ZMLUVA O ZABEZPEČENÍ PLNENIA BEZPEČNOSTNÝCH OPATRENÍ A NOTIFIKAČNÝCH POVINNOSTÍ

uzatvorená podľa ustanovenia § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej ako „**Obchodný zákonník**“) a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „**ZoKB**“)

(ďalej ako „**Zmluva**“)

medzi:

Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky
so sídlom: Černyševského 50, 851 01 Bratislava
zastúpený: JUDr. Ing. Tomáš Drucker, MSc., minister
IČO: 00164381
DIČ: 2020798725
bankové spojenie: Štátna pokladnica
IBAN: SK80 8180 0000 0070 0006 5236

(ďalej ako „**Prevádzkovateľ**“ alebo aj ako „**ministerstvo**“)

a

DITEC, a.s.
so sídlom: Mlynské Nivy 55, 821 09 Bratislava - mestská časť Ružinov
zapísaný v: Obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka č.: 769/B
osoba konajúca v mene spoločnosti: Ing. Csaba Baráth, predseda predstavenstva
IČO: 31385401
DIČ: 2020304198
IČ DPH: SK2020304198
bankové spojenie: Tatra banka, a.s.
IBAN: SK93 1100 0000 0026 2700 7344

(ďalej ako „**Dodávateľ**“)

(Prevádzkovateľ a Dodávateľ spolu ďalej ako „**Zmluvné strany**“ a každý samostatne aj ako „**Zmluvná strana**“)

PREAMBULA

1. Zmluvné strany uzatvárajú túto Zmluvu podľa § 19 ods. 2 ZoKB za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na **Zmluvu o dodávke, podpore a rozvoji informačného systému elektronické služby regionálneho a vysokého školstva** uzatvorenú medzi Zmluvnými stranami dňa 29.12.2022, zverejnenú v Centrálnom registri zmlúv pod č. 0912/2022, ID zmluvy 7332451 (ďalej len „**Osobitná zmluva**“).
2. Prevádzkovateľ je prevádzkovateľom základnej služby v zmysle ZoKB. Základnou službou Prevádzkovateľa sú informačné systémy verejnej správy.
3. Dodávateľ poskytuje Prevádzkovateľovi činnosti na základe Osobitnej zmluvy (ďalej len „**služby**“) ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby podľa § 19 ods. 2 ZoKB.
4. Dodávateľ prehlasuje, že sa oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tejto Zmluvy.
5. Dodávateľ sa zaväzuje vykonávať všetky činnosti definované v tejto Zmluve v súlade s platnými právnymi predpismi. Zmluvné strany zhodne prehlasujú, že nie sú zbavené zodpovednosti za plnenie vlastných povinností, ktoré im vyplývajú zo ZoKB a ostatných právnych predpisov vydaných v súlade so ZoKB.
6. Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia Osobitnou zmluvou alebo ZoKB a inými právnymi predpismi vydanými v súlade so ZoKB.

Článok I.
Predmet Zmluvy

1. Predmetom tejto Zmluvy je určenie práv, povinností a záväzkov Zmluvných strán pri plnení bezpečnostných opatrení a notifikačných opatrení realizovaných v nadväznosti na Osobitnú zmluvu.

Článok II.
Miesto plnenia Zmluvy

1. Miestom plnenia tejto Zmluvy sú najmä sídla alebo pracoviská Prevádzkovateľa, sídlo alebo pracovisko Dodávateľa, alebo sídla a pracoviská subdodávateľov, ak to vyplýva z Osobitnej zmluvy. V prípade zmeny alebo doplnenia sídla alebo pracoviska Zmluvných strán, Zmluvné strany e-mailom informujú kontaktné osoby uvedené v čl. VIII. tejto Zmluvy, a to najneskôr do 30 kalendárnych dní od vykonania tejto zmeny.

Článok III.
Práva a povinnosti Zmluvných strán

1. Dodávateľ sa na základe tejto Zmluvy zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa, s ktorými ho Prevádzkovateľ preukázateľne oboznámi.

2. Dodávateľ vyhlasuje, že súhlasí s tým, že bezpečnostná politika Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa. Kontaktná osoba uvedená v čl. VIII. tejto Zmluvy je povinná oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne preukázateľne potvrdí akceptáciu zmien bezpečnostnej politiky a oboznámenie sa nimi.

3. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.

4. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek stanovených pre Prevádzkovateľa podľa ZoKB alebo vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z. vydanej na základe § 32 ods. 1 písm. b) ZoKB, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov (ďalej len „**vyhláška NBÚ**“), a to zaslaním e-mailu na kontaktnú osobu Prevádzkovateľa uvedenú v čl. VIII. tejto Zmluvy.

5. Dodávateľ sa zaväzuje hlásiť všetky informácie, ktoré majú vplyv na túto Zmluvu zaslaním e-mailu na kontaktnú osobu Prevádzkovateľa uvedenú v čl. VIII. tejto Zmluvy.

6. Dodávateľ je povinný:

   a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa,

   b) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa (ďalej len „**incidenty**“),

   c) zasielať Prevádzkovateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak,

   d) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby,

   e) po ukončení zmluvného vzťahu vrátiť, previesť alebo podľa pokynu Prevádzkovateľa preukázateľne zničiť všetky informácie Prevádzkovateľa, ku ktorým má Dodávateľ počas trvania tejto Zmluvy prístup,

   f) okrem už uvedeného prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 2 ZoKB a podľa vyhlášky NBÚ a v rozsahu špecifikovanom v prílohe č. 1 tejto Zmluvy.

7. Dodávateľ môže zapojiť do poskytovania služieb na základe Osobitnej zmluvy ďalšieho dodávateľa (ďalej len „**subdodávateľ**“), ak mu to vyplýva, resp. vyplynie z ustanovení Osobitnej zmluvy počas doby jej platnosti a účinnosti. V prípade zapojenia subdodávateľa je dodávateľ povinný zabezpečiť plnenie bezpečnostných opatrení a notifikačných povinností subdodávateľom minimálne v rozsahu, ako je ustanovené touto Zmluvou.

8. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu nadobudnutia účinnosti tejto Zmluvy až do skončenia platnosti a účinnosti Osobitnej zmluvy, pokiaľ z právnych predpisov uvedených v tejto Zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti Osobitnej zmluvy.

9. Dodávateľ sa zaväzuje viesť zoznam svojich pracovníkov a pracovníkov svojho subdodávateľa, ktorí majú prístup k informáciám a údajom Prevádzkovateľa. Dodávateľ je povinný hlásiť Prevádzkovateľovi každú zmenu v tomto zozname, a to bezodkladne zaslaním oznámenia na kontaktnú osobu Prevádzkovateľa uvedenú v článku VIII. tejto Zmluvy spôsobom a rozsahom

v zmysle ustanovenia podľa prílohy č. 2. Po nadobudnutí účinnosti tejto Zmluvy je dodávateľ povinný vyhotoviť predmetný zoznam a bezodkladne zaslať Prevádzkovateľovi

10. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi (i) dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany" všeobecne záväznými právnymi predpismi, najmä podľa ZoKB a vyhlášky NBÚ, a (ii) v súlade s § 9 ods. 4 vyhlášky NBÚ, že v prípadoch súvisiacich s vývojom a akvizíciou siete a informačného systému základnej služby Prevádzkovateľa bude tieto služby uskutočňovať s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v stratégii.

11. Ostatný konkrétny rozsah činnosti Dodávateľa je stanovený Osobitnou zmluvou.

12. Prevádzkovateľ sa zaväzuje bez zbytočného odkladu poskytnúť Dodávateľovi akúkoľvek súčinnosť nevyhnutnú alebo požadovanú Dodávateľom za účelom jeho riadneho plnenia si povinností v zmysle tejto Zmluvy, najmä (nie však výlučne) zabezpečiť dostupnosť kontaktných osôb a iných pracovníkov Prevádzkovateľa, udeliť potrebné povolenia, prístupy k systémom Prevádzkovateľa a sprístupniť dokumentáciu alebo iné nevyhnutné podklady.

Článok IV.
Nahlasovanie kybernetických bezpečnostných incidentov

1. Dodávateľ je povinný bezodkladne nahlásiť Prevádzkovateľovi každý kybernetický bezpečnostný incident, o ktorom sa dozvie, ako aj všetky skutočnosti majúce vplyv na zabezpečovanie kybernetickej bezpečnosti, a to nasledovným spôsobom:

   a) elektronickou poštou zaslaním elektronickej správy na e-mailovú adresu: bezpecnostny.incident@minedu.sk a **dctech@iedu.sk** (nahlásenie kybernetického bezpečnostného incidentua ostatné skutočnosti majúce vplyv na zabezpečenie kybernetickej bezpečnosti), pričom do predmetu správy uvedie označenie alebo číslo tejto Zmluvy alebo Osobitnej zmluvy. Elektronickú správu zároveň Dodávateľ zašle v kópii na kontaktnú osobu Prevádzkovateľa uvedenú v článku VIII. tejto Zmluvy, alebo

   b) telefonicky na telefónnom čísle Prevádzkovateľa: **+421 2 59374 250**;

   pričom súčasťou hlásenia je aj určenie závažnosti incidentu.

2. Ak v čase hlásenia incidentu stále trvajú prejavy incidentu, Dodávateľ odošle Prevádzkovateľovi neúplné hlásenie aj s odkazom, že ide o neúplné hlásenie. Dodávateľ neúplné hlásenie bez zbytočného odkladu doplní po obnove riadnej a úplnej prevádzky siete a všetkých informačných systémov Prevádzkovateľa.

3. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou incidentov (ďalej len „**Reaktívne opatrenia**"), a to ako na výzvu Prevádzkovateľa, tak aj bez ich výzvy, ak sa o incidente dozvie.

4. Dodávateľ pri reakciách na incidenty spolupracuje výlučne s Prevádzkovateľom, ktorému poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré by mohli mať vplyv na implementáciu Reaktívnych opatrení v budúcnosti.

5. Dodávateľ bez zbytočného odkladu oznámi Prevádzkovateľovi implementáciu Reaktívnych opatrení. Ak o to Prevádzkovateľ požiada, po úspešnej implementácii Reaktívneho opatrenia Dodávateľ predloží návrh bezpečnostných opatrení a postupov, ktoré zabezpečia, že nedôjde k opakovaniu, pokračovaniu či šíreniu incidentu (ďalej len „**Ochranné opatrenie**"). Ak Dodávateľ

nenavrhne ochranné opatrenia alebo ak sú navrhované ochranné opatrenia zjavne neúspešné, Dodávateľ poskytne súčinnosť a bude spolupracovať s Objednávateľom na jeho návrhu.

6. Po implementácii Ochranného opatrenia poskytne Dodávateľ na požiadanie Poskytovateľa súčinnosť pri preverovaní efektívnosti opatrenia.

Článok V.
Zodpovednosť za škodu, sankčný mechanizmus

1. Dodávateľ berie na vedomie, že riadne a včasné neplnenie jeho zmluvných a zákonných povinností v súlade s touto Zmluvou môže spôsobiť Prevádzkovateľovi škody, pričom zodpovednosť za škodu podľa tejto Zmluvy sa bude spravovať primerane úpravou zodpovednosti za škodu a sankčným mechanizmom podľa Osobitnej zmluvy.

Článok VI.
Kontrola a audit

1. Prevádzkovateľ je oprávnený vykonať u Dodávateľa kontrolu alebo audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy. Výdavky spojené s vykonaním auditu znáša Prevádzkovateľ.

2. Dodávateľ sa zaväzuje, že Prevádzkovateľovi umožní kedykoľvek vykonať audit, ktorým si Prevádzkovateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností v oblasti kybernetickej bezpečnosti a tiež bude zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.

3. Akékoľvek nedostatky alebo pochybenia zistené auditom je Dodávateľ povinný odstrániť najneskôr do 90 (slovom: deväťdesiatich) kalendárnych dní odo dňa podpisu písomnej zápisnice z vykonania auditu vypracovanej Prevádzkovateľom a podpísanej oboma Zmluvnými stranami, ktorej obsahom bude detailný popis zistených nedostatkov a pochybení vrátane konkrétnych návrhov opatrení na nápravu.

4. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a v prípade potreby umožniť mu sprístupniť svoje priestory, dokumentáciu , technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, umožniť osobám určených Prevádzkovateľom vstup do svojich priestorov a zabezpečiť im dokumentáciu a technické vybavenie potrebné na plnenie úloh podľa tejto Zmluvy. Výkon auditu však v žiadnom prípade nesmie spôsobiť prerušenie prevádzky a/alebo vážne narušenie obchodnej kontinuitu prevádzky Dodávateľa. Audit nesmie byť vykonávaný pravidelne, maximálne 1-krát (slovom: jedenkrát) za jeden kalendárny rok. Zároveň, výkon auditu nesmie ohrozovať dôvernosť citlivých údajov, ktoré nesúvisia s touto Zmluvou a/alebo Osobitnou zmluvou a musí byť vždy vykonávaný za prítomnosti osoby poverenej Dodávateľom.

5. Prevádzkovateľ je povinný oznámiť Dodávateľovi najmenej 30 (slovom: tridsať) pracovných dní vopred, že chce u Dodávateľa vykonať audit.

6. Prevádzkovateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Prevádzkovateľ a osoby ním určené pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov.

Článok VII.
Mlčanlivosť

1. Zmluvné strany sa v zmysle § 12 ZoKB zaväzujú zachovávať mlčanlivosť o podmienkach spolupráce podľa tejto Zmluvy, ako aj o všetkých skutočnostiach týkajúcich sa druhej Zmluvnej strany (najmä, nie však výlučne, obchodnej povahy), ktoré im boli sprístupnené počas trvania tejto Zmluvy alebo ktoré sa im stali iným spôsobom známe. Uvedené sa týka najmä skutočností týkajúcich sa kybernetickej bezpečnosti a osobných údajov príslušníkov/zamestnancov Zmluvných strán. Povinnosť mlčanlivosti trvá aj po skončení tejto Zmluvy alebo Osobitnej zmluvy bez časového obmedzenia.
2. Dodávateľ zabezpečí, aby každý zamestnanec Dodávateľa, ktorý má prístup k informáciám a údajom Prevádzkovateľa a je uvedený v zozname Dodávateľa vedeného podľa čl. III. ods. 9 Zmluvy, dodržiaval mlčanlivosť v rozsahu podľa § 12 ods. 1 ZoKB.
3. Výnimky z povinností podľa tohto článku tejto Zmluvy upravujú najmä ZoKB a iné príslušné všeobecne záväzné právne predpisy.

Článok VIII.
Kontaktné osoby na úseku kybernetickej bezpečnosti

1. Zmluvné strany sú povinné komunikovať pri plnení povinností podľa tejto Zmluvy prostredníctvom kontaktných osôb Zmluvných strán, ktorých kontaktné údaje sú uvedené v tomto čl. VIII. Zmluvy alebo iným vhodným spôsobom, pričom vo všetkých prípadoch musí byť prenos informácií uskutočnený za podmienok umožňujúcich chránený prenos informácií. Konkrétny spôsob a formu takého oznámenia budú Zmluvné strany voliť podľa hľadiska účelnosti a naliehavosti nahlasovaných informácií.
2. Prevádzkovateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:

meno a priezvisko:	Mgr. Miroslav Odor
funkcia/pracovná pozícia:	manažér kybernetickej a informačnej bezpečnosti
telefónne číslo:	+421 2 59374 250
e-mailová adresa:	miroslav.odor@minedu.sk

3. Dodávateľ určuje nasledovnú kontaktnú osobu na úseku kybernetickej bezpečnosti pre komunikáciu s Prevádzkovateľom:

meno a priezvisko:	Ing. Róbert Šimek
funkcia/pracovná pozícia:	account manager
telefónne číslo:	+421 910 877 579
e-mailová adresa:	rosimek@ditec.sk

4. Kontaktné osoby podľa bodov 2 alebo 3 tohto článku môže príslušná Zmluvná strana zmeniť, ak bezodkladne a preukázateľne oznámi novú kontaktnú osobu druhej Zmluvnej strane v písomnej forme, a to bez povinnosti uzatvoriť dodatok k tejto Zmluve. V prípade, ak kontaktné osoby majú prístup k informáciám a údajom Prevádzkovateľa a Dodávateľa, sú povinné zachovávať mlčanlivosť podľa § 12 ods. 1 ZoKB.

Článok IX.
Doba trvania, podmienky a spôsob ukončenia Zmluvy

1. Tato Zmluva sa uzatvára na dobu určitú, a to od nadobudnutia jej účinnosti až do skončenia platnosti a účinnosti Osobitnej zmluvy.
2. Túto Zmluvu je možné ukončiť vždy dohodou Zmluvných strán o skončení trvania Zmluvy, a to ku dňu uvedenému v takej dohode.
3. Zmluvné strany sú oprávnené písomne odstúpiť od tejto Zmluvy v prípadoch a z dôvodov podľa Obchodného zákonníka a iných príslušných právnych predpisov vydanými v súlade so ZoKB.
4. Odstúpenie od Zmluvy musí mať písomnú formu, musí byť doručené druhej Zmluvnej strane a musí byť v ňom uvedený konkrétny dôvod odstúpenia, inak je neplatné.
5. Povinnosť doručiť odstúpenie od tejto Zmluvy podľa tohto článku Zmluvy sa považuje v konkrétnom prípade za splnenú dňom prevzatia odstúpenia od tejto Zmluvy alebo odmietnutím prevziať odstúpenie od tejto Zmluvy. Ak sa v prípade doručovania prostredníctvom poštového podniku vráti poštová zásielka s odstúpením od tejto Zmluvy ako nedoručená alebo nedoručiteľná, považuje sa za doručenú dňom, v ktorom poštový podnik vykonal jej doručovanie.
6. Zánik tejto Zmluvy sa netyká tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto Zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy, ku ktorému dôjde do jej zániku.

Článok X.
Záverečné ustanovenia

1. Práva a povinnosti Zmluvných strán touto Zmluvou neupravené sa riadia príslušnými ustanoveniami Obchodného zákonníka, ZoKB a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
2. Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpísania zástupcami Zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.
3. Zmluvné strany sa zaväzujú, že si nebudú vytvárať prekážky pri plnení tejto Zmluvy a vynaložia maximálne úsilie na zmierlivé urovnanie prípadných sporov vzniknutých z tejto Zmluvy. V prípade, že sa nedohodnú formou zmieru, budú svoje spory riešiť na príslušnom všeobecnom súde Slovenskej republiky.
4. Táto Zmluva môže byť menená alebo dopĺňaná len formou postupne číslovaných dodatkov k tejto Zmluve, ktoré musia mať písomnú formu a musia byť podpísané zástupcami Zmluvných strán.
5. V prípade, ak sa akékoľvek ustanovenie tejto Zmluvy stane neplatným, nespôsobí to neplatnosť Zmluvy ako celku. Zmluvné strany sa v takomto prípade zaväzujú vzájomným rokovaním nahradiť

neplatné alebo neúčinné ustanovenie novým ustanovením tak, aby ostal zachovaný obsah, zámer a sledovaný účel Zmluvy.

6. Neoddeliteľnou súčasťou tejto Zmluvy sú jej prílohy:

   a) Príloha č. 1 – Špecifikácia a rozsah bezpečnostných opatrení,
   b) Príloha č. 2 – Zoznam pracovných rolí.

7. Táto Zmluva bola vyhotovená v štyroch (4) rovnopisoch, dve (2) vyhotovenia pre Prevádzkovateľa, dve (2) vyhotovenia pre Dodávateľa.

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

V Bratislave, dňa .....

Dodávateľ:

_____

DITEC, a.s.
Ing. Csaba Baráth, predseda predstavenstva

V Bratislave, dňa .....

Prevádzkovateľ:

_____

Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky
JUDr. Ing. Tomáš Drucker, MSc., minister

PRÍLOHA č. 1
Špecifikácia a rozsah bezpečnostných opatrení

Konkrétne opatrenia Dodávateľa v jednotlivých oblastiach:

1. Pre oblasť hodnotenia zraniteľností a bezpečnostných aktualizácii Dodávateľ najmä identifikuje technické zraniteľnosti informačných systémov ako celku, prostredníctvom nasledujúcich opatrení
   a) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
   b) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
   c) využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2. Za účelom zabezpečenia konzistentného nasadzovania potrebných softvérových opráv, aktualizácií a plošnej aplikácie aktualizácií na zariadeniach, pre ktoré je softvérová aktualizácia či záplata vydaná Dodávateľ najmä
   a) identifikuje potreby softvérových záplat a aktualizácií,
   b) eviduje softvérové záplaty a aktualizácie a informácie o ich nasadení alebo o dôvodoch ich nenasadenia,
   c) rozhoduje o vhodnom prístupe k otestovaniu softvérových záplat a aktualizácií,
   d) zabezpečuje implementáciu softvérových záplat a aktualizácií,
   e) aktualizuje plán softvérových záplat a aktualizácií.

   Neschválené aktualizácie nie sú prípustné.

3. Pre oblasť ochrany proti škodlivému kódu Dodávateľ zabezpečí nasledovné požiadavky na ochranu proti škodlivému kódu, a to najmä
   a) určenie zodpovednosti používateľov za prevenciu pred škodlivým kódom,
   b) určenie pravidiel pre inštaláciu a používanie systémov prevencie škodlivého kódu,
   c) monitorovanie potenciálnych ciest prieniku škodlivého kódu do prostredia sietí a informačných systémov.

4. Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že
   a) v reálnom čase vykonávajú kontrolu prístupu k digitálnemu obsahu vrátane sieťovej prevádzky, sťahovania, spúšťania alebo otvárania súborov, priečinkov na vymeniteľnom alebo vzdialenom úložisku a prístupu k webovým sídlam a cloudovým službám,
   b) spúšťajú pravidelné kontroly úložísk vrátane cloudových a pripojených vymeniteľných úložísk, najmenej raz ročne,
   c) neoprávneným používateľom je zabránené v prístupe k obsahu prostredníctvom funkcie filtrovania obsahu,
   d) používateľom je zamedzené v pokusoch odinštalovať alebo zakázať funkcie systému na ochranu proti škodlivému kódu.

5. Pre oblasť sieťovej a komunikačnej bezpečnosti realizuje Dodávateľ nasledovné opatrenia:
   a) riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, a to najmä využitím nástrojov na ochranu integrity sietí, ktoré sú zabezpečené segmentáciou sietí, informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len informačné systémy s rovnakými bezpečnostnými požiadavkami, rovnakej kategórie a s podobným účelom,

b) povoľovanie prepojenia medzi segmentmi siete, ktoré sú chránené firewallom, na princípe zásady najnižších privilégií,
c) zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup, napríklad s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,
d) v sieťach sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete,
e) spojenia do externých sietí sú smerované cez sieťový firewall,
f) prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,
g) udržiavanie zoznamu vstupno-výstupných bodov na hranici siete v aktuálnom stave,
h) použitie automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
i) blokovanie neoprávnených spojení zo zdrojov identifikovaných ako škodlivé alebo spôsobujúce hrozby, ak to nastavenie informačného systému umožňuje,
j) neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty,
k) prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
l) implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
m) smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
n) vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
o) vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

6. Pre oblasť riadenia prístupov realizuje Dodávateľ nasledovné opatrenia:
a) riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému,
b) riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb Prevádzkovateľa, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov, a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou,
c) riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu,
d) pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému,
e) zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,
f) využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení,

prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení, a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy),

g) výkon kontroly prístupových účtov a prístupových oprávnení v pravidelných intervaloch, najmenej raz ročne, na overenie súladu schválených oprávnení so skutočným stavom vykonávania oprávnení a detekciu a následné trvalé zablokovanie nepoužívaných prístupových účtov, o čom vedie záznam preukázateľným spôsobom,

h) určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

7. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Dodávateľ nasledovné opatrenia pozostávajúce najmä z riešenia kybernetických bezpečnostných incidentov, ktoré pozostáva najmä z:

a) prípravy a vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov; na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmä
   - postup pri internom nahlasovaní kybernetických bezpečnostných incidentov,
   - postup pri hlásení kybernetických bezpečnostných incidentov podľa § 24 ods. 1 Zákona o KB,
   - postup pri riešení jednotlivých typov kybernetických bezpečnostných incidentov a spôsob ich vyhodnocovania a
   - spôsob evidencie kybernetických bezpečnostných incidentov a použitých riešení, súčasťou evidencie sú na zabezpečenie dôkazu alebo dôkazného prostriedku aj informácie na základe ktorých sa identifikuje vznik a pôvod kybernetického bezpečnostného incidentu,

b) monitorovania a analyzovania udalostí v sieťach a informačných systémoch,

c) detekcie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát,

d) zberu relevantných informácií o kybernetických bezpečnostných incidentoch a z vyhodnocovania kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch,

e) riešenia zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov; proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom
   - pridelenia zodpovednosti a určenia postupov na zvládanie kybernetických bezpečnostných incidentov,
   - zavedenia procesu získavania a uchovávania podkladov potrebných na analýzu kybernetickej bezpečnostnej udalosti a kybernetického bezpečnostného incidentu,
   - prijímania opatrení na odvrátenie alebo zmiernenie vplyvu kybernetického bezpečnostného incidentu,

f) zavedenia pravidelného testovania, najmenej raz ročne, procesu nahlasovania kybernetických bezpečnostných incidentov, v zmysle štandardov a postupov vypracovaných podľa odseku 2, s vedením záznamov o takomto testovaní,
g) vedenia záznamov o kybernetických bezpečnostných incidentoch vrátane použitých riešení, prešetrovania a určenia príčin vzniku kybernetického bezpečnostného incidentu, aktualizácie bezpečnostnej politiky a prijatia primeraných bezpečnostných opatrení zamedzujúcich opakovanému výskytu kybernetického bezpečnostného incidentu a určenia fyzickej osoby zodpovednej za nahlasovanie a odovzdávanie hlásení o kybernetických bezpečnostných incidentoch,
h) vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Prevádzkovateľom.

8. Pre oblasť zaznamenávania udalostí a monitorovania sietí a informačných systémov realizuje Poskytovateľ opatrenia podľa § 15 vyhlášky NBÚ č. 362/2018 Z. z., najmä implementuje centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu
   a) centrálnych sieťových prvkov a serverov,
   b) služieb prístupných do externých sietí,
   c) kritických interných serverov a služieb.

PRÍLOHA č. 2
Zoznam pracovných rolí

Meno a priezvisko pracovníka	Pracovná rola	Dodávateľ/subdodávateľ			E-mail	Telefónny kontakt
		Obchodné meno	IČO	Adresa		