účinkami od odo dňa doručenia (*ex nunc*). Odstúpenie od Zmluvy sa nedotýka nároku na náhradu škody ani nároku na zmluvnú pokutu, ktorý vznikol v dôsledku porušenia povinností (§ 351 ods.1 Obchodného zákonníka) a všetkých právnych následkov porušenia Zmluvy, ku ktorým došlo do zániku Zmluvy.

(4) Zánik tejto Zmluvy nemá vplyv na práva a povinnosti Zmluvných strán, ktoré vznikli počas existencie tejto Zmluvy a neboli ku dňu jej zániku riadne vysporiadané. Zánik tejto Zmluvy nemá tiež vplyv na práva a povinnosti, z ktorých obsahu a účelu vyplýva, že sa majú uplatňovať aj po zániku tejto Zmluvy.

Článok XIII
Záverečné ustanovenia

(1) Zmluvné strany sa dohodli, že odplata za všetky plnenia a činnosti podľa tejto Zmluvy sa riadi pravidlami odplaty za poskytovanie služieb podľa Hlavnej zmluvy, pokiaľ sa Zmluvné strany nedohodnú inak.

(2) Táto Zmluva nadobúda platnosť dňom jej podpisu oboma Zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky podľa § 5a ods. 2 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.

(3) Ustanovenia tejto Zmluvy je možné meniť len na základe dohody Zmluvných strán uzatvorenej vo forme písomných a vzostupne očíslovaných dodatkov k tejto Zmluve, podpísaných oboma Zmluvnými stranami; to neplatí pre zmenu údajov o Zmluvných stranách obsiahnutých v záhlaví tejto Zmluvy a pre údaje o kontaktných osobách, kedy postačuje písomné oznámenie o zmene týchto údajov, ktoré musí byť doručené druhej Zmluvnej strane.

(4) Ak niektoré otázky nemožno riešiť podľa ustanovení tejto Zmluvy alebo ak niektoré otázky nie sú v tejto Zmluve riešené, riešia sa podľa príslušných právnych predpisov v oblasti kybernetickej bezpečnosti a podľa zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

(5) Všetky prílohy tejto Zmluvy tvoria jej neoddeliteľnú súčasť. Prílohami k tejto Zmluve sú
- Príloha č. 1 – Špecifikácia bezpečnostných opatrení Partnera
- Príloha č. 2 – Zoznam bezpečnostnej dokumentácie

(6) Táto Zmluva sa vyhotovuje v 2 (dvoch) rovnopisoch, pričom každá zo Zmluvných strán si ponechá 1 (jeden) rovnopis.

(7) Zmluvné strany vyhlasujú, že majú spôsobilosť na právne úkony v plnom rozsahu a ich zmluvná voľnosť nie je žiadnym spôsobom obmedzená. Zmluvné strany ďalej vyhlasujú, že túto Zmluvu uzatvorili na základe ich skutočnej, slobodnej a vážnej vôle, ktorej prejav zachytený v obsahu tejto Zmluvy je dostatočne určitý a zrozumiteľný, túto Zmluvu uzatvorili dobromyseľne a v súlade so zásadami poctivého obchodného styku a neuzatvorili ju ani v omyle, ani pod nátlakom a ani v tiesni za nápadne nevýhodných podmienok, túto Zmluvu si prečítali, obsahu tejto Zmluvy porozumeli a na znak súhlasu s obsahom tejto Zmluvy ju prostredníctvom osôb oprávnených konať v ich mene podpísali.

V Bratislave dňa

Železničná spoločnosť Cargo Slovakia, a.s.

Ing. Jaroslav Daniška
predseda predstavenstva a generálny riaditeľ

Mgr. Matej Hambálek, MBA
podpredseda predstavenstva

V xxxxxxxxxxxxxx dňa

xxxxx