Zmluva o zabezpečení správy IKT a správy sietí, komponentov, plnenia bezpečnostných opatrení a notifikačných povinností

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

(ďalej ako „SLA Zmluva“ alebo „zmluva“)

medzi zmluvnými stranami:

Objednávateľ:

Obchodné meno:	**Centrum podporných služieb**
Sídlo:	Starohájska 6868/10, 917 01 Trnava
IČO:	53 243 188
DIČ:	2121331795
Zastúpená:	Mgr. Ľuboš Krajčír - riaditeľ
Bankové spojenie (názov banky):	Štátna pokladnica

(ďalej ako „Objednávateľ“)

Poskytovateľ:

Obchodné meno:	**Invidia solutions, a.s**
Sídlo:	Klincová 35, 821 08 Bratislava
IČO:	46041958
IČ DPH:	SK2023207230
Osoba oprávnená konať:	Ing. Mariana Veselá
Registrácia:	Obchodný register Mestského súdu Bratislava III, oddiel SRO, vložka č. 70925/B
Bankové spojenie (názov banky):	Všeobecná úverová banka

(ďalej ako „Poskytovateľ“)

(Objednávateľ a Poskytovateľ ďalej spoločne aj ako „zmluvné strany“)

Preambula

Táto zmluva upravuje komplexné poskytovanie správy cloudových služieb Microsoft 365 (Office 365), bezpečnostného riešenia typu Endpoint Detection & Response (EDR), podporných sieťových a hardvérových komponentov, používateľských účtov a súvisiacich technických a organizačných činností. Zmluva je s možnosťou navyšovania počtu podporovaných používateľov z 40 na max. 100.

Zmluva sa uzatvára na základe výsledkov verejného obstarávania na poskytovanie služieb, ktoré vykonal Objednávateľ postupom podlimitnej zákazky bez zverejnenia vo vestníku v súlade s § 108 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov – zákazka s názvom: „Poskytovanie služieb IT podpory a správy IT infraštruktúry“.

Článok I
Predmet zmluvy

1.1 Predmetom tejto zmluvy je poskytovanie služieb Objednávateľovi zo strany Poskytovateľa, pričom rozsah poskytovaných služieb je v rámci paušálu uvedený v Prílohe č. 1 a v rámci objednávkových služieb v Prílohe č. 2, ktoré tvoria neoddeliteľnú súčasť tejto zmluvy (ďalej len „služby“).

1.2 Miestom poskytovania služieb podľa Príloha č. 7 - popis lokalít a pracovísk pre poskytovanie služieb.

1.3 Poskytovateľ sa zaväzuje zaistiť pri poskytovaní služieb Objednávateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany“ v zmysle zákona o kybernetickej bezpečnosti a zároveň plniť podmienky zriaďovateľa Trnavského samosprávneho kraja ako Objednávateľa kritickej základnej služby v pozícií zriaďovateľa CPS.

1.4 Poskytovateľ sa zaväzuje chrániť všetky informácie poskytnuté Objednávateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

1.5 Poskytovateľ vyhlasuje, že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.

1.6 Objednávateľ sa zaväzuje zaplatiť Poskytovateľ za poskytnuté služby cenu Príloha č. 3 tejto zmluvy.

Článok II.

Všeobecné bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

2.1. Poskytovateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy v oblastiach podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti v rozsahu podľa vyhlášky a v rozsahu špecifikovanom v bezpečnostnej politike Objednávateľa.

2.2. Poskytovateľ vykonáva len činnosti, ktoré vyplývajú z podstaty služieb poskytovaných na základe tejto zmluvy, všeobecne záväzných právnych predpisov alebo na základe požiadavky Objednávateľa. Na výkon týchto činností môže poveriť Poskytovateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v Prílohe č. 6 - Zoznam osôb a pracovných rolí Objednávateľa a Poskytovateľa. Poskytovateľ je povinný oznámiť Objednávateľovi každú zmenu v Prílohe č. 6 bezodkladne na e-mailovú adresu kontaktnej osoby Objednávateľa.

2.3. Poskytovateľ je povinný písomne informovať Objednávateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Poskytovateľom na účely plnenia tejto zmluvy.

2.4. Poskytovateľ súhlasí s bezpečnostnou politikou Objednávateľa a s tým, že bezpečnostná politika Objednávateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Objednávateľa a aktuálnym hrozbám dotýkajúcich sa Poskytovateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa. Objednávateľ je povinný bezodkladne oboznámiť Poskytovateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Poskytovateľ následne preukázateľne potvrdí akceptáciu zmien bezpečnostnej politiky.

2.5. Poskytovateľ sa zaväzuje prijímať a dodržiavať najmenej bezpečnostné opatrenia Objednávateľa, ktoré tvoria Prílohu č. 1 k tejto zmluve. Poskytovateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami Objednávateľa.

2.6. Poskytovateľ súhlasí s tým, že bezpečnostné opatrenia Objednávateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov Objednávateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov Objednávateľa, pričom nie je potrebné uzatvoriť dodatok k zmluve. Poskytovateľ sa zaväzuje dodržiavať takto zmenené alebo doplnené

bezpečnostné opatrenia Objednávateľa od okamihu, v ktorom ho s nimi Objednávateľ preukázateľne zoznámi.

2.7. Poskytovateľ je povinný plniť bezpečnostné opatrenia a notifikačné povinnosti v oblasti kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti počas celej doby trvania tejto zmluvy, pokiaľ zo všeobecne záväzných právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Poskytovateľa aj po skončení platnosti a účinnosti tejto zmluvy.

2.8. Poskytovateľ je povinný v rámci prevencie pred kybernetickými incidentmi:

a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez siete a informačné systémy Poskytovateľa nebolo možné ohroziť siete a informačné systémy Objednávateľa,

b) preukázateľne vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy na výkon činností a tejto zmluvy alebo budú mať prístup k dátam alebo informáciám Objednávateľa,

c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,

d) sledovať hrozby, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Objednávateľa,

e) predchádzať vzniku kybernetických incidentov implementovaním najmä bezpečnostných opatrení v prostredí Poskytovateľa,

f) v prípade vzniku kybernetických incidentov v prostredí Poskytovateľa, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,

g) prijímať od Objednávateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Objednávateľa.

h) zasielať Objednávateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a

i) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Objednávateľa.

Článok III.

Mlčanlivosť a dôvernosť informácií

3.1 Poskytovateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy na výkon činností a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. Poskytovateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu Objednávateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa.

3.2 Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.

3.3 Poskytovateľ je povinný chrániť všetky informácie, ku ktorým má prístup na základe tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Objednávateľa alebo osoby spriaznenej s Objednávateľom alebo s ktorými sa oznámil v dôsledku vlastnej činnosti s tým, že všetci dotknutí zamestnanci Poskytovateľa, jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých Poskytovateľ poskytuje služby podľa zmluvy s tretími stranami (ďalej len „tretia osoba“) sú povinní zaviazať sa k zachovávaniu mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

3.4 Poskytovateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba, a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

3.5 Poskytovateľ je povinný zabezpečiť, aby sa každá osoba uvedená v Prílohe č. 3 zaviazala zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti. Tento záväzok mlčanlivosti je Poskytovateľ povinný preukázať Objednávateľovi u každej z týchto osôb.

3.6 Poskytovateľ a Objednávateľ majú zavedenú štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Zmluvné strany spracúvajú osobné údaje podľa 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) (Ú. v. EÚ L 119, 4. 5. 2016) o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3.7 Spracovanie osobných údajov bude upravené zmluvami, ktoré určia záväzky, kompetencie a pravidlá pre správu osobných údajov v prípade, že nastanú okolnosti vyžadujúce ich spracovanie.

Článok I V .

Audit kybernetickej bezpečnosti

4.1 Objednávateľ je oprávnení vyžadovať súčinnosť pri audite u Poskytovateľa audit zameraný na overenie plnenia povinností Poskytovateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Poskytovateľa na plnenie úloh na úsek u kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Poskytovateľa pre plnenie cieľov tejto zmluvy. Výdavky Objednávateľa spojené s vykonaním auditu znáša Objednávateľ.

4.2 Poskytovateľ sa zaväzuje, že Objednávateľovi umožní kedykoľvek vykonať audit, ktorým si Objednávateľ overí mieru a efektívnosť plnenia povinností pokiaľ zákon o kybernetickej bezpečnosti to bude vyžadovať z pozícií Objednávateľa základnej služby alebo z dôvodu požiadaviek z auditu u Objednávateľa základnej kritickej služby Trnavského samosprávneho kraja, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Poskytovateľ 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 Poskytovateľa.

4.3 Prípadné nedostatky zistené auditom je Poskytovateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote šesťdesiat (60) kalendárnych dní.

4.4 Objednávateľ môže audit u Poskytovateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti Objednávateľa pri výkone auditu realizuje Objednávateľom poverená tretia osoba.

4.5 Poskytovateľ je pri audite povinný spolupracovať s Objednávateľom a sprístupniť priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, umožniť osobám určených Objednávateľom voľný vstup do svojich priestorov a zabezpečiť im dokumentáciu a technické vybavenie potrebné na plnenie úloh podľa tejto zmluvy.

4.6 Objednávateľ je povinný oznámiť Poskytovateľovi najmenej desať (10) pracovných dní vopred svoj zámer vykonať u Poskytovateľa súčinnosť pri audite.

4.7 Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje zodpovednosti Poskytovateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.

4.8 Objednávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Objednávateľ a osoby ním určené pri návšteve priestorov Poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny Poskytovateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „BOZP") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné

zdolávanie požiarov (ďalej len „PO“), s ktorými boli v súlade s týmto bodom, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Objednávateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Poskytovateľ. Poskytovateľ je povinný preukázateľne informovať osoby určené Objednávateľom o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Poskytovateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Poskytovateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Poskytovateľa.

Článok V.

Osobitné ustanovenia

5.1 Poskytovateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenia kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti, prípadne sektorové vyhlášky.

5.2 Poskytovateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na Službu Objednávateľa alebo by sa mohli týkať kybernetickej bezpečnosti Objednávateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

5.3 Poskytovateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania a riešenia kybernetických incidentov a dokumentovania školení svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Poskytovateľa podieľať na plnení tejto zmluvy) a na žiadosť Objednávateľa mu predložiť túto dokumentáciu.

5.4 V prípade, ak Poskytovateľ plní túto zmluvu prostredníctvom svojich subPoskytovateľov, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subPoskytovateľov tak, aby boli naplnené ciele tejto zmluvy. Poskytovateľ je povinný zabezpečiť, aby Objednávateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subPoskytovateľov.

5.5 Všetky informácie, ktoré majú vplyv na plnenie tejto zmluvy sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na e-mailové adresy kontaktných osôb uvedené v záhlaví tejto zmluvy a súčasne na e-mailovú adresu riaditeľa a zároveň informovať zriaďovateľa ÚTTSK na incident@trnava-vuc.sk.

5.6 Poskytovateľ vyhlasuje,S že si je vedomý, že neplnenie alebo porušenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť Objednávateľa. Vzhľadom na uvedenú skutočnosť, Poskytovateľ zodpovedá v celom rozsahu za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky a za dôsledky a škodu vzniknutú Objednávateľovi alebo akejkoľvek tretej osobe v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu. Objednávateľ má voči Poskytovateľovi nárok na náhradu preukázateľnej škody, ako aj nárok na náhradu pokút právoplatne uložených orgánmi moci a iných nákladov (napr. povinnosť Objednávateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Objednávateľovi vzniknú v súvislosti s porušením uvedených záväzkov Poskytovateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka.

5.7 V prípade porušenia povinnosti alebo záväzku Poskytovateľa vyplývajúceho mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky, je Poskytovateľ povinný ako nárok Objednávateľa na náhradu škody v plnej výške, ako aj nárok na náhradu pokút právoplatne uložených orgánmi moci a iných nákladov (napr. povinnosť Objednávateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Objednávateľovi vzniknú v súvislosti s porušením povinností Poskytovateľa, tým nie sú dotknuté.

5.8 Po ukončení tejto zmluvy je Poskytovateľ povinný podľa pokynu Objednávateľa vrátiť alebo previesť na Objednávateľa všetky údaje a informácie, ku ktorým mal počas trvania tejto zmluvy prístup, ako aj údaje a informácie získané v súvislosti s plnením tejto zmluvy, resp. tieto údaje a informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane Poskytovateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach Objednávateľa.

5.9 Poskytovateľ bezodkladne po ukončení tejto zmluvy, najneskôr však do troch (3) dní, predloží Objednávateľovi 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 Objednávateľa. Objednávateľ na základe sumarizácie podľa predchádzajúcej vety písomne informuje Poskytovateľa o tom, ktoré podklady a informácie má Poskytovateľ vrátiť Objednávateľovi, previesť na Objednávateľa a ktoré má zničiť. Poskytovateľ

je povinný splniť si povinnosť podľa predchádzajúcej vety najneskôr do piatich (5) dní odo dňa, kedy Objednávateľ informoval Poskytovateľa o spôsobe naloženia s týmito podkladmi a informáciami.

5.10 Po ukončení tejto zmluvy je Poskytovateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Objednávateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania služby ak nevyplýva dlhšia doba trvania Poskytovateľom udelených (poskytnutých) licencií, práv a/alebo súhlasov.

Článok VI
Doba trvania zmluvy, miesto poskytovania služieb

6.1 Zmluva sa uzatvára na dobu určitú v trvaní 12 mesiacov odo dňa nadobudnutia účinnosti.

6.2 Po uplynutí tejto doby môže byť zmluva predĺžená po vzájomnej dohode oboch zmluvných strán písomným dodatkom.

6.3 Ak sa Zmluvné strany nedohodnú inak, miestom poskytovania služieb sú pracoviská Objednávateľa podľa prílohy č. 7 tejto Zmluvy, a ak to technické podmienky umožňujú a ak sa Zmluvné strany na tom dohodnú, Poskytovateľ môže poskytovať služby aj prostredníctvom vzdialeného prístupu. Poskytovateľ je povinný rešpektovať všetky bezpečnostné, organizačné a technické opatrenia a ďalšie relevantné predpisy Objednávateľa spojené s prácou v priestoroch Objednávateľa i s prístupom k informačným technológiám a sieti Objednávateľa, ktoré Objednávateľ poskytol Poskytovateľovi.

Článok VII
Cena a platobné podmienky

7.1 Zmluvné strany sa dohodli, že Objednávateľ je povinný zaplatiť mesačne Poskytovateľovi za služby poskytnuté na základe tejto SLA Zmluvy cenu vo výške 142 188, - EUR s DPH v členení:

Cena bez DPH:	115 600,00 EUR
DPH 23%:	26 588,00 EUR
Cena s DPH:	142 188,00 EUR

celkom (slovom: stoštyridsaťdvatisícstoosemdesiatosem EUR)
(ďalej len ako „**Zmluvná cena**“).

7.2 Zmluvná cena je zložená z nasledujúcich služieb:

a) Prevádzka IT infraštruktúry – podľa počtu zariadení, pri základnom počte 40 ks je cena za mesiac za zariadenie vo výške 2 800,00 EUR bez DPH (slovom dvetisícosemsto EUR). Pri náraste prevádzky IT o 10 ks je cena za mesiac za zariadenie navýšená o 620,00 EUR bez DPH (slovom šesťstodvadsať EUR).

Pri prevádzke IT pre 100 ks je cena za mesiac za zariadenie 5 500,00 EUR bez DPH (slovom päťtisícpäťsto EUR).

b) Správa a zabezpečenie licencií - súčasťou zriadenia služby je konfigurácia licenčného prostredia vrátane napr. Microsoft O365. Za každé zariadenie (licenciu) do počtu 100 ks je stanovená jednotková cena 100,00 EUR bez DPH (slovom jednosto EUR).

c) Správa a zabezpečenie bezpečnostných licencií - týka sa inštalácie a konfigurácie bezpečnostného softvéru. Jednotková cena za túto službu je 1 000,00 EUR bez DPH (slovom jedentisíc EUR).

d) Jednorazové zriadenie servisnej služby - súčasťou zriadenia je aj inštalácia politík a obslužného softvéru. Jednotková cena za túto službu je 5 000,00 EUR bez DPH (slovom päťtisíc EUR).

e) Rozvoj IT systémov - cena za tieto služby bude účtovaná formou manday (jeden pracovný deň špecialistu), a to vo výške 560,- EUR bez DPH (slovom: päťstošesťdesiat EUR) za jeden manday. Cena za 60 manday je vo výške 33 600,00 EUR bez DPH (slovom tridsaťtritisícšesťsto EUR)

7.3 Služby na vyžiadanie, ktoré neboli zahrnuté do pravidelnej mesačnej prevádzky a budú poskytnuté na základe individuálnej požiadavky Objednávateľa, budú účtované samostatne, alebo na základe individuálnej cenovej ponuky, ktorá bude Objednávateľovi pred poskytnutím služby predložená na schválenie. Medzi tieto služby patria najmä, nie však výlučne: ad-hoc konzultácie, mimozmluvné zásahy, pohotovosť mimo štandardného času, implementácie nových riešení, či migrácie systémov. Cena za tieto služby sú definované v prílohe č. 2.

7.4 Poskytovateľ vystaví faktúru za poskytnutie služieb po uplynutí mesiaca, v ktorom boli tieto služby poskytnuté, najneskôr do 15 pracovných dní po skončení kalendárneho mesiaca. Fakturácia bude prebiehať mesačne so splatnosťou 30 pracovných dní odo dňa doručenia na e-mailovú adresu: faktury@cpstt.sk .

7.5 Objednávateľ sa zaväzuje za poskytnuté služby Poskytovateľovi riadne a včas zaplatiť.

7.6 Faktúra musí obsahovať náležitosti faktúry ako daňového dokladu, popis predmetu plnenia a cenu v EUR bez DPH a s DPH s vyčíslením výšky príslušnej DPH.

7.7 V prípade, že faktúra nebude obsahovať náležitosti podľa predchádzajúceho odseku tohto článku Zmluvy alebo bude obsahovať nesprávne údaje, Objednávateľ je oprávnený vrátiť ju Poskytovateľovi a Poskytovateľ je povinný vystaviť novú faktúru s novou lehotou splatnosti.

7.8 Zmluvné strany sa dohodli, že ak v priebehu trvania Zmluvy príde k legislatívnej zmene sadzby DPH, bude cena uvedená v tomto článku upravená v súlade s príslušnou zmenou, a to písomným dodatkom k tejto zmluve.

7.9 V prípade omeškania so zaplatením peňažnej sumy má Poskytovateľ právo žiadať od Objednávateľa úrok z omeškania vo výške podľa Nariadenia vlády Slovenskej republiky č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení Nariadenia vlády č. 303/2014 Z. z.

7.10 V prípade nedodržania reakčného času uvedeného v Prílohe č. 8 tejto Zmluvy Poskytovateľom, je Poskytovateľ povinný poskytnúť Objednávateľovi zľavu zo Zmluvnej ceny v zmysle Článku VII ods. 7.1tejto Zmluvy,:

- vo výške 0,03% za každý, aj začatý deň od uplynutia reakčnej doby.

Článok VIII
Oprávnené osoby a komunikácia

8.1 Zmluvné strany sa dohodli, že osobami oprávnenými komunikovať vo veciach týkajúcich sa poskytovania Služieb podľa tejto SLA Zmluvy (Oprávnená osoba Objednávateľa a Oprávnená /Zodpovedné osoby Poskytovateľa) sú:

a) Za Objednávateľa:

Oprávnená osoba Objednávateľa

Meno a funkcia: Mgr. Ľuboš Krajčír, riaditeľ

b) Za Poskytovateľa:

Oprávnené osoby Poskytovateľa

1. Meno a funkcia: Mgr. Pavol Veselý

2. Meno a funkcia: Mgr. Eva Rusnáková

Článok IX.

Záverečné ustanovenia

9.1. Táto zmluva nadobúda platnosť dňom podpisu ma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.

9.2. Táto zmluva sa uzatvára na dobu určitú, a to do skončenia platnosti a účinnosti

zmluvy, resp. do vyčerpania rámca tejto zmluvy .

9.3. Každá zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade uvedenom vo všeobecne záväznom právnom predpise alebo tejto zmluve. Odstúpenie od tejto zmluvy je možné vykonať v písomnej forme, pričom odstúpenie od zmluvy musí byť riadne doručené druhej zmluvnej strane. V prípade platného odstúpenia od tejto zmluvy sa zmluva považuje za zrušenú momentom doručenia písomného odstúpenia od tejto zmluvy druhej zmluvnej strany

9.4. Objednávateľ je oprávnený odstúpiť od tejto zmluvy v prípade, ak Poskytovateľ poruší akúkoľvek povinnosť alebo záväzok plynúci mu z tejto zmluvy.

9.5. Objednávateľ je oprávnený vypovedať túto zmluvu aj bez udania dôvodu s výpovednou lehotou tri (3) mesiace. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola doručená výpoveď Poskytovateľovi.

9.6. Ukončením tejto zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy okrem práv a povinností, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do skončenia tejto zmluvy.

9.7. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

9.8. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán. Prípadné spory, o ktorých sa zmluvné strany nedohodnú, budú postúpené na rozhodnutie na vecne mieste príslušnému súdu.

9.9. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve, ak táto zmluva neustanovuje inak.

9.10. Kontaktné osoby zmluvných strán a ich kontaktné údaje môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu alebo kontaktné údaje druhej zmluvnej strane v písomnej forme, pričom nie je potrebné uzatvoriť dodatok k zmluve.

9.11. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu neplatných alebo nevykonateľných ustanovení.

9.12. Neoddeliteľnou súčasťou tejto zmluvy sú:

- Príloha č. 1 – Rozsah poskytovaných služieb v rámci paušálu

- Príloha č. 2 – Rozsah poskytovaných služieb v rámci objednávkových služieb
- Príloha č. 3 - Cenová štruktúra zmluvy:
- Príloha č. 4 - Špecifikácia a rozsah bezpečnostných opatrení
- Príloha č. 5 - Spôsob hlásenia bezpečnostného a/alebo prevádzkového incidentu
- Príloha č. 6- Zoznam osôb a pracovných rolí Objednávateľa a Poskytovateľa
- Príloha č. 7- popis lokalít a pracovísk pre poskytovanie služieb
- Príloha č. 8- SLA parametre a metrík, BCM/DRP

9.13. Táto zmluva sa vyhotovuje v štyroch (4) rovnopisoch, po dvoch (2) pre každú zmluvnú stranu.

9.14. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Trnave, dňa 23.9.2025	V Bratislave, dňa 23.9.2025
Mgr. Ľuboš Krajčír v.r.	Ing. Mariana Veselá v.r.
Za Objednávateľa: Mgr. Ľuboš Krajčír riaditeľ	Za Poskytovateľa: Ing. Mariana Veselá predseda predstavenstva

Príloha č. 1 Rozsah poskytovaných služieb v rámci paušálu

v súlade s prílohou č. 4 Špecifikácia a rozsah bezpečnostných opatrení:

a) Správa Microsoft 365
b) správa tenantov, licencií, skupín a rolí;
c) konfigurácia Exchange Online, SharePoint, OneDrive a Teams;
d) implementácia bezpečnostných politík (Conditional Access, MFA, DLP, AIP, Defender for Office 365);
e) zabezpečenie integrácie s doménou cpstt.sk, Entra ID a možnosť prepojenia podľa politík ÚTTSK zo systémami
f) Správa EDR riešenia
g) nasadenie, konfigurácia a správa EDR agentov na koncových zariadeniach;
h) kontinuálne monitorovanie udalostí, automatizovaná detekcia a reakcia, izolácia staníc;
i) Technická podpora a helpdesk, mesačný SLA report (dostupnosť, incidenty, využité licencie, patch status);
j) hotline v pracovných dňoch
k) vzdialená aj osobná asistencia na pracoviskách uvedených v zmluve;
l) podpora pri problémoch s e-mailom, periférami, špecializovanými aplikáciami;
m) správa životného cyklu zariadení, pozáručný servis a priebežná inventarizácia.
n) Prevádzka infraštruktúry a middleware
o) patch management OS Windows Server/Client, Linux podľa potreby;
p) údržba virtuálnych serverov a sieťových prvkov (napr. firewally, VPN, Wi-Fi kontroléry)
q) zálohovanie a obnova (3-2-1 princíp, šifrovanie, testované DR scenáre);
r) vybudovanie a správa sprostredkovateľskej (middleware) vrstvy pre VPN integráciu IS TTSK a tretích strán.
s) Monitoring logov a riešenie možných incidentov
t) Inštalácia a aktualizácia operačných systémov a bezpečnostných
u) Diagnostika a riešenie problémov so softvérom a hardvérom
v) Podpora pri problémoch s perifémymi zariadeniami (tlačiarne, skenery, čítačky kariet
w) Technická asistencia pre zamestnancov
x) Školenia v oblasti IT bezpečnosti a efektívneho využívania IT prostriedkov
y) Pomoc pri obnove zabudnutých hesiel a nastavení účtov
z) Individuálna podpora pri práci so špecializovanými aplikáciami
aa) Nastavovanie a konfigurácia e-mailových klientov a komunikačných nástrojov
bb) Riešenie problémov s tlačou a skenovaním dokumentov
cc) Evidencia zariadení a správa životného cyklu IT techniky

Príloha č. 2 Rozsah poskytovaných služieb v rámci objednávkových služieb

Zmeny funkčnosti sa realizujú nezávisle od paušálnych služieb, vykazujú sa osobitnými výkazmi a fakturujú sa osobitne.

Medzi služby rozvoja sú zaradené aj veľké zmeny funkčnosti, konfigurácie a nastavení, ktoré sú síce vynútené zmenami prevádzkového prostredia Objednávateľa, avšak ich rozsah neumožňuje, aby boli vykonané v rámci malých zmien služieb podpory prevádzky.

Súčasťou realizácie objednávkových služieb rozvoja je zakaždým aj aktualizácia príslušnej dokumentácie.

Na základe Požiadavky na zmenu Poskytovateľ vypracuje rozpočet realizácie zmeny, návrh riešenia, analýzu dopadu, predpokladaný harmonogram prác a návrh akceptačných testov. Proces pokračuje schvaľovacími úlohami a je zakončený objednaním prác. V rámci akceptačného testovania Objednávateľ overí súlad dodaného komponentu s funkčnosťou uvedenou v požiadavke na zmenu. V prípade, ak Objednávateľ zruší alebo preruší objednávku, Poskytovateľ má právo na doteraz vykonané práce vystaviť akceptačný list zrealizovaných prác spolu s faktúrou za poskytnuté služby.

Človekohodina – je merná jednotka pre vykazovanie prácnosti, za ktorú sa považuje 1 (jeden) pracovný manday (60 minút) jedného pracovníka Poskytovateľa. Najmenšia jednotka fakturácie podľa tejto Servisnej zmluvy je 0,5 manday (0,5 MD).

Max. počet je 60 MD za celkové trvanie zmluvy v celkovej sume 560,00 EUR bez DPH za manday.

Rozsah objednávkových služieb:

1. riešenie vzniknutých požiadaviek na zmeny v nastavení siete a zariadení nad rámec paušálnych služieb
2. školenia a preškolenia podľa požiadaviek objednávateľa
3. aktualizácia užívateľskej a technickej dokumentácie
4 upgrade aplikačného sw a ďalších verzii
5 maintenance SW a infraštruktúry

Príloha č. 3 Cenová štruktúra zmluvy:

- Paušálna mesačná sadzba – zahŕňa kompletnú správu, podporu pre užívateľov, údržbu middleware a monitoring;
- prírastkové licencie M365, EDR agent, rozšírenie zálohovacej kapacity;
- Práca nad rámec – vývoj integrácií, komplexné projekty;

Položka	Počet	Jednotka	Cena za zariadenie bez DPH (EUR) Špecifikácia pre výpočet
Prevádzka IT pre 40 užívateľov	40	zariadenie/mes.	Cena × 12 mesiacov
Nárast o 10 užívateľov	1	zariadenie/mes.	Cena × 12 mesiacov
Prevádzka IT pre 100 užívateľov	100	zariadenie/mes.	Cena × 12 mesiacov
Zriadenie a konfigurácia O365	100	ks	jednorazovo
Inštalácia politík a obsl. SW MS 365	1	ks	jednorazovo
Inštalácia a konfigurácia bez. sw EDR	1	ks	jednorazovo
Rozvoj IT systémov	60	MD	Počas trvania zmluvy

Príloha č. 4 Špecifikácia a rozsah bezpečnostných opatrení

Personálna bezpečnosť

1. Poskytovateľ zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.
2. Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
3. Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
4. Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.

5. Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov, najmä:

    a. prideľovanie prístupových práv,

    b. zásady tvorby a používania hesiel,

    c. zásady ochrany pred infiltráciou škodlivým kódom,

    d. zásady bezpečného používania elektronickej pošty, e. zásady bezpečného používania internetu,

    f. zásady bezpečného používania komunikačných nástrojov a sociálnych sietí, g. zásady používania prenosných zariadení a médií,

    h. zálohovanie údajov,

    i. riešenie kybernetických bezpečnostných incidentov, ochranu fyzického majetku,

    k. pohyb v priestoroch Poskytovateľa.

6. Zavedenie procesu preukázateľného poučenia a oznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.

7. Zavedenie procesu preukázateľného oznámenia správcov informačných technológií správy s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.

8. Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, ako aj opatreniami a postupmi zavedenými v organizácii správcu na ich elimináciu najmenej raz za rok.

9. Oznámenie so zamestnancom, na ktorého je možné sa obracať s otázkami a nejasnosťami pri používaní informačných technológií správy a bezpečnostných mechanizmov informačných technológií správy.

Riadenie prístupov

1. Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií správy.

2. Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií správy.

3. Zavedenie pravidiel na zmenu používateľských hesiel.

4. Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.

5. Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.

6. Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.

7. Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.

8. Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá umožní používateľom najmä:

    a. zabezpečiť absolútnu kontrolu nad heslom svojho používateľského účtu,

    b. presadzovať určenú štruktúru hesla,

    c. vyžadovať pravidelnú zmenu hesla,

    d. uchovávať a prenášať používateľské heslá bezpečným spôsobom.

9. Zabezpečenie formálneho riadenia a autorizácie prideľovania privilegovaných prístupov do informačných technológií správy a ich obmedzenie len na nevyhnutné prípady.

10. Preskúmavanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za rok.

11. Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií správy a na prácu na diaľku.

12. Automatické zaznamenávanie každého prístupu administrátora do informačných technológií správy a automatické zaznamenávanie prístupu používateľa.

13. Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií správy.

14. Implementácia centrálnej správy identít (IDM)

15. Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok.

16. Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných

prístupových oprávnení a ich preskúmavanie každých 12 mesiacov.

17. Implementácia, vynucovanie prístupových rolí v informačných technológiách správy.

18. Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov 12 mesiacov.

Bezpečnosť pri prevádzke informačných systémov a sietí

1. Na účinnú prevenciu pred stratou dát u Poskytovateľa sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru, prevádzkových systémov u ktorých sa vykonáva správa, napr. prístupový systém, kamerový systém a pod.
2. Poskytovateľ vypracuje a dodržiava politiku zálohovania, ktorá definuje požiadavky Objednávateľa na zálohovanie vrátane doby uchovávania, testovania záloh, ako aj opatrenia na ochranu záložných médií.
3. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykateľného priestoru.
5. Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.
6. Zabezpečenie vykonania testu obnovy informačných technológií správy a údajov z prevádzkovej zálohy najmenej raz za rok.
7. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.
8. Prevádzkové postupy informačných technológií správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú.
9. Všetky zmeny v prevádzkovaných informačných technológiách správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.
10. Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrh

adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.

11. Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.

12. V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.

13. Na jednotlivých prvkoch informačných technológií správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií správy:

    a. operačné systémy,

    b. virtualizácie prostredie pokiaľ je prevádzkované

    c. aplikačný softvér,

    d. pracovné stanice,

    e. sieťové zariadenia, vrátane bezpečnostných zariadení,

    f. databázové prostredia, pokiaľ je prevádzkované

    g. webové prostredia, pokiaľ je prevádzkované

14. Monitorovanie informačných technológií správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.

15. Vzájomné oddelenie vývojového, integračného, pred produkčného a produkčného prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

Hodnotenie zraniteľností a bezpečnostné aktualizácie

Nastavenie automatickej aktualizácie operačného systému a aplikácií.

1. Poskytovateľ zavedie pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.

2. Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných Poskytovateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.

3. Vykonávanie hodnotenie zraniteľností najmenej polročne.

4. Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných technológií.

5. Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií.

6. Jednotlivé prvky informačných technológií správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií správy.

7. Primárnymi zdrojmi na identifikáciu nových zraniteľností a bezpečnostných aktualizácií sú:

   a. informácie zo systémov a automatizovaných technológií pre aktualizáciu,

   b. informačný servis výrobcov technológií,

   c. výstupy z bezpečnostných technológií,

   d. výsledky penetračných testov,

   e. oznámenia a varovania orgánov štátnej správy a autorít v oblasti kybernetickej bezpečnosti,

   f. webové stránky a portály spoločností zameraných na publikovanie zraniteľnosti pokiaľ sú v správe Poskytovateľa

9. Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií.

10. Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou.

11. Po implementácii aktualizácie sa aktualizuje prvok informačných technológií správy verifikovaný, najmä jeho správna funkcionalita.

12. Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť (6) mesiacov.

13. Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.

Ochrana proti škodlivému kódu

1. Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom.
2. V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.
3. Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na:
    a. používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD, b. škodlivé e-mailové prílohy a odkazy,
    c. podozrivé a škodlivé webové stránky a odkazy,
    d. externú a internú sieťovú komunikáciu u Poskytovateľa vrátane webových sídiel, e. prenos súborov z externých sietí.
4. Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.
5. Zavedenie ochrany informačných technológií správy pred škodlivým kódom najmenej v rozsahu:
    a. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
    b. detekcie prítomnosti škodlivého kódu na všetkých používaných informačných technológiách správy,
    c. kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
    d. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu.
6. Zavedenie ochrany pred nevyžiadanou elektronickou poštou pokiaľ je v správe Poskytovateľa
7. Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov sieti v správe Poskytovateľa

Sieťová a komunikačná bezpečnosť

1. Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu.
2. Na sieťových zariadeniach sa implementujú najmenej tieto bezpečnostné opatrenia:

a. pravidelná aktualizácia firmvéru,

b. zmena továrensky nastavených autentifikačných údajov,

c. pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,

d. vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu.

3. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.

4. Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.

5. Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.

6. Správa počítačových sietí je riadená a kontrolovaná.

7. Pri prenose údajov prostredníctvom siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb.

8. Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment.

9. Sieťové služby, používatelia a jednotlivé prvky informačných technológií správy musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni.

10. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia.

11. Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu.

12. Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov.

13. Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami.

14. Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu.

15. Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii.

16. Vzdialený prístup do vnútornej siete Poskytovateľa musí podliehať autentifikácii a autorizácii.

17. Poskytovateľ implementuje technológiu detekcie a prevencie firewall najmenej na perimetri siete umiestnenej pred chránenú časť siete pokiaľ je firewall aplikovaný

18. Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom pokiaľ sú v správe Poskytovateľa.

Zaznamenávanie udalostí a monitorovanie

Zaznamenávanie úspešných a neúspešných autentifikačných udalostí.

1. Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií .
2. Pre každý prvok informačných technológií správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií musia byť podľa tejto špecifikácie nakonfigurované.
3. Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej tieto udalosti:
    a. úspešné a neúspešné autorizačné udalosti,
    b. úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
    c. úspešné a neúspešné prístupy k log súborom,
    d. úspešné a neúspešné prístupy k systémovým zdrojom,
    e. vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
    f. zmeny v prístupových oprávneniach,
    g. aktivácia a deaktivácia bezpečnostných mechanizmov,
    h. spustenie a zastavenie procesov,

i. konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,

j. spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,

k. významné aktivity v sieťovej komunikácii,

l. požiadavka na autentizačné služby vrátane označenia požadujúcej entity,

m. IP adresy pridelené prostredníctvom služby DHCP.

4. Jednotlivé záznamy v log súboroch obsahujú najmenej tieto informácie o každej zaznamenanej udalosti, ak sú k dispozícii:

   a. čas a dátum udalosti,

   b. identifikácia používateľa,

   c. identifikácia zariadenia,

   d. informácia týkajúca sa udalosti,

   e. indikácia úspešnosti, alebo zlyhania operácie,

   f. pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port.

5. Záznamy udalostí sa uchovávajú najmenej 12 mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.

6. Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.

7. Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.

8. Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií správy synchronizovaný prostredníctvom presného časového zdroja.

9. Poskytovateľ vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií správy.

10. Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.

11. Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva

automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.

12. Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.
13. Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.
14. Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením.
15. Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

Fyzická bezpečnosť a bezpečnosť prostredia

1. Informačné technológie sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.
2. Umiestnenie informačných technológií správy v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa.
3. Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami.
4. Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám.
5. Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj pravidlá:
    a. údržby, uchovávania a evidencie technických komponentov informačných technológií správy a zariadení informačných technológií správy,

b. používania zariadení informačných technológií správy na iné účely, než na aké sú pôvodne určené,

c. používania zariadení informačných technológií správy mimo určených priestorov,

d. vymazávania, vyraďovania a likvidovania zariadení informačných technológií správy a všetkých typov relevantných záloh,

e. prenosu technických komponentov informačných technológií správy alebo zariadení informačných technológií správy mimo priestorov orgánu riadenia,

f. narábania s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačných technológií správy tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

6. Prvky informačných technológií správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie.

7. Podporná infraštruktúra informačných technológií správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora.

8. Pre informačné technológie správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.

Príloha č. 5 Spôsob hlásenia bezpečnostného a/alebo prevádzkového incidentu

1. Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v záhlaví tejto zmluvy.

2. Pri nahlasovaní incidentu je potrebné uviesť, že sa jedná o bezpečnostný incident v zmysle tejto zmluvy a tiež kontaktnú osobu, s ktorou je možné komunikovať za účelom získania dodatočných informácií súvisiacich s procesom analýzy a riešenia bezpečnostného incidentu.

3. Samotný spôsob a forma hlásenia bezpečnostné incidentu sa bude riadiť platným predpisom Objednávateľa – „Riadenie bezpečnostných a prevádzkových incidentov“.

Príloha č. 6 Zoznam osôb a pracovných rolí Objednávateľa a Poskytovateľa

A. <u>Objednávateľ:</u>

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	E-mail
		Zodpovednosť za realizáciu projektu		
		Osoba zodpovedná za SLA		

B. <u>Poskytovateľ:</u>

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	E-mail
Pavol Veselý	Projekt manager	Zodpovednosť za realizáciu projektu		
Eva Rusnáková	SLA manager	Osoba zodpovedná za SLA		

Príloha č. 7 – popis lokalít a pracovísk pre poskytovanie služieb

Centrum podporných služieb je príspevková organizácia zriadená trnavským samosprávnym krajom na zabezpečenie podpornej činnosti v oblasti investícií, správy majetku, prevádzky v rámci Trnavského samosprávneho kraja.

Centrum podporných služieb (CPS) má sídlo na Starohájskej 10 v Trnave a s pracoviskami v rámci trnavského kraja na ktorých sú detašovaní zamestnanci CPS. Spoločnosť je založená jediným spoločníkom - Trnavským samosprávnym krajom.

Spoločnosť na svoju činnosť využíva priestory a pracoviská nachádzajúce v rôznych lokalitách, servisné služby budú poskytované na pracoviskách v týchto lokalitách:

Adresa	**Mesto**	**Dostupnosť**
Starohájska 10	Trnava	08:00 do 16:00 hod.
Sibírska 1	Trnava	08:00 do 16:00 hod.
Spojená škola, Námestie sv. Martina 5	Holíč	08:00 do 16:00 hod.
Budova internátu, Štúrova 141/32	Senica	08:00 do 16:00 hod.

Príloha č. 8 - SLA PARAMETRE A METRIKY, BCM/DPR.

A./ parametre

Priorita	**Definícia**	**Maximálny reakčný čas**	**Maximálna doba odstránenia**	**KPI (mesačne)**
P1 – Kritická porucha	Výpadok celej produkčnej služby/komponentu s dopadom na >50 % používateľov alebo nedostupnosti kľúčových dát	≤ 1 h (telefonická eskalácia)	≤ 24 h	Dostupnosť ≥ 99,9 %
P2 – Závažný problém	Výrazné obmedzenie funkcionality bez úplného výpadku, dopad na 10–50 % používateľov	≤ 4 h	≤ 2 prac. dni	MTTR ≤ 16 h
P3 – Štandardná zmena	Bežná servisná požiadavka (oprava účtu, konfigurácia siete atď.)	≤ 8 h	≤ 5 prac. dní	≥ 95 % splnených v termíne
P4 – Menej závažná požiadavka	Konzultačná úloha, nízky dopad, bez výpadku	≤ 3 prac. dni	≤ 10 prac. dní	≥ 90 % splnených v termíne

Časové pokrytie poskytovania Paušálnych služieb

Popis	Parameter	Poznámka
Prevádzkové hodiny	od 8:00 hod. - do 16:00 hod. počas pracovných dní	Pracovné dni
Servisné okno	od 16:00 hod. - do 8:00 hod. počas pracovných dní; 24 hodín od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov	Realizácia servisných zásahov (servisné okná) je vždy mimo prevádzkových hodín (pracovného času).

B./ plán BCM/DR (Business Continuity & Disaster Recovery)

1. Preventívna fáza
   • kvartálna analýza rizík, aktualizácia BIA
   • udržiavanie RPO ≤ 24 hodín a RTO ≤ 24 h pre služby
2. Reakčná fáza
   • aktivácia krízového štábu do 60 min
   • paralelný komunikačný kanál (Signal/Teams Outage Bridge)
3. Obnovovacia fáza
   • fail-over na DR lokalitu (Azure Site Recovery)
   • verifikácia integrity dát (hash-check)
   • postupný návrat na produkčný tenant po root-cause analýze
4. Testovanie
   • tabletop test 1× ročne
   • plný technický DR test min. 1× za 18 mesiacov s výslednou správou pre TTSK
5. Vypracovanie plánu BCM/DRP nie je v paušálnej časti zmluvy