Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 1100045171

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:	Drieňová 24, 820 09 Bratislava
Zapísaná:	Obchodný register Okresného súdu Bratislava I oddiel: Sro, vložka č. 3496/B
IČO:	35 914 921
DIČ:	2021920065
IČ DPH:	SK2021920065
Konajúca:	Ing. Roman Gono – predseda predstavenstva Ing. Jaroslav Daniška – podpredseda predstavenstva

(ďalej len **„ZSSK CARGO“**)

a

2./	**TORY CONSULTING, a.s.**
Sídlo:	Slovenskej jednoty 10, 040 01 Košice
Zapísaná:	Obchodný register Okresného súdu Košice I Oddiel: Sa, Vložka číslo: 879/V
IČO:	36 174 777
DIČ:	2020043916
IČ DPH:	SK2020043916
Konajúca:	RNDr. Roman Kekeňák – predseda predstavenstva a generálny riaditeľ

(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 sietí a informačných systémov poskytuje ZSSK CARGO ako prevádzkovateľovi základnej služby činnosti súvisiace so správou a rozvojom informačného systému SAP , a to podľa predmetu nasledovných zmlúv:

1100019098 - 6986/2017-O8

(vyššie uvedené zmluvy budú označovanie len ako „**Hlavné zmluvy**“).

(2) Rozsah činnosti Partnera je špecifikovaný 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 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) dodržiavať bezpečnostné politiky ZSSK CARGO, vyjadriť s nimi súhlas a plniť povinnosti vyplývajúce z bezpečnostnej dokumentácie ZSSK CARGO, s ktorou bol oboznámený,

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 na 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.

(3) Bezodkladne po ukončení tejto Zmluvy, najneskôr však do 3 dní, Partner predloží ZSSK CARGO sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča dát, ktoré 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 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 uvedené 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.

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) preukázateľne oboznámiť Partnera s bezpečnostnými politikami ZSSK CARGO do 15 dní po nadobudnutí účinnosti zmluvy;
c) dodržiavať a prijať bezpečnostné opatrenia v zmysle B. časti Prílohy č. 1 tejto Zmluvy,
d) bezodkladne písomne informovať Partnera o akýchkoľvek zmenách bezpečnostných politík relevantných pre plnenia záväzkov Partnera,
e) 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 Hlavných zmlúv a tejto Zmluvy, povinný najmä:

a) dodržiavať bezpečnostné politiky ZSSK CARGO,

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 pokynov ZSSK CARGO aktualizovať alebo dopĺňať,
c) mať vypracovanú bezpečnostnú dokumentáciu najmenej v rozsahu stanovenom v časti B. Prílohy č. 1 tejto Zmluvy a túto aktualizovať tak, aby zodpovedala reálnemu stavu vzťahujúcemu sa k činnostiam, ktoré pre ZSSK CARGO podľa Hlavných zmlúv a tejto Zmluvy zabezpečuje; ak je Partner poskytovateľom základnej služby alebo digitálnej služby je povinný 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.,
d) bezodkladne písomne oznámiť ZSSK CARGO akúkoľvek zmenu v špecifikácií a rozsahu ním prijatých bezpečnostných opatrení,
e) dodržiavať 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 pokyny týkajúce sa uplatňovania bezpečnostných opatrení Partnera a uplatňovania bezpečnostných politík ZSSK CARGO,
b) kontrolovať plnenie záväzkov Partnera podľa tejto Zmluvy a vykonať u Partnera bezpečnostný audit podľa článku VIII tejto Zmluvy.

(5) Zmluvné strany berú na vedomie, že ZSSK CARGO je povinná podrobiť 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 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, zaväzuje sa Partner v súčinnosti so ZSSK CARGO prijať a implementovať všetky 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, 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. 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 akejkoľvek zmeny v špecifikácií a rozsahu bezpečnostných opatrení podľa tohto článku Zmluvy 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 zmene 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 Hlavných zmlúv 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 namieta voči osobe ďalšieho dodávateľa, Partner nie je oprávnený takého ďalšieho dodávateľa zapojiť za účelom zabezpečenia plnenia podľa príslušnej Hlavnej zmluvy pre ZSSK CARGO.

(3) Ak Partner zapojí ďalšieho dodávateľa zabezpečujúceho plnenie podľa niektorej z Hlavných zmlúv 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, 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 uvedenie:
   a) službu 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 5 pracovných dní pred termínom auditu vykonať u Partnera audit 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.

(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 záverečnú správu o výsledkoch auditu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

(5) V prípade, ak Partner neodstráni nedostatky vyplývajúce z opatrení na nápravu v lehote určenej ZSSK CARGO podľa odseku 4 tohto článku Zmluvy, ZSSK CARGO má právo odstúpiť od všetkých Hlavných zmlúv alebo od príslušnej Hlavnej zmluvy, ak sa porušenie príslušnej povinnosti týka činností, ktoré sú viazané len na niektorú z Hlavných zmlúv; 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. 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. V prípade, ak Partner neodstráni nedostatky v sieti, informačných systémoch alebo akékoľvek iné nedostatky identifikované Národným bezpečnostným úradom podľa § 27a Zákona o kybernetickej bezpečnosti 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.

(2) 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.

(3) Partner je povinný ZSSK CARGO nahradiť sumu pokuty, ktorá bola ZSSK CARGO uložená Národným bezpečnostným úradom alebo iným príslušným orgánom verejnej správy, ak pokuta bola ZSSK CARGO uložená z dôvodu porušenia povinnosti Partnera podľa tejto Zmluvy a/alebo podľa Zákona o kybernetickej bezpečnosti. Náhradou podľa predchádzajúcej vety nie je dotknuté právo ZSSK CARGO na nárok na náhradu ostatnej škody spôsobenej porušením povinnosti Partnera, pre ktorú bola ZSSK CARGO pokuta uložená a ani na nárok na zaplatenie zmluvnej pokuty dohodnutej pre porušenie povinností Partnera v rozsahu prevyšujúcom škodu, ktorá tým bola ZSSK CARGO spôsobená.

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:
	Administrátor		
	Administrátor		

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

Meno a priezvisko	Označenie role:	E-mail:	Tel. číslo:
	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 strany 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 jednotlivých Hlavných zmlúv, 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, ktorá 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 Hlavných zmlúv.

(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 všetkých Hlavných zmlúv (t.j. zánikom poslednej z nich).

(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.

(5) Zánikom tejto Zmluvy dochádza automaticky k zániku všetkých Hlavných zmlúv, ak sa Zmluvné strany nedohodnú dodatočne písomne inak.

Článok XIII
Záverečné ustanovenia

(1) Zmluvné strany sa dohodli, že všetky plnenia a činnosti podľa tejto Zmluvy si budú Zmluvné strany poskytovať bezodplatne, resp. že odplata za činnosti stanovené touto Zmluvou je zahrnutá v odplate za poskytovanie služieb podľa Hlavnej zmluvy.

(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 – Rozsah činnosti a špecifikácia bezpečnostných opatrení Partnera a ZSSK CARGO

(6) Táto Zmluva sa vyhotovuje v 4 (štyroch) rovnopisoch, pričom každá zo Zmluvných strán si ponechá 2 (dva) rovnopisy.

(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. Roman Gono
predseda predstavenstva a generálny riaditeľ

Ing. Jaroslav Daniška
podpredseda predstavenstva

V Bratislave dňa

TORY CONSULTING, a.s

RNDr. Roman Kekeňák
predseda predstavenstva
a generálny riaditeľ

Príloha č. 1- Rozsah činností a špecifikácia bezpečnostných opatrení

Časť A: Rozsah činností a špecifikácia bezpečnostných opatrení Partnera Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 1100045171

Rozsah činnosti a špecifikácia bezpečnostných opatrení Partnera
Sú vykonávané bezpečnostné opatrenia v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti
Bezpečnostné opatrenia sú realizované v závislosti od klasifikácie informácií a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služby.
Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá je udržovaná aktuálna a zodpovedajúca reálnemu stavu.
Bezpečnostné opatrenia sa prijímajú najmä pre oblasť • organizácie kybernetickej bezpečnosti a informačnej bezpečnosti, • riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti, • personálnej bezpečnosti, • riadenia prístupov, • riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, • bezpečnosti pri prevádzke informačných systémov a sietí, • hodnotenia zraniteľností a bezpečnostných aktualizácií, • ochrany proti škodlivému kódu, • sieťovej a komunikačnej bezpečnosti, • akvizície, vývoja a údržby informačných sietí a informačných systémov, • zaznamenávania udalostí a monitorovania, • fyzickej bezpečnosti a bezpečnosti prostredia, • riešenia kybernetických bezpečnostných incidentov, • kryptografických opatrení, • kontinuity prevádzky, • auditu, riadenia súladu a kontrolných činností.
Partner zabezpečí detekovanie, evidovanie kybernetických bezpečnostných incidentov (KBI), zavádzanie postupov riešenia KBI a samotné riešenie KBI podľa normy ISO/IEC 27001:2013.
V prípade, že Partner pri svojej pracovnej činnosti v rámci IS pre ZSSK CARGO zistí kybernetický bezpečnostný incident, zabezpečí jeho neodkladné nahlásenie kontaktnej osobne ZSSK CARGO, ktorá je uvedená v Zmluve, a ktorá ďalej zabezpečuje spracovanie, hlásenie a riešenie kybernetických bezpečnostných incidentov do centrálneho systému včasného varovania.
Partner v prípade, že sa jedná o kybernetický bezpečnostný incident na úrovni IS pre ZSSK CARGO, ktorý spravuje, zabezpečí plnú súčinnosť pri jeho riešení v spolupráci so ZSSK CARGO.
Partner zabezpečil určenie kontaktnej osoby pre prijímanie a evidenciu hlásení a uviedol ju v Zmluve.
Partner dopracuje komunikačné manuály k IS vo vzťahu k ZS, aby prideľovanie privilégií pre prácu s IS bolo jasne určené a dodržiavala sa zásada najnižších privilégií podľa pravidiel/požiadaviek definovaných ZSSK CARGO.
Partner dopracuje komunikačné manuály k IS, aby obsahovali jasne spracované zodpovednosti pre prácu s IS s dodržaním zásad oddeľovania zodpovedností podľa pravidiel/požiadaviek definovaných ZSSK CARGO.
Partner zavedie potrebnú ochranu operačných systémov firewallom a softvérom na antivírusovú/antimalware ochranu na základe odporúčaní internej Rady pre kybernetickú bezpečnosť Partnera a na základe interných protokolov, ktoré spĺňajú maximálnu možnú mieru ochrany a zabezpečenia podľa normy ISO/IEC 27001:2013.
Partner prijme opatrenia potrebné na vykonávanie pravidelného posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zo zariadenia Partnera, ktoré sa vzdialene pripája do internej siete ZSSK CARGO podľa normy ISO/IEC 27001:2013.

Podľa pravidiel/požiadaviek ZSSK CARGO dopracuje Partner do IS riešenie pre centrálne zaznamenávanie činnosti IS.
Dodržiavať odporúčané politiky aktualizácií a riadenia záplat pre systémy v správe Partnera, ktoré pristupujú do internej siete ZSSK CARGO a sú v súlade s odporúčaniami NBÚ na základe bezpečnostných varovaní SK-CERT. podľa pravidiel/požiadaviek definovaných ZSSK CARGO. Zabezpečiť aktualizáciu informačného systému z pohľadu bezpečnostných aktualizácií počas trvania zmlúv o poskytovaní služieb 1100019098 - 6986/2017-O8
Sledovať bezpečnostné varovania na webovej stránke SK-CERT.

Časť B: Špecifikácia bezpečnostných opatrení ZSSK CARGO Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 1100045171

Špecifikácia bezpečnostných opatrení ZSSK CARGO
Vypracovať dokument Stratégia kybernetickej bezpečnosti ZSSK CARGO podľa prílohy 1 Vyhlášky NBÚ č. 362/2018 Z. z.
Vykonať audit kybernetickej bezpečnosti podľa § 29 Zákona o kybernetickej bezpečnosti.
V rámci existujúcej organizačnej štruktúry vytvoriť pozíciu manažéra kybernetickej bezpečnosti.
Dopracovať komunikačné manuály k IS vo vzťahu k ZS, aby prideľovanie privilégií pre prácu s IS bolo jasne určené a dodržiavala sa zásada najnižších privilégií.
Dopracovať komunikačné manuály k IS, aby obsahovali jasne spracované zodpovednosti pre prácu s IS s dodržaním zásad oddeľovania zodpovedností.
Stanoviť zásady vykonávania nezávislého hodnotenia efektivity a účinnosti prijatých opatrení v rámci Stratégie kybernetickej bezpečnosti ZSSK CARGO.
Na základe kompetencií vyšpecifikovaných v Stratégii kybernetickej bezpečnosti ZSSK CARGO pre súčasných, resp. nových zamestnancov SICT, upraviť ich pracovné náplne podľa požiadaviek Zákona o kybernetickej bezpečnosti.
Detailne identifikovať a evidovať primárne a podporné aktíva v štruktúre: • Procesy a informácie • Hardvér (koncové zariadenia) • Softvér (operačný, podporný a aplikačný) • Sieť (sieťové zariadenia) • Zamestnanci (správa a administrácia, používatelia, dodávatelia SW aplikácií) • Lokalita (externé prostredie, kancelárie, zóny, objekty) • Organizácia (autority, organizačné zložky, dodávatelia). Uviesť pravidlá centrálneho monitoringu koncových zariadení v správe ZSSK CARGO.
Zaviesť proces manažérstva rizík podľa STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.
Posúdiť dopady, ktoré by vznikli, ak by základná činnosť bola prerušená: • dopady na zamestnancov, resp. verejné blaho, • dopad poškodenia alebo straty aktív podniku (napr. hmotný/nehmotný majetok), • dopad porušenia požiadaviek všeobecne záväzných predpisov, • poškodenie dobrého mena, • poškodenie finančnej životaschopnosti, • zhoršenie kvality poskytovanej služby,

poškodenie životného prostredia.
Zabezpečiť pravidelné vstupné e-learningové školenie nových a pravidelné preškoľovanie stávajúcich používateľov o pravidlách používania IT zariadení a kultúre informačnej bezpečnosti.
Pravidelne opakovať nezávislé kontroly, audity a penetračné testy zamerané na jednotlivé zraniteľné miesta podporných aktív (HW, SW, siete, zamestnanci, lokality, organizácie) a to ako vo vnútornom, tak aj vonkajšom prostredí ZSSK CARGO. Využiť možnosť kontroly danú nariadením GDPR [článok 28 ods. 3 písm. h) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)] ako aj Zákonom o kybernetickej bezpečnosti [§8 písm. h) Vyhlášky NBÚ č. 362/2018 Z. z.].
Doplniť v Pracovnom poriadku ZSSK CARGO závažné a menej závažné porušenie pracovnej disciplíny z pohľadu kybernetickej bezpečnosti.
Vypracovať a doplniť metodiku na pripájanie mobilných zariadení (súkromných, verejných, PDA) do firemnej siete a politiky vynútenia zabezpečenia mobilných prostriedkov.
Zaviesť potrebnú ochranu operačných systémov softvérovým firewallom či softvérom na antivírusovú/antimalware ochranu po konzultácii s dodávateľom IS. Získať a dopracovať spôsob riešenia a získané informácie do sieťovej dokumentácie.
Zvážiť nasadenie IDS/IPS systémov alebo riešenia, ktoré takéto nástroje integruje (komerčné Fortigate IPS, Cisco IPS), open-Source Suricata IDS. Integrácia do systémov bezpečnosti. Následne vypracovať metodiku a politiky nasadenia a ladenia IDS systémov za účelom optimálneho miesta nasadenia a zníženia množstva False-positive hlásení. Zvážiť nasadene SIEM nástroja, či CSIRT tím nástroja (napr. AT&T Cybersecurity)
Zabezpečiť všetky mobilné zariadenia pripájajúce sa do siete LAN (WiFi) softvérom ESET Mobile Security, resp. jeho ekvivalentom. Vypracovať politiku/metodiku na pripájanie zariadení dodávateľov a zákazníkov do firemnej siete. Prijať opatrenia potrebné na vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete.
Vypracovať jednotnú metodiku a pravidlá riadenia záplat a aktualizácii pre systémy v správe ZSSK CARGO. Vyžiadať informácie od dodávateľov IS (resp. správcu daných IS) o systéme aplikácie aktualizácií, zjednotiť s vlastnými metodikami. Zabezpečiť aktualizáciu systémov IS_ND a IS_ED z pohľadu aktualizácií po skončení zmluvy.
Vykonávať procesy testovania záloh.
Vypracovať pravidlá pre ochranu pred škodlivým kódom.
Vypracovať metodiku pre zaznamenávanie bezpečnostných záznamov.
Dopracovať riadenie prístupu používateľov k IS z pohľadu požiadaviek systému riadenia bezpečnosti a doplniť do komunikačných manuálov.
Zvážiť nasadenie centrálneho systému správy a vyhodnocovania logov. Zvážiť riešenie prepojenia autentifikácie prístupu do WiFi cez AD v ZSSK CARGO.
Vypracovať pravidlá a politiky kryptografickej ochrany informácií, spôsobov využívania systému certifikačnej autority (systém PKI), systému manažmentu kľúčov využívaný pre podporu kryptografických operácií (odhaľovanie slabých hesiel, generovanie hesiel, likvidácia hesiel, distribúcia hesiel, ukladanie, zálohovania a obnova a pod.).
Určiť osobu (manažér kybernetickej bezpečnosti) zodpovednú za nahlasovanie závažných kybernetických

bezpečnostných incidentov, ktoré nastali v sieťach a informačných systémoch. Vypracovať postup hlásenia, riešenia a znižovania následkov bezpečnostných incidentov. Sledovať bezpečnostné varovania na webovej stránke SK-CERT.
Zvážiť nasadenie nástroja pre zber a vyhodnocovanie informácií o KBI vo svojej vlastnej infraštruktúre.
Je potrebné vypracovať riešenie pre centrálne zaznamenávanie činnosti: - IS systémov vo vzťahu k základnej službe - MS Active Directory - centrálnych sieťových prvkov (firewall, VPN koncentrátor, switch, MPLS router, ...). Analyzovať potreby vhodnosti NMS a centrálnych logovacích systémov s minimálnymi funkciami ako je požadované vyhláškou s prepojením na log systémy dodávateľov.
Vypracovať pravidlá pre vedenie prevádzkových záznamov. Pridelenie zodpovednosti osobe/tímu za monitoring logovacích záznamov v daných IS. Odobrať právo modifikovať logovacie záznamy všetkým používateľom bez výnimky. Vybudovať zabezpečený kanál pre posielanie logovacích záznamov na centrálne úložisko, resp. vytvoriť a použiť dedikovanú manažmentovú sieť.
Zabezpečiť serverovňu (Technologická miestnosť – Serverovňa BA, KE) ako režimové pracovisko so zabezpečením technickými ochrannými opatreniami (EPS a EZS/TPS s min. triedou zabezpečenia 2) a so zabezpečením neoprávneného prístupu neautorizovaných osôb formou mechanických ochranných opatrení zvyšujúcimi ich pasívnu ochranu (otvorové výplne, uzamykacie systémy s min. bezpečnostnou triedou 3 podľa STN EN 1627). Všetky aktívne prvky by mali byť zabezpečené prepäťovou ochranou a taktiež proti výpadku hlavného zdroja napájania.
Zabezpečiť režimové pracovisko ZSSK CARGO určené ZSSK CARGO pred výpadkom zdroja elektrickej energie.
Zaviesť prevádzkový poriadok s určením oprávnených osôb na vstup do serverovne, smernicu na spôsob vedenia evidencie návštev, overovať totožnosť osôb (zoznam oprávnených osôb) a evidovať ich do knihy na to určenej. V rámci predmetovej ochrany je potrebné dbať na uzamykanie rack skríň.
Implementovať politiku režimových opatrení fyzickej a objektovej bezpečnosti.
Spracovať havarijné plány, plány kontinuity činností a plány obnovy informačných systémov podľa medzinárodného štandardu STN EN ISO 22301 Ochrana spoločnosti. Systémy manažérstva plynulého podnikania.
Zavedenie a popísanie postupov zálohovania konfigurácie aktívnych sieťových prvkov (Firewall, switch, ...), a častí systémov IS. Zabezpečenie geografickej dislokácie záloh. Pokiaľ zálohy obsahujú aj aktíva v klasifikačnom stupni chránené a vyššie, zabezpečiť ich šifrovanie. Určenie osoby zodpovednej za tvorbu záloh a ich kontrolu.