ZMLUVA O POSKYTOVANÍ SLUŽIEB SPRÁVY A ROZVOJA CALL CENTRA A TELEKOMUNIKAČNÉHO PROSTREDIA V SOCIÁLNEJ POISŤOVŇI

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb.,
Obchodného zákonníka v platnom znení

(ďalej len „zmluva“)

objednávateľ:

Názov:	Sociálna poisťovňa
Sídlo:	Ul. 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Ilko generálny riaditeľ Sociálnej poisťovne
IČO:	30 807 484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
SWIFT:	SPSRSKBA

(ďalej len „objednávateľ“) a

dodávateľ:

Názov:	ALCASYS Slovakia, a.s.
Sídlo:	Staré grunty 36 841 04 Bratislava
V mene dodávateľa koná:	Ing. Ján Kostka predseda predstavenstva ALCASYS Slovakia, a.s.
IČO:	35 879 335
DIČ:	2021805764
IČ DPH:	SK2021805764
Bankové spojenie:	[redacted]
IBAN:	
SWIFT:	
Zapísaný v:	Obchodnom registry Mestského súdu Bratislava III, Oddiel: Sa, Vložka číslo: 3296/B.

(ďalej len „dodávateľ“)

(spolu aj ako „zmluvné strany“)

Článok 2
Východiskové podklady

1. Východiskovým podkladom na uzatvorenie tejto zmluvy na poskytovanie služieb správy a rozvoja call centra a telekomunikačného prostredia v Sociálnej poisťovni,; (ďalej len „Zmluva“) sú súťažné podklady a ponuka dodávateľa zo dňa 26.09.2023 predložená objednávateľovi v rámci zadávania nadlimitnej zákazky podľa § 5 ods. 2 a § 66 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene

a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“).

Článok 3
Predmet zmluvy a rozsah

1. Predmetom tejto zmluvy je záväzok dodávateľa poskytovať pre objednávateľa služby pre call centrá, komunikačné systémy a servisné služby spojené s telekomunikačnou technikou a sieťami. Komunikačnými systémami sa rozumejú hlasové komunikačné systémy (IPPBX a prislúchajúce koncové zariadenia), informačo-poradenské centrum (IPC) a s ním spojené služby, telekomunikačné siete (fyzické siete na pracoviskách a súvisiace LAN komponenty), opravy a výmeny vadných komponentov a zmenové požiadavky podľa požiadaviek objednávateľa. Dodávateľ sa zaväzuje poskytovať predmetné služby v rozsahu:
    1.1. Zabezpečenie obnovy licencií bližšie uvedených v bodoch 1.1.1-1.1.15 Prílohy č. 1 tejto zmluvy,
    1.2. Zabezpečenie licencií bližšie uvedených v bodoch 1.2.1-1.2.10 Prílohy č. 1 tejto zmluvy,
    1.3. Zabezpečenie služieb technickej podpory komunikačných systémov a servisných služieb, ktoré sú bližšie špecifikované v bodoch 1.3.1-1.3.11 Prílohy č. 1 tejto zmluvy,
    1.4. Dodanie hardvérových komponentov k poskytovaným službám uvedených v bodoch 1.4.1-1.4.38 Prílohy č. 1 tejto zmluvy,
    1.5. Poskytovanie servisnej starostlivosti bližšie špecifikovanej v bodoch 1.5.1-1.5.6 Prílohy č. 1 tejto zmluvy.
2. Cenová kalkulácia, množstvo a detailná špecifikácia predmetu zmluvy je uvedená v Prílohe č. 1 tejto zmluvy.
3. Dodávateľ sa zaväzuje poskytovať objednávateľovi špecifikované služby vrátane dodania príslušných hardvérových komponentov počas štyridsaťosem (48) mesiacov odo dňa účinnosti tejto zmluvy.
4. Objednávateľ sa zaväzuje za užívanie poskytnutých služieb zaplatiť cenu dohodnutú v Prílohe č. 1 Cenová kalkulácia k tejto zmluve, množstvo a podrobná špecifikácia predmetu zmluvy.
5. Dodané hardvérové komponenty môže objednávateľ odmietnuť prevziať, ak objednávateľ zistí preukázateľné vady, nedostatočnú kvalitu alebo tiež v prípade, ak nie sú hardvérové komponenty dodané za dohodnutú cenu.

Článok 4
Miesto dodania, množstvo, termín a spôsob plnenia

1. Miestom dodania predmetu zmluvy sú lokality objednávateľa – ústredie, pobočky uvedené v tabuľke č. 1 Prílohy č. 1 tejto zmluvy a vysunuté pracoviská uvedené v tabuľke č. 2 Prílohy č. 1 k tejto zmluve.

2. Dodávateľ sa zaväzuje dodávať jednotlivé položky predmetu zmluvy na základe objednávok vystavených objednávateľom. V prípade objednania:
    a. predmetu zmluvy podľa článku 3 tejto zmluvy, ktorého dodaním bude obnovená doterajšia služba, zriadená nová služba alebo nová funkcionalita, dodaná systémová zmena s prácnosťou v rozsahu do tridsať (30) človekodní alebo dodaný nový hardvérový komponent - do lehoty desiatich (10) pracovných dní odo dňa preukázateľného doručenia objednávky dodávateľovi,
    b. riešenia technických porúch/incidentov v lehotách, ktoré sú bližšie špecifikované v tabuľke č. 4 a tabuľke č. 5 Prílohy č. 2 k tejto zmluve, stanovených podľa času na úplné odstránenie technickej poruchy od nahlásenia technickej poruchy/požiadavky zo strany objednávateľa – (FT total – fix time total),
    c. systémových zmien väčšieho rozsahu s prácnosťou nad tridsať (30) človekodní (servis na vyžiadanie) v lehote do tridsiatich (30) pracovných dní od preukázateľného doručenia objednávky dodávateľovi.
3. Dodanie licencií a služieb v zmysle článku 3 bod 1.1, 1.2 a 1.3 tejto zmluvy sa bude považovať za splnené na základe preberacieho protokolu.
4. Dodanie hardvérových komponentov v zmysle článku 3 bod 1.4 tejto zmluvy bude splnené odovzdaním a prevzatím v mieste dodania zodpovedným zástupcom objednávateľa, ktorý vykoná kontrolu druhu, kvality, rozsahu, množstva a ceny.

Článok 5
Cena

1. Cena za predmet tejto zmluvy podľa článku 3 bod 1.1 až 1.5 je stanovená dohodou zmluvných strán v EUR, v súlade so zákonom NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhláškou MF SR č. 87/1996 Z. z. v znení neskorších predpisov, ktorou sa vykonáva zákon NR SR č. 18/1996 Z. z o cenách v znení neskorších predpisov.
2. Celková cena za predmet tejto zmluvy je 6 807 000,00 EUR bez DPH (slovom: šesťmiliónov osemstosedemtisíc eur). Celková cena vrátane DPH je 8 168 400,00 EUR s DPH, (slovom: osemmiliónov stošesťdesiatosemtisícštyristo eur).
3. Podrobná cenová kalkulácia predmetu tejto zmluvy vrátane jednotkových cien je uvedená v Prílohe č. 1 k tejto zmluve.

   Dodávateľ je platcom DPH. DPH bude účtovaná v aktuálnej sadzbe podľa všeobecne záväzných právnych predpisov, platných v čase zdaniteľného plnenia.
4. Celková cena za predmet tejto zmluvy a jednotkové ceny podľa Prílohy č. 1 k tejto zmluve obsahujú všetky náklady dodávateľa spojené s dodaním predmetu tejto zmluvy vrátane súvisiacich služieb uvedených v článku 3 v bode 1 tejto zmluvy a tiež všetky dane, clá, poplatky, platby vyberané v rámci uplatňovania nesadzobných opatrení ustanovené osobitnými predpismi, ako aj iné náklady súvisiace s plnením predmetu tejto zmluvy.
5. Dodávateľovi nevznikne nárok na úhradu žiadnych dodatočných nákladov, ktoré si nezapočítal do ceny predmetu tejto zmluvy.

Článok 6
Platobné podmienky

1. Zmluvné strany sa dohodli, že úhrada za predmet tejto zmluvy podľa článku 3 bod 1 bude realizovaná formou bezhotovostného platobného styku bez zálohovej platby na základe splnenia predmetu tejto zmluvy. Dodávateľ berie na vedomie a súhlasí, že nie je oprávnený požadovať zaplatenie ceny na iný bankový účet než ten, ktorý je uvedený v záhlaví zmluvy; k zmene bankového účtu, na ktorý bude objednávateľ uhrádzať svoje splatné záväzky zo zmluvy môže dôjsť iba uzavretím dodatku k zmluve, predmetom ktorého bude zmena čísla IBAN a/alebo kódu SWIFT (BIC) bankového účtu dodávateľa v záhlaví zmluvy.
2. Každá požiadavka na zriadenie alebo rozšírenie služby, dodanie alebo obnovu licencií, alebo dodanie tovaru dodávateľom bude zadaná cez ServisDesk objednávateľa. Dodávateľ na požiadavku spracuje konkrétnu cenovú ponuku podľa zodpovedajúcich položiek jednotkového cenníka Prílohy č. 1 k tejto zmluve. Dodávateľ poskytne služby/dodá tovar/licencie po schválení ponuky objednávateľom. Po poskytnutí služby/dodaní tovaru/licencie podpíšu obe strany preberací protokol/, ktorý tvorí podklad na fakturáciu. Fakturáciu za vykonané služby/dodané tovary zrealizuje dodávateľ raz mesačne/štvrťročne do pätnástich (15) kalendárnych dní po ukončení príslušného mesiaca/kalendárneho štvrťroka.
3. Jednotlivé čiastkové úhrady za predmet tejto zmluvy budú realizované na základe samostatného daňového dokladu – faktúry. Dodávateľovi vznikne právo na vystavenie faktúry dňom riadneho a včasného dodania predmetu tejto zmluvy podľa článku 4 tejto zmluvy. Neoddeliteľnou súčasťou faktúry za dodanie služieb podľa článku 3 bod 1.1 až 1.5 tejto zmluvy je /preberací protokol preukazujúci dodanie jednotlivých čiastkových plnení. Neoddeliteľnou súčasťou faktúry za dodanie tovaru podľa článku 3 bod 1.4 tejto zmluvy je preberací protokol.
4. Faktúra za dodaný tovar musí obsahovať názov a množstvo dodaného tovaru, jednotkovú cenu a fakturovanú sumu za dodaný tovar, sadzbu DPH v % a výšku DPH v EUR, celkovú fakturovanú sumu v EUR bez DPH a celkovú fakturovanú sumu v EUR s DPH.
5. Ak dodanie servisnej starostlivosti podľa článku 3 bod 1.5 tejto zmluvy bude zrealizované za len za čas mesiaca, dodávateľ sa zaväzuje v príslušnom mesiaci faktúrovať len pomerovú časť cenníkovej ceny uvedenej v Prílohe č. 1 k tejto zmluve, t.j. len za tie dni, za ktoré bola servisná starostlivosť reálne poskytnutá.
6. Objednávateľ je oprávnený započítať akúkoľvek svoju i nesplatnú pohľadávku, ktorú má voči dodávateľovi, s pohľadávkou, i nesplatnou, ktorá vznikne z tejto zmluvy objednávateľovi. Zápočet pohľadávok môže objednávateľ voči dodávateľovi uplatniť pri úhrade faktúry dodávateľa.
7. Splatnosť faktúry je najneskôr do tridsať (30) dní odo dňa jej doručenia do podateľne objednávateľa.
8. Dodávateľ sa zaväzuje vyhotovenú faktúru zaslať listinne poštou a súčasne v textovo čitateľnom súbore vo formáte PDF elektronicky na e-mailovú adresu objednávateľa faktury@socpoist.sk, a to bezodkladne po jej vystavení; takto predložená faktúra nesmie byť vo forme obrázku, ale musí byť strojovo čitateľná. Dodávateľ vyhlasuje, že obsah faktúry poslanej poštou sa bude zhodovať s faktúrou poslanou v elektronickej podobe na e-mailovú adresu objednávateľa.

Miestom doručenia faktúry v listinnej forme je Sociálna poisťovňa, ústredie, Ul. 29. augusta 8 a 10, 813 63 Bratislava. Všetky faktúry vyplývajúce z tejto zmluvy podliehajú povinnosti zverejnenia zo strany objednávateľa.

9. Dodávateľom vystavená faktúra ako daňový doklad musí byť vyhotovená v súlade s ustanoveniami zákona č. NR SR 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov. V prípade, ak faktúra vystavená dodávateľom nebude obsahovať všetky zákonom stanovené náležitosti alebo bude obsahovať nesprávne alebo neúplné údaje, objednávateľ má právo takúto faktúru vrátiť dodávateľovi na jej doplnenie, resp. opravu a dodávateľ je povinný podľa charakteru nedostatku vystaviť novú, opravenú, resp. doplnenú faktúru s novou lehotou splatnosti. Dodávateľ je zároveň povinný bezodkladne poslať opravenú alebo novú faktúru znovu aj v elektronickej podobe na e-mailovú adresu uvedenú v predchádzajúcom bode tohto článku tejto zmluvy.
10. Dodávateľ nie je oprávnený postúpiť pohľadávku voči objednávateľovi na tretiu osobu.
11. Zmluvné strany sa dohodli, že objednávateľ má právo znížiť cenu o hodnotu zmluvnej pokuty dohodnutej v tejto zmluve, uplatnenej objednávateľom voči dodávateľovi.

Článok 7
Nadobudnutie vlastníckeho práva

1. Užívacie právo k dodanému tovaru podľa článku 3 bod 1.4 tejto zmluvy nadobudne objednávateľ momentom dodania – podpísania dodacieho listu. Objednávateľ nadobudne vlastnícke právo k tovaru dňom riadneho splnenia záväzku, t. j. písomným odovzdaním a prevzatím predmetu tejto zmluvy na dodacom liste.

Článok 8
Zodpovednosť za vady, záruka a záručná doba

1. Dodávateľ sa zaväzuje, že poskytne predmet zmluvy podľa podmienok dohodnutých v tejto zmluve a v Prílohe č. 1 k tejto zmluve.
2. Dodávateľ sa zaväzuje, že dodá tovar podľa článku 3 bod 1.4 tejto zmluvy, ktorý je schválený na dovoz a predaj v Slovenskej republike, resp. v rámci Európskej únie a bude vyhovovať platným medzinárodným normám, STN licenciám a všeobecne záväzným právnym predpisom.
3. Dodávateľ sa zaväzuje, že tovar v čase odovzdania objednávateľovi a počas stanovenej záručnej doby bude funkčný a spĺňať vlastnosti položiek a komponentov stanovené podľa Prílohy č. 1 k tejto zmluve.
4. Ak má tovar vady už v čase odovzdania a preberania, objednávateľ tovar neprevezme a vráti ho dodávateľovi, ktorý je povinný vady odstrániť do tridsiatich (30) kalendárnych dní, ak sa zmluvné strany v konkrétnom prípade s prihliadnutím na charakter vád nedohodnú inak. Do času, kým dodávateľ nedodá tovar bez vád, je v omeškaní s dodaním tovaru.

5. Dodávateľ zodpovedá za vady, ktoré má tovar v okamihu, keď prechádza nebezpečenstvo škody na tovare na objednávateľa a za vady tovaru, ktoré sa vyskytnú po prevzatí tovaru v záručnej dobe.
6. Dodávateľ je povinný poskytovať služby v zmysle tejto zmluvy kvalitne a s vynaložením odbornej starostlivosti.
7. Dodávateľ zodpovedá objednávateľovi za škodu, ktorá vznikne objednávateľovi v súvislosti s vadami poskytnutých služieb alebo iných úkonov vykonaných poskytovateľom podľa tejto zmluvy.
8. V prípade riadneho oznámenia vád poskytnutých služieb a iných úkonov vykonaných poskytovateľom podľa tejto zmluvy má objednávateľ právo požadovať a poskytovateľ povinnosť bezplatne odstrániť vady v lehote do tridsať (30) dní od oznámenia.
9. Dodávateľ je povinný začať s odstraňovaním vady služieb poskytnutých poskytovateľom podľa tejto zmluvy bez zbytočného odkladu od oznámenia.
10. Dodávateľ nezodpovedá za vady vzniknuté v dôsledku neodborného zásahu alebo neodborného užívania zo strany objednávateľa alebo tretích osôb.
11. V prípade sporu o zodpovednosť za vadu je dodávateľ povinný reklamovanú vadu poskytnutých služieb a iných úkonov vykonaných dodávateľom podľa tejto zmluvy odstrániť v termíne určenom objednávateľom.
12. Zmluvné strany sa dohodli, že dodávateľ odstraňuje vady v lokalite objednávateľa podľa Prílohy č. 1 k tejto zmluve, t.j. na mieste, kde vada vznikla na vlastné náklady.
13. Ak dodávateľ neodstráni vady v lehotách určených v tejto zmluve, je objednávateľ oprávnený po písomnej výzve adresovanej poskytovateľovi vykonať odstránenie vád samostatne alebo ich vykonaním poveriť tretiu osobu. Takto vzniknuté náklady je dodávateľ povinný uhradiť objednávateľovi do štrnástich (14) kalendárnych dní odo dňa doručenia faktúry o ich vyúčtovaní. Ustanovenie tohto odseku tohto článku zmluvy nemá vplyv na zodpovednosť dodávateľa za ďalšie vady, resp. na dodávateľom poskytnutú záruku.
14. Dodávateľ sa zaväzuje, že na predmete tejto zmluvy podľa článku 3 bod 1.1 až 1.3 tejto zmluvy nie sú žiadne právne vady a vyhlasuje, že je oprávnený vykonávať a udeliť všetky práva spojené s dodaním predmetu zmluvy a zodpovedá za ich nerušený výkon objednávateľom.
15. V prípade, že tretia osoba akýmkoľvek spôsobom uplatní práva na dodaný predmet zmluvy, ktoré sú nezlučiteľné s právami vykonávanými objednávateľom, dodávateľ sa zaväzuje vykonať všetky opatrenia potrebné na nápravu a nerušený výkon práv objednávateľa, vrátane prípadných návrhov na začatie súdneho konania.
16. Dodávateľ poskytne objednávateľovi na realizované plnenie predmetu zmluvy podľa článku 3 bod 1.1 až 1.4 tejto zmluvy záručnú dobu dvadsaťštyri (24) mesiacov, ktorá začne plynúť od ich protokolárneho odovzdania a prevzatia. Záruka sa vzťahuje na prevádzkyschopnosť a funkčnosť predmetu zmluvy podľa článku 3 bod 1.1 až 1.3 tejto zmluvy za predpokladu riadnej starostlivosti a údržby predmetu zmluvy objednávateľom.
17. Dodávateľ poskytne objednávateľovi na realizované plnenie predmetu zmluvy

podľa článku 3 bod 1.5 tejto zmluvy záručnú dobu dvanásť(12) mesiacov, ktorá začne plynúť od ich protokolárneho odovzdania a prevzatia.

18. Práva zo zodpovednosti za vady, ktoré sa vyskytnú v záručnej dobe musí objednávateľ uplatniť u dodávateľa v záručnej dobe, inak zanikajú.
19. Dodávateľ sa zaväzuje, že počas záručnej doby bezplatne (vrátane dopravy) odstráni vady predmetu zmluvy najneskôr do sedemdesiatdva (72) hodín od telefonického hlásenia vady (poruchy), následne potvrdenej e-mailovou správou na dohodnutej e-mailovej adrese objednávateľa dispecing@socpoist.sk.
20. Odstránením vád sa rozumie zabezpečenie prevádzkyschopnosti predmetu zmluvy tak, aby bola zabezpečená minimálne v takom rozsahu a kvalite ako pred vznikom vady (poruchy).
21. Ak pôjde o vadu, ktorá by mohla spôsobiť alebo spôsobila na predmete zmluvy vznik havarijného stavu, dodávateľ sa zaväzuje nastúpiť na odstránenie vád bezodkladne od ich oznámenia objednávateľom, ktoré v tomto prípade môžebyť telefonické na čísle [redacted] alebo prostredníctvom e-mailu [redacted].
22. Pri zodpovednosti za vady sa zmluvné strany budú riadiť ustanoveniami § 422 a nasl. Obchodného zákonníka.

Článok 9

Zmluvné pokuty, úrok z omeškania a náhrada škody

1. V prípade omeškania dodávateľa s poskytnutím súvisiacich služieb uvedených v článku 3 bod 1.1 až 1.3 tejto zmluvy v termínoch dohodnutých v článku 4 tejto zmluvy, je objednávateľ oprávnený uplatniť si nárok na zmluvnú pokutu vo výške 5% z hodnoty nedodanej služby a to za každý, aj začatý deň omeškania, ak sa zmluvné strany nedohodnú inak. Dodávateľ sa zaväzuje, že takúto zmluvnú pokutu zaplatí objednávateľovi najneskôr do tridsať (30) dní odo dňa jej uplatnenia.
2. V prípade omeškania dodávateľa s dodaním tovaru podľa článku 3 bod 1.4 tejto zmluvy termíne dohodnutom v článku 4 tejto zmluvy, je objednávateľ oprávnený uplatniť si nárok na zmluvnú pokutu vo výške 5% z hodnoty nedodaného tovaru a za každý, aj začatý deň omeškania, ak sa zmluvné strany nedohodnú inak. Dodávateľ sa zaväzuje, že takúto zmluvnú pokutu zaplatí objednávateľovi najneskôr do tridsať (30) dní odo dňa jej uplatnenia.
3. V prípade, ak je dodávateľ v omeškaní s vybavením oprávnenej reklamácie podľa článku 8 bod 8 tejto zmluvy, objednávateľ je oprávnený uplatniť si nárok na zmluvnú pokutu vo výške 5 % z hodnoty nedodaného tovaru a za každý, aj začatý deň omeškania, ak sa zmluvné strany nedohodnú inak. Dodávateľ sa zaväzuje, že takúto zmluvnú pokutu zaplatí objednávateľovi najneskôr do tridsať (30) dní odo dňa jej uplatnenia.
4. V prípade omeškania dodávateľa s pravidelným reportovaním stavu úloh za definované obdobie (raz za ¼ rok ku 10 dňu po ukončení predchádzajúceho kalendárneho štvrťroka vyhodnocovací meeting s objednávateľom v zmysle prílohy č. 2), bude objednávateľ oprávnený uplatniť si nárok na zmluvnú pokutu

vo výške 250 EUR za každý deň omeškania s vykonaním tejto povinnosti.

5. V prípade omeškania objednávateľa s úhradou faktúry v dohodnutej lehote, je dodávateľ oprávnený uplatniť si nárok na úrok z omeškania maximálne vo výške určenej nariadením vlády Slovenskej republiky č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení nariadenia vlády č. 303/2014 Z. z. Takto uplatnený úrok z omeškania je objednávateľ povinný uhradiť do tridsať (30) dní odo dňa doručenia jeho vyúčtovania na základe faktúry.
6. Objednávateľ má právo uplatniť si nárok na dohodnuté zmluvné pokuty voči dodávateľovi aj po odovzdaní predmetu zmluvy, ak dodatočne zistí, že dodávateľ porušil záväzky dohodnuté v zmluve.
7. Uhradením zmluvných pokút nezaniká nárok objednávateľa na náhradu škody, ktorá prevyšuje výšku zmluvnej pokuty a nezaniká povinnosť, pre porušenie ktorej bola sankcia uložená.
8. Pri nebezpečenstve škody na predmete tejto zmluvy platia ustanovenia § 455 a nasl. Obchodného zákonníka.
9. V súlade s § 364 Obchodného zákonníka sa zmluvné strany dohodli na započítaní vzájomných pohľadávok. Objednávateľ je oprávnený započítať zmluvné pokuty podľa tohto článku tejto zmluvy proti cene za predmet zmluvy.
10. V prípade vzniku škody porušením povinností vyplývajúcich z tejto zmluvy budú zmluvné strany postupovať v súlade s príslušnými ustanoveniami Obchodného zákonníka.
11. Úhradou zmluvnej pokuty sa dodávateľ nezbavuje povinnosti pokračovať v plnení predmetu tejto zmluvy, ani nahradiť škodu, ktorá porušením povinností vznikla.

Článok 10
Ochrana dôverných informácií a informačná bezpečnosť

1. Zmluvné strany, ich zamestnanci ako aj ich subdodávatelia a ich zamestnanci sú povinní zachovávať v tajnosti všetky dôverné informácie, ktoré sú uvedené v tejto zmluve a v jej prílohách a/alebo ktoré budú uvedené v jej dodatkoch a prílohách, a/alebo ktoré im boli poskytnuté, alebo ktoré inak získali v súvislosti so zmluvou, alebo s ktorými sa oboznámili počas plnenia zmluvy, resp. ktoré súvisia s predmetom plnenia, s údajmi, ktoré podliehajú ochrane podľa zákona č. 18/2018 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 nariadenia o ochrane údajov) (GDPR) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s údajmi získanými v rámci predzmluvných rokovaní, ktoré súvisia s touto zmluvou, s výnimkou nasledujúcich prípadov:
    a) ak je poskytnutie informácie od dotknutej zmluvnej strany uložené na základe všeobecne záväzných právnych predpisov alebo na základe povinnosti uloženej postupom podľa všeobecne záväzných právnych predpisov (napr. zákon 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,

b) ak je informácia verejne dostupná z iného dôvodu, ako je porušenie povinnosti mlčanlivosti dotknutou zmluvnou stranou, informácie, ktoré už sú v deň podpísania zmluvy verejne známe, alebo ktoré je možné už v deň podpísania tejto zmluvy získať z bežne dostupných informačných prostriedkov,

c) ak sa jedná o informácie, ktoré sa stanú po podpísaní zmluvy verejne známymi, alebo ktoré možno po tomto dni získať z bežne dostupných informačných prostriedkov,

d) ak je informácia poskytnutá odborným poradcom dotknutej zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti, alebo ak sa voči dotknutej zmluvnej strane zaviazali povinnosťou mlčanlivosti,

e) ak je to potrebné pre účely akéhokoľvek súdneho, rozhodcovského, správneho alebo iného konania, ktorého je dotknutá zmluvná strana účastníkom,

f) ak je informácia poskytnutá so súhlasom druhej zmluvnej strany.

2. Dodávateľ sa ako sprostredkovateľ zaväzuje uzavrieť s objednávateľom ako prevádzkovateľom sprostredkovateľskú zmluvu v zmysle článku 28 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 (GDPR) a/alebo podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení, ktorá tvorí Prílohu č. 7 k tejto zmluve.

3. Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej zmluvnej strany nevyužijú pre seba alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k dôverným informáciám. Za tretie osoby sa nepokladajú členovia orgánov zmluvných strán, subdodávatelia, audítori alebo právni poradcovia zmluvných strán, ktorí sú ohľadne im sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.

4. Zmluvné strany, subdodávatelia a ich zamestnanci sa zaväzujú, že všetky zúčastnené osoby a subjekty budú s poskytnutými informáciami a zistenými skutočnosťami nakladať ako s dôvernými informáciami.

5. Dodávateľ sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov realizujúcich predmet plnenia zmluvy dodržiavanie:

   a) povinnosti ochrany dôverných informácií a záväzku mlčanlivosti o údajoch, s ktorými počas plnenia predmetu zmluvy pre objednávateľa prišli do styku, a to aj po ukončení pracovného, resp. služobného pomeru,

   b) zákazu využitia dôverných informácií, s ktorými prišli do styku pre osobnú potrebu, zákazu ich zverejnenia, poskytnutia a sprístupnenia s výnimkou orgánov činných v trestnom konaní.

6. Požiadavka v bode 5 tohto článku zmluvy bude zabezpečená podpísaním vyhlásenia o mlčanlivosti zo strany príslušného zamestnanca.

7. Všetky podklady s dôvernými informáciami poskytnuté dodávateľovi a evidované údaje musia byť po ukončení obchodných vzťahov bez vyzvania odovzdané objednávateľovi alebo podľa jeho rozhodnutia vymazané alebo skartované. Táto

povinnosť sa vzťahuje aj na vyhotovené kópie. Toto ustanovenie neplatí v prípade vzájomných zmlúv a projektovej dokumentácie medzi zmluvnými stranami, ktoré ale nesmú byť bez súhlasu objednávateľa sprístupnené tretej osobe inak, ako to dovoľuje táto zmluva.

8. Dodávateľ sa zaväzuje, že sa v žiadnom prípade bez vedomia objednávateľa nepokúsi získať prístup k informáciám, ktoré:
   a) sú prenášané na poskytovanej infraštruktúre a sú súčasťou prenášaných údajov,
   b) nie sú pre neho potrebné na výkon poskytovanej služby a ani ich žiadnym spôsobom nezneužije v prípade, ak sa k nim neoprávnene dostane.
9. Dodávateľ sa zaväzuje, že pred každým plánovaným servisným zásahom zašle na adresu dispecing@socpoist.sk zoznam zamestnancov dodávateľa, vykonávajúcich servisný zásah, s termínom prístupu do informačného systému Sociálnej poisťovne v štruktúre podľa Prílohy č. 6 k tejto zmluve a pri každom neplánovanom (operatívnom) zásahu vyplní a zašle požadované údaje pokiaľ možno pred, inak ihneď po vykonaní zásahu.
10. Zmluvné strany sa zaväzujú, že budú ochraňovať dôverné informácie druhej zmluvnej strany s rovnakou starostlivosťou, ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti.
11. Ustanovenia predchádzajúcich bodov budú platiť aj po dobe platnosti a účinnosti zmluvy, a to až do doby, kedy sa informácie stanú verejne známymi.
12. Dodávateľ je povinný na požiadanie objednávateľa bezodplatne

a) akceptovať poverenia objednávateľa ako prevádzkovateľa podľa článku 29 GDPR a/alebo podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení na spracúvanie osobných údajov a/alebo

b) uzavrieť ako tretia osoba s objednávateľom ako prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Článok 11
Skončenie zmluvy

1. Táto zmluva môže skončiť:
   a) splnením,
   b) písomnou dohodou zmluvných strán,
   c) výpoveďou,
   d) odstúpením od tejto zmluvy ktoroukoľvek zmluvnou stranou pri podstatnom porušení tejto zmluvy.
2. Táto zmluva môže byť skončená písomnou dohodou zmluvných strán alebo výpoveďou ktorejkoľvek zmluvnej strany aj bez uvedenia dôvodu. Zmluvné strany sa dohodli na šesťmesačnej výpovednej lehote, ktorá začne plynúť prvým dňom kalendárneho mesiaca nasledujúceho po doručení písomnej výpovede druhej zmluvnej strane.

3. Objednávateľ môže od tejto zmluvy odstúpiť:

   a) v prípade podstatného porušenia tejto zmluvy dodávateľom; za podstatné porušenie zmluvných povinností sa považuje:

      - dodanie tovaru, ktorý nebude spĺňať požadovanú špecifikáciu, množstvo, kvalitu, rozsah, cenu alebo podmienky špecifikované v zmluve a v Prílohe č. 1 k tejto zmluve,
      - omeškanie dodávateľa s dodávkou tovaru a súvisiacich služieb (o viac ako 30 dní) oproti termínu podľa článku 4 tejto zmluvy,
      - opakované omeškanie (viac ako 2 krát) s odstránením prípadných vád predmetu tejto zmluvy spôsobom dohodnutým v článku 8 bod 3 tejto zmluvy,

   b) v prípade nepodstatného porušenia tejto zmluvy dodávateľom, len ak dodávateľ nesplní svoju povinnosť ani v dodatočne primeranej lehote, ktorá mu bola poskytnutá,

   c) v prípade opakovaného porušenia akýchkoľvek povinností dodávateľom, ktoré vyplývajú z ustanovení tejto zmluvy alebo z ustanovení všeobecne záväzných právnych predpisov, za opakované sa považuje preukázateľne porušenie dvakrát a viackrát,

   d) podľa § 19 zákona o verejnom obstarávaní.

4. Odstúpeniu od tejto zmluvy musí predchádzať upozornenie objednávateľa na neplnenie zmluvných povinností dodávateľom a na možnosť skončenia tejto zmluvy odstúpením.

5. Dodávateľ môže od tejto zmluvy odstúpiť v prípade, ak je objednávateľ v omeškaní s úhradou riadne vystavenej faktúry o viac ako tridsať (30) dní odo dňa jej doručenia do podateľne objednávateľa. Skončeniu tejto zmluvy musí predchádzať upozornenie na neplnenie platobných povinností objednávateľa a na možnosť ukončenia tejto zmluvy odstúpením.

6. Dodávateľ nepostúpi bez predchádzajúceho písomného súhlasu objednávateľa ani inak neprevedie práva a povinnosti vyplývajúce z tejto zmluvy v celku ani v jej časti inému subjektu a nepostúpi časť alebo celkovú výšku svojich pohľadávok na tretiu osobu. Objednávateľ je oprávnený túto zmluvu vypovedať v jednomesačnej výpovednej lehote, v prípade ak dodávateľ poruší toto ustanovenie.

7. Dodávateľ je povinný vopred informovať objednávateľa o každej zmene vlastníctva spoločnosti alebo jej časti. Objednávateľ si vyhradzuje právo zmluvu vypovedať v jednomesačnej výpovednej lehote, ak dôjde k prechodu vlastníctva spoločnosti alebo jej časti z dodávateľa na iný právny subjekt.

8. Odstúpenie musí byť uskutočnené písomnou formou a bude účinné dňom jeho doručenia druhej zmluvnej strane.

9. Odstúpením od tejto zmluvy nezaniká objednávateľovi povinnosť uhradiť Dodávateľovi už zrealizované čiastkové plnenia podľa tejto zmluvy.

10. Úplná alebo čiastočná zodpovednosť zmluvnej strany bude vylúčená v prípadoch zásahu vyššej moci.

11. Pod vyššou mocou sa rozumejú okolnosti, ktoré nastanú po uzavretí tejto zmluvy

ako výsledok nepredvídateľných a zmluvnými stranami neovplyvniteľných prekážok. V prípade, že takáto okolnosť bude dodávateľovi alebo objednávateľovi brániť v plnení povinností podľa tejto zmluvy, bude zmluvná strana dotknutá vyššou mocou zbavená zodpovednosti za čiastočné alebo úplné nesplnenie záväzkov vyplývajúcich z tejto zmluvy primerane počas doby, po ktorú pôsobili tieto okolnosti.

12. Skončením tejto zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy s výnimkou ustanovení, ktoré sa týkajú nároku na náhradu škody vzniknutej porušením tejto zmluvy, nároku súvisiaceho s reklamáciou tovaru, nároku na zaplatenie dohodnutej pokuty podľa ustanovení tejto zmluvy a ďalej ustanovenia tejto zmluvy, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení tejto zmluvy, napr. záruka, ochrana dôverných informácií a informačná bezpečnosť.

Článok 12
Osobitné ustanovenia

1. Na plnenie predmetu tejto zmluvy môže dodávateľ využiť subdodávateľov. Dodávateľ je povinný pri uzatvorení tejto zmluvy uviesť zoznam subdodávateľov, ktorý obsahuje údaje o všetkých známych subdodávateľoch dodávateľa v čase uzatvorenia tejto zmluvy a údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Zoznam subdodávateľov tvorí Prílohu č. 4 k tejto zmluve a obsahuje okrem uvedených údajov podiel plnenia z tejto zmluvy v % a stručný opis časti tejto zmluvy, ktorá bude predmetom subdodávky.
2. Dodávateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi, ktorý je uvedený v Prílohe č. 4 k tejto zmluve najneskôr do piatich (5) pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví tejto zmluvy.
3. V prípade zmeny subdodávateľa je dodávateľ najneskôr tri (3) pracovné dni pred zmenou subdodávateľa povinný písomne oznámiť objednávateľovi údaje o navrhovanom novom subdodávateľovi a o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Zmena nového subdodávateľa sa vykoná zápisom o zmene prílohy dňom jej podpísania zmluvnými stranami a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky (ďalej len „register“). Vzor zápisu o zmene prílohy ku zmluve tvorí Prílohu č. 5 k tejto zmluve; osobami oprávnenými konať vo veciach zmeny Prílohy č. 4 k tejto zmluve sú:

za dodávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

za objednávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

4. Navrhovaný subdodávateľ musí spĺňať podmienky účasti týkajúce sa osobného postavenia podľa § 32 zákona o verejnom obstarávaní a nesmú u neho existovať dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7 a 8 zákona o verejnom obstarávaní.
5. Využitím subdodávateľov nie je dotknutá zodpovednosť dodávateľa za plnenie predmetu tejto zmluvy.
6. Objednávateľ podpísaním tejto zmluvy akceptuje všetkých subdodávateľov dodávateľa, čo však dodávateľa nezbavuje zodpovednosti za kvalitu plnenia predmetu tejto zmluvy podľa všeobecne záväzných právnych predpisov a tejto zmluvy.
7. Pri plnení predmetu tejto zmluvy treťou osobou (subdodávateľom) má dodávateľ zodpovednosť akoby plnil predmet tejto zmluvy sám.
8. Zoznam subdodávateľov s ich identifikačnými údajmi v rozsahu: (i) meno a priezvisko alebo obchodné meno, resp. názov, (ii) adresa pobytu alebo sídlo, (iii) IČO alebo dátum narodenia, ak nebolo pridelené IČO, (iv) podiel plnenia na tejto Zmluvy v percentuálnom vyjadrení, je uvedený v Prílohe č. 4 tejto zmluvy.
9. Dodávateľ (v prípade skupiny dodávateľov každý člen skupiny dodávateľov), jeho subdodávatelia a subdodávatelia podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov (ďalej len „zákon o registri partnerov verejného sektora“), ktorí sú uvedení v Prílohe č. 4 k tejto zmluve, musia byť v súlade s § 11 ods. 1 zákona o verejnom obstarávaní zapísaní do registra partnerov verejného sektora podľa zákona o registri partnerov verejného sektora, ak im zákon o registri partnerov verejného sektora takúto povinnosť ukladá. Odberateľ neuzatvorí túto zmluvu s dodávateľom, ak v čase uzatvorenia zmluvy nebude mať on, jeho subdodávatelia alebo subdodávatelia podľa zákona o registri partnerov verejného sektora splnenú podmienku zápisu v registri partnerov verejného sektora , alebo ak on, jeho subdodávatelia alebo subdodávatelia podľa zákona o registri partnerov verejného sektora, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora, majú v registri

partnerov verejného sektora zapísaného konečného užívateľa výhod, ktorým je osoba podľa § 11 ods. 1 písmena c) zákona o verejnom obstarávaní, alebo ak dodávateľovi bude uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní.

10. Objednávateľ môže podľa § 19 ods. 3 zákona o verejnom obstarávaní odstúpiť od zmluvy, ak dodávateľ v čase uzatvorenia zmluvy nebol zapísaný v registri partnerov verejného sektora, ak mu zákon o registri partnerov verejného sektora túto povinnosť ukladá alebo ak bol vymazaný z registra partnerov verejného sektora, alebo ak mu bol právoplatne uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní. Ak sa po uzavretí zmluvy stala konečným užívateľom výhod dodávateľa, jeho subdodávateľa osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní, môže odberateľ odstúpiť od zmluvy po uplynutí 30 dní odo dňa, keď táto skutočnosť nastala, ak táto skutočnosť stále trvá.
11. Dodávateľ zodpovedá za správnosť a úplnosť údajov zapísaných o ňom v registri partnerov verejného sektora, identifikáciu konečného užívateľa výhod vo svojej spoločnosti, ako aj overovanie identifikácie konečného užívateľa výhod v zmysle § 11 Zákona o registri partnerov verejného sektora.
12. Dodávateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu svojich identifikačných a kontaktných údajov.
13. Dodávateľ vyhlasuje, že má k dispozícii kvalifikovaných expertov v súlade s požiadavkami objednávateľa na preukázanie technickej a odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Dodávateľ sa zaväzuje, že požadované služby bude poskytovať objednávateľovi prostredníctvom osôb, ktorými preukazoval splnenie podmienok účasti technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Nahradenie, alebo doplnenie týchto osôb inými osobami je možné len so súhlasom objednávateľa. V prípade nahradenia osôb musia osoby, ktoré ich nahradia, spĺňať rovnaké podmienky ako sa požadovali v rámci preukázania splnenia podmienok účasti technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní.
14. V prípade zmeny niektorého z expertov, ktorí sú uvedení v Prílohe č. 6 k tejto zmluve, je dodávateľ povinný toto písomne oznámiť objednávateľovi najneskôr do piatich (5) pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví zmluvy, údaje o navrhovanom novom expertovi. Zmena nového experta sa vykoná zápisom o zmene Prílohy č. 6 k tejto zmluve, ktorá nadobudne platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky; vzor zápisu o zmene prílohy zmluvy tvorí Prílohu č. 5 k tejto zmluve; osobami oprávnenými konať vo veciach zmeny Prílohy č. 6 k tejto zmluve sú:

za dodávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

za objednávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

15. Dodávateľ je povinný vopred informovať objednávateľa o každej zmene vlastníctva spoločnosti alebo jej časti. Objednávateľ si vyhradzuje právo zmluvu vypovedať v jednomesačnej výpovednej lehote, ak dôjde k prechodu vlastníctva spoločnosti alebo jej časti z dodávateľa na iný právny subjekt.
16. Ak sa dodávateľ v súvislosti s plnením povinností podľa tejto zmluvy dostane do súdneho konania s treťou osobou, alebo by takéto súdne konanie hrozilo, bezodkladne o tom vyrozumie objednávateľa. Objednávateľ bude povinný na požiadanie dodávateľa dať ihneď k dispozícii dodávateľovi všetky potrebné informácie a podklady. Táto povinnosť vznikne príslušným vyrozumením. Uvedená povinnosť bude platiť recipročne aj pre dodávateľa, pokiaľ by sa do takéhoto konania dostal objednávateľ. Vzájomná podpora sa poskytne iba v prípadoch, ak nedošlo k porušeniu všeobecne záväzných právnych predpisov v súvislosti s plnením tejto zmluvy.
17. Dodávateľ je povinný bezodkladne písomne oznámiť objednávateľovi začatie akéhokoľvek súdneho, rozhodcovského, exekučného, konkurzného, reštrukturalizačného alebo obdobného konania, ktoré sa začalo proti nemu alebo ktoré sám inicioval v súvislosti s predmetom tejto zmluvy. Ďalej je povinný bezodkladne oznámiť objednávateľovi, ak niektorý z veriteľov dodávateľa podal proti nemu návrh na vyhlásenie konkurzu a návrh na povolenie reštrukturalizácie alebo vstup do likvidácie a jej ukončenie.
18. Túto zmluvu je možné meniť počas jej trvania bez nového verejného obstarávania v súlade s ustanovením § 18 zákona o verejnom obstarávaní a v súlade s európskou legislatívou. Zmena tejto zmluvy musí byť písomná.
19. Dodávateľ vyhlasuje, že ku dňu uzavretia tejto zmluvy je/nie je (vyberie dodávateľ) závislou osobou voči objednávateľovi v zmysle § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v zmení neskorších predpisov. Každú zmenu súvisiacu s personálnym, ekonomickým alebo iným prepojením voči objednávateľovi v súvislosti s ustanovením § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov je dodávateľ povinný objednávateľovi písomne oznámiť a to do päť (5) dní odo dňa vzniku zmeny.

Článok 13

Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona NR SR č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona NR SR č. 546/2010 Z. z., ktorým sa dopĺňa zákon NR SR č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Dodávateľ berie na vedomie povinnosť objednávateľa zverejniť túto zmluvu v plnom rozsahu, na čo mu dáva svojím podpisom súhlas.
2. Táto zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.Zmluva sa uzatvára na dobu štyridsaťosem (48) mesiacov odo dňa nadobudnutia jej účinnosti.
3. V prípade, ak je alebo sa stane niektoré z ustanovení tejto zmluvy neplatné, neúčinné alebo nevykonateľné, nebude tým dotknutá platnosť, účinnosť a vykonateľnosť ostatných zmluvných dojednaní. Zmluvné strany sú si povinné poskytnúť vzájomnú súčinnosť pre to, aby neplatné, neúčinné alebo nevykonateľné ustanovenie bolo nahradené takým ustanovením platným, účinným a vykonateľným, ktoré v najvyššej možnej miere zachováva ekonomický účel zamýšľaný neplatným, neúčinným alebo nevykonateľným ustanovením.
4. Túto zmluvu je možné meniť alebo dopĺňať iba formou písomných dodatkov, ktoré budú jej neoddeliteľnou súčasťou s výnimkou zmeny Prílohy č. 4 a 6 k tejto zmluve, ktorá sa vykoná zápisom o zmene prílohy podľa vzoru uvedeného v Prílohe č. 5 k tejto zmluve.
5. Práva a povinnosti z tejto zmluvy prechádzajú i na prípadných právnych nástupcov zmluvných strán.
6. Zmluvné strany sa v súlade s ustanovením § 262 ods. 1 Obchodného zákonníka dohodli, že záväzkový vzťah založený touto zmluvou sa spravuje Obchodným zákonníkom. Vzťahy zmluvných strán, neupravené touto zmluvou sa budú riadiť príslušnými ustanoveniami Obchodného zákonníka, zákona o verejnom obstarávaní a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky a európskou legislatívou.
7. Zmluvné strany sa zaväzujú, že všetky spory, vyplývajúce z tejto zmluvy, budú riešiť predovšetkým formou dohody. Prípadné spory, o ktorých sa zmluvné strany nedohodnú, budú sa riadiť právnym poriadkom Slovenskej republiky a budú postúpené na rozhodnutie vecne a miestne príslušnému súdu.

8. Neoddeliteľnou súčasťou tejto zmluvy sú prílohy:

   Príloha č. 1: Cenová kalkulácia, špecifikácia, množstvo a miesto plnenia predmetu zmluvy,

   Príloha č. 2: Technická špecifikácia predmetu zmluvy,

   Príloha č. 3: Vzor preberacieho protokolu,

   Príloha č. 4: Zoznam subdodávateľov,

   Príloha č. 5: Vzor zápisu o zmene Prílohy,

   Príloha č. 6: Zoznam expertov

   Príloha č. 7: Sprostredkovateľská zmluva,

   Príloha č. 8: Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

9. Táto zmluva je vyhotovená v štyroch (4) rovnopisoch, po dva (2) rovnopisy pre každú zmluvnú stranu.

10. Zmluvné strany vyhlasujú, že obsah tejto zmluvy je prejavom ich slobodnej vôle, dohoda nebola uzavretá v tiesni a ani za zvlášť nevýhodných podmienok. Súčasne vyhlasujú, že si ju riadne a dôsledne prečítali, jej obsahu rozumeli a právnym účinkom porozumeli a na znak súhlasu ju vlastnoručne podpísali.

V Bratislave, dňa	V Bratislave, dňa
Za dodávateľa:	Za objednávateľa:
.....	.....
Ing. Ján Kostka	**Ing. Michal Ilko**
predseda predstavenstva	generálny riaditeľ Sociálnej poisťovne
ALCASYS Slovakia, a.s.	

Príloha č. 1

CENOVÁ KALKULÁCIA, ŠPECIFIKÁCIA, MNOŽSTVO A MIESTO PLNENIA PREDMETU ZMLUVY

p. č.	Názov položky	Produktové číslo	Merná jednotka	Predpokladané množstvo	Cena v EUR bez DPH za 1 mernú jednotku	Cena v EUR s DPH za 1 mernú jednotku
1.1.	**Zabezpečenie obnovy licencií**					
1.1.1.	Zabezpečenie obnovy licencii RSI Routing Services Interface Server - 5 agents for Genesys Integration software license (predĺženie licenčného supportu o 12 mesiacov)	3BA09523AA	licencia	4	2 450,00	2 940,00
1.1.2.	Zabezpečenie obnovy licencii RSI Routing Services Interface Server – additional 5 agents for Genesys (predĺženie licenčného supportu o 12 mesiacov)	3BA09524AA	licencia	124	255,00	306,00
1.1.3.	Zabezpečenie obnovy licencií OEM v8.5 - Workspace / WebGAD / Ticketing (predĺženie licenčného supportu o 12 mesiacov)	3AP20364ACAB	licencia	1 840	112,50	135,00
1.1.4.	Zabezpečenie obnovy licencií Genesys Engage On Premise Base Package NR (predĺženie licenčného supportu o 12 mesiacov)	PEP-D-BASEPACKAGE-NR	licencia	640	660,00	792,00
1.1.5.	Zabezpečenie obnovy licencií v8.1 - Genesys Outbound Voice - SUB 60 (predĺženie licenčného supportu o 12 mesiacov)	3GP08809ACAA-SUB	licencia	240	305,00	366,00
1.1.6.	Zabezpečenie obnovy licencií v8.5 - Genesys Voice Platform (incl add'l capability) – SUB (predĺženie licenčného supportu o 12 mesiacov)	3GP21277ACAA-SUB	licencia	160	350,00	420,00
1.1.7.	Zabezpečenie obnovy licencií v8.1 - Proactive Contact - E-mail/SMS – SUB (predĺženie licenčného supportu o 12 mesiacov)	3GP08822ACAA-SUB	licencia	8	750,00	900,00
1.1.8.	Zabezpečenie obnovy licencií v8.5 - Social Engagement Pkg – SUB (predĺženie licenčného supportu o 12 mesiacov)	3GP21219ACAA-SUB	licencia	20	1 450,00	1 740,00
1.1.9.	Zabezpečenie obnovy licencií v8.1 - Recording Connector (incl Active) – SUB (predĺženie licenčného supportu o 12 mesiacov)	3GP21312ACAA-SUB	licencia	640	85,00	102,00
1.1.10.	Zabezpečenie obnovy1 licencie v9.0 - Genesys Chatbot Orchestration (# 3,6 mil turns) – SUB (predĺženie licenčného supportu o 12 mesiacov)	3GP114794ACAA-SUB	balík	4	14 400,00	17 280,00
1.1.11.	Zabezpečenie obnovy licencií OEM v8,5 – NLU - Skengine (predĺženie licenčného supportu o 12 mesiacov)	3GP114794ANET-SUB	licencia	4	9 600,00	11 520,00
1.1.12.	Zabezpečenie obnovy licencií NICE Quality Management Platform - New License (predĺženie licenčného supportu o 12 mesiacov)	NICE-QM-QMP	licencia	560	110,00	132,00
1.1.13.	Zabezpečenie obnovy licencií AIR Voice Capture - New License (predĺženie licenčného supportu o 12 mesiacov)	NICE-IM-VC-AIR	licencia	560	100,00	120,00
1.1.14.	Zabezpečenie obnovy licencií AIR Screen Capture - New License	NICE-IM-SCC-AIR	licencia	560	70,00	84,00

p. č.	Názov položky	Produktové číslo	Merná jednotka	Predpokladané množstvo	Cena v EUR bez DPH za 1 mernú jednotku	Cena v EUR s DPH za 1 mernú jednotku
	(predĺženie licenčného supportu o 12 mesiacov)					
1.1.15.	Alcatel-Lucent Solution Premier Service (per license) (predĺženie licenčného supportu o 12 mesiacov)	SPS OXO_OXE_OV	licencia	28 708	11,60	13,92
1.2.	**Zabezpečenie licencií**					
1.2.1.	Licencia IPT -IP Premium license - 1 user	X	ks	3 000	135,00	162,00
1.2.2.	IP Softphone - Agent software license	X	ks	150	90,00	108,00
1.2.3.	SIP network link software license including eSBC	X	ks	240	260,00	312,00
1.2.4.	Základná pracovná pozícia agenta Nice recording licencia (CSTA IP DR-link + AIR Voice Capture + NICE Platform)	X	ks	120	1 150,00	1 380,00
1.2.5.	Rozšírenie základnej pozície agenta Genesys Multimedia Ticketing	X	ks	120	225,00	270,00
1.2.6.	Rozšírenie základnej pozície agenta Genesys Social Engagement (FB) Pkg - SUB	X	ks	10	1 450,00	1 740,00
1.2.7.	Rozšírenie základnej pozície agenta Genesys Outbound Voice - SUB	X	ks	200	305,00	366,00
1.2.8.	Rozšírenie ostatných komponentov systému Genesys Voice Platform - SUB– kanál IVR systému	X	ks	40	350,00	420,00
1.2.9.	Rozšírenie základnej pozície agenta Nice quality management (NICE Quality Management)	X	ks	120	323,00	387,60
1.2.10.	Základná pracovná pozícia agenta IPPBX endpoint (IP Premium license + RSI CC Routing SI + Headset Binaural, Noice cancelation,USB-A)	X	ks	120	475,00	570,00
1.3.	**Zabezpečenie služieb technickej podpory komunikačných systémov a servisných služieb**					
1.3.1.	TECHNICKÁ PODPORA - Základné montážne práce	X	hod	6 000	45,00	54,00
1.3.2.	TECHNICKÁ PODPORA - Základná správa systému Alcatel Lucent technológie	X	hod	800	75,00	90,00
1.3.3.	TECHNICKÁ PODPORA - Pokročilá správa systému Genesys / Nice technológie	X	hod	1 200	75,00	90,00
1.3.4.	TECHNICKÁ PODPORA - Analýza a návrh	X	hod	1 200	75,00	90,00
1.3.5.	TECHNICKÁ PODPORA - Konfigurácia systému	X	hod	12 000	75,00	90,00
1.3.6.	TECHNICKÁ PODPORA - Softwarový vývoj	X	hod	3 200	75,00	90,00
1.3.7.	TECHNICKÁ PODPORA - Testovanie	X	hod	800	75,00	90,00
1.3.8.	TECHNICKÁ PODPORA pre KAMPAŇ TYPU A (SZČO, mesačný výkaz poistného) v rozsahu: Príprava 1 dávky dát, Spustenie 1 dávky dát, Výstupný report z 1 dávky dát (do 2-och týždňov od vyhodnotenia kampane), Počet (e-mail a- alebo SMS) správ v množstve od 0 do 100 000 kontaktov	X	Ks	2 000	95,00	114,00
1.3.9.	TECHNICKÁ PODPORA pre KAMPAŇ TYPU A (SZČO, mesačný výkaz poistného) v rozsahu: Príprava 1 dávky dát, Spustenie 1 dávky dát, Výstupný report z 1 dávky dát (do 2-och týždňov od vyhodnotenia kampane), Počet (e-mail a- alebo SMS) správ v	X	Ks	2 000	95,00	114,00

p. č.	Názov položky	Produktové číslo	Merná jednotka	Predpokladané množstvo	Cena v EUR bez DPH za 1 mernú jednotku	Cena v EUR s DPH za 1 mernú jednotku
	množstve od 100 001 do 200 000 kontaktov					
1.3.10.	TECHNICKÁ PODPORA pre KAMPAŇ TYPU B (zamestnávatelia) v rozsahu: Príprava 3 dávok dát, Spustenie 3 dávok dát, Výstupný report z 3 dávok dát (do 2-och týždňov od spustenia kampane), Počet (e-mail a- alebo SMS) správ od 0 do 100 000 kontaktov	X	ks	2 000	95,00	114,00
1.3.11.	TECHNICKÁ PODPORA pre KAMPAŇ TYPU B (zamestnávatelia) v rozsahu: Príprava 3 dávok dát, Spustenie 3 dávok dát, Výstupný report z 3 dávok dát (do 2-och týždňov od spustenia kampane), Počet (e-mail a- alebo SMS) správ od 100 001 do 200 000 kontaktov	X	ks	2 000	95,00	114,00
1.4.	**Dodanie hardvérových komponentov k poskytovaným službám**					
1.4.1.	Základná pracovná pozícia agenta Genesys Engage On Premise Base Package NR : SIP Interaction, Qualification&Parking, CIM, CHAT, E-mail, SMS, Workspace/AIC, Infomart, CX Insights + HA	X	Ks	200	660,00	792,00
1.4.2.	IP Tel manager - Dual Gigabit Ethernet Enterprise DeskPhone with Corded Handset, Dual Stack NOE-SIP, 3.5 inch 320x240 color display, HD Audio, 2 USB-C (ALE-300)	X	Ks	300	350,00	420,00
1.4.3.	IP Tel referent - Entry-level DeskPhone, NOE-SIP, 128x64 pixels, black and white LCD with backlit, 6 soft keys, 2 Gigabit Ethernet ports, HD Audio (A8008G)	X	Ks	600	180,00	216,00
1.4.4.	IP Tel Basic - Dual Port Gigabit Ethernet Basic SIP DeskPhone 2.8 inch 132x64 Black and White display with backlight, 2 SIP accounts, 3 Line Keys, 4 soft Keys, HD Audio (ALE-2)	X	Ks	2 100	105,00	126,00
1.4.5.	Mediagateway / virtualizačný box S (min požiadavky) - 1 x Intel CPU 16 Core alebo AMD CPU 20 core, Speed 2.4 GHz, možnosť rozšírenia na 2 x CPU - RAM min 192 GB, možnosť rozšírenia na min. 256 (24 RAM Slots) - 1 x Zdroj s možnosťou rozšírenia na 2 x zdroj, min. 500W - HDD slot min. 8 SFF/LFF (SSD Mixed Use/HDD min. 10 k podľa potreby) 4TB - LAN 1x 4 port 1 GB - Remote manažment - Smart Array with battery backup - OS Windows STD/Datacenter - VMware vSphere Standard	X	Ks	16	12 700,00	15 240,00
1.4.6.	Mediagateway / virtualizačný box XL(minimálne požiadavky) - 2 x Intel CPU 16 Core alebo AMD CPU 20 core, Speed 2.4 GHz - RAM min 256 GB, moznost rozsirenia na min. 512 (24 RAM Slots) - 2 x Zdroj , min. 800W - HDD slot min. 8 SFF/LFF (SSD Mixed Use/HDD min. 10 k podľa	X	Ks	8	34 600,00	41 520,00

p. č.	Názov položky	Produktové číslo	Merná jednotka	Predpokladané množstvo	Cena v EUR bez DPH za 1 mernú jednotku	Cena v EUR s DPH za 1 mernú jednotku
	potreby) 10 TB, možnosť rozšírenia na 24 SFF - Možnosť voľby doplniť dva NVMe HDD pre OS - LAN 1x 4 port 1 GB - Remote manazment - Smart Array with battery backup - OS Windows STD/Datacenter - VMware vSphere Standard					
1.4.7.	Power back-up 185W/1H	X	Ks	8	499,80	599,76
1.4.8.	7AH/12V battery	X	Ks	80	25,00	30,00
1.4.9.	Cooling kit Rack 3	X	Ks	80	110,00	132,00
1.4.10.	Headset Binaural, Noice cancelation,USB-A	X	Ks	120	78,00	93,60
1.4.11.	Headset Binaural, Noice cancelation, wireless	X	Ks	80	215,00	258,00
1.4.12.	Switch 10 PoE, 1G BaseT, fanless	X	Ks	120	750,00	900,00
1.4.13.	Switch 24 PoE, 1G BaseT, fanless	X	Ks	80	1 250,00	1 500,00
1.4.14.	Switch 48 PoE, 1G BaseT	X	Ks	40	2 150,00	2 580,00
1.4.15.	Stacking cable 1m	X	Ks	120	100,00	120,00
1.4.16.	Rack RMA-27-A86-CAY-A1	X	Ks	56	450,00	540,00
1.4.17.	Rack RMA-42-A86-CAY-A1	X	Ks	8	520,00	624,00
1.4.18.	P-panel KEL 24xRJ45, prázdny	X	Ks	160	16,00	19,20
1.4.19.	Držiak patchkáblov 1U kovový	X	Ks	160	6,00	7,20
1.4.20.	Panel 8x230V,prepäťová ochrana s filtrom, automatická poistka 10 A/250 V	X	Ks	64	27,00	32,40
1.4.21.	Ventil. Jed.strešná 2x vent.	X	Ks	64	115,00	138,00
1.4.22.	Polica 19" 450mm so zadnými podperami	X	Ks	64	21,00	25,20
1.4.23.	Kábel KEL F/UTP Cat.5E	X	meter	134 400	0,50	0,60
1.4.24.	Modul Keystone KEL cat.5E/s	X	Ks	7 680	2,10	2,52
1.4.25.	Zás KEL 2xRJ45 modul na omietku	X	Ks	3 840	4,65	5,58
1.4.26.	Patchkábel/s KEL CAT5E LSOH 0,5m	X	Ks	2 400	2,20	2,64
1.4.27.	Patchkábel/s KEL CAT5E 2m PVC	X	Ks	2 400	1,10	1,32
1.4.28.	Elektrotechnický materiál (prívod 230V+Uzemnenie rackov)	X	Ks	64	360,00	432,00
1.4.29.	P-panel FO výsuvný 24xSC, LC-LC Duplex	X	Ks	24	34,00	40,80
1.4.30.	Držiak patchkáblov 1U kovový	X	Ks	24	6,00	7,20
1.4.31.	Kazeta FO pre 2x12 zvarov, komplet	X	Ks	24	5,00	6,00
1.4.32.	Pigtail LC singlemode OS2 9/125, 2m	X	Ks	96	1,60	1,92
1.4.33.	Ochrana FO zvaru 40 mm	X	Ks	96	0,20	0,24
1.4.34.	Adapter FO OS2 LC-LC Duplex	X	Ks	96	2,00	2,40
1.4.35.	Patchkábel FO E9/125 SM LC-LC-Duplex 1m	X	Ks	96	10,50	12,60
1.4.36.	Kábel FO 4-vl 9/125 SM OS2, central loose tube	X	meter	2 400	0,60	0,72
1.4.37.	Žľab 100/40, 2m	X	meter	6 000	10,50	12,60
1.4.38.	Žľab 24/22, 2m	X	meter	6 000	2,50	3,00
1.5.	**Poskytovanie servisnej starostlivosti**					
1.5.1.	Garantované SLA : Po-Pia 7:00 - 19:00, dostupnosť centrálny telco systém 99,8%, telco systémy pobočky 99%, IPC 99,8%	x	mesiac	48	1 800,00	2 160,00
1.5.2.	HelpDesk pre všetky systémy dostupný 24 x 7 cez médiá : - telefón, - e-mail, - servicedesk,	x	mesiac	48	1 200,00	1 440,00

p. č.	Názov položky	Produktové číslo	Merná jednotka	Predpokladané množstvo	Cena v EUR bez DPH za 1 mernú jednotku	Cena v EUR s DPH za 1 mernú jednotku
	Response time 1 hodina					
1.5.3.	Incident management - riešenie incidentov & spare parts on stock (predpoklad 80 výjazdov on-site + 400 hodín)	x	mesiac	48	2 380,00	2 856,00
1.5.4.	profylaktika remote (4 x ročne Alcatel-Lucent ústredie, 1 x ročne Alcatel-Lucent pobočky; 4 x ročne & Genesys & Nice)	x	mesiac	48	1 100,00	1 320,00
1.5.5.	business continuity testy (overenie funkčnosti HA) (Alcatel-Lucent centrálny uzol & Genesys & Nice - 1 x ročne)	x	mesiac	48	320,00	384,00
1.5.6.	Maintenance realizačné práce = starostlivosť o software - patchovanie a update (podľa potreby), upgrade Alcatel-Lucent (1 x ročne), update Genesys a NICE (240 hodín prác mimo prevádzkovú dobu SP)	x	mesiac	48	1 500,00	1 800,00

ZOZNAM PRACOVÍSK/LOKALÍT S TELEKOMUNIKAČNÝMI SYSTÉMAMI A ZOZNAM PRACOVÍSK BEZ TELEKOMUNIKAČNÝCH SYSTÉMOV

Tabuľka č. 1 Zoznam pracovísk/lokalít s telekomunikačnými systémami a počtami užívateľov telefónie

č.	Lokalita	Systém	# Users
1	**Banská Bystrica**, Kapitulská č.27	OXO Connect	160
2	**Bardejov**, Hurbanova 6	OXO Connect	80
3	**Bratislava** - 29. augusta + vysunuté pracoviská	OXE R12.4	2 418
4	**Bratislava** - Záhradnícka 31	OXE R12.4	349
5	**Bratislava** - Nevädzova	GW-29	počet zahrnutý v rámci lokality č.3
6	**Brezno**, B.Němcovej 4	OXO Connect	28
7	**Čadca** - vysunuté prac., Fraňa Kráľa 1054	OXO Connect	42
8	**Čadca**, Štúrova 2078	OXO Connect	56
9	**Dolný Kubín**, Aleja slobody 1878	OXO Connect	58
10	**Dubnica n. Váhom**, Partizánska 149/1	OXO Connect	24
11	**Dunajská Streda**, Galantská cesta 693/5	OXO Connect	80
12	**Humenné**, Námestie slobody 58	OXO Connect	144
13	**Komárno**, Petőfiho 7	OXO Connect	120
14	**Košice**, Festivalové námestie 1398	OXE R12.4	220
15	**Levice**, Sv.Michala č. 4	OXO Connect	112
16	**Liptovský Mikuláš**, Štúrova 34	OXO Connect	80
17	**Lučenec**, Dr. Vodu 6	OXO Connect	112
18	**Martin**, Námestie SNP 4	OXO Connect	112
19	**Michalovce**, Nám.osloboditeľov 81	OXO Connect	96
20	**Nitra**, Slančíkovej 3	OXO Connect	112
21	**Nové Zámky,** Námestie Györgya Széchényiho 10	OXE R12.4	350
22	**Považská Bystrica**, Kukučínova 208/23	OXO Connect	160
23	**Poprad,** 1. mája 24	OXE R12.4	170
24	**Prešov**, Masarykova 1	OXO Connect	191
25	**Rimavská Sobota**, K. Mikszátha 6/311	OXO Connect	88

26	**Rožňava**, Štítnická 12	OXO Connect	160
27	**Senica**, ul. Hollého 1219	OXO Connect	80
28	**Snina**, Partizánska 1057	OXO Connect	80
29	**Spišská Nová Ves**, Elektrárenská 10	OXO Connect	112
30	**Stará Ľubovňa**, Budovateľská 42	OXO Connect	112
31	**Svidník**, Sov. hrdinov 121	OXO Connect	56
32	**Topoľčany**, M.R.Štefánika 2269/18	OXO Connect	112
33	**Trebišov,** M.R.Štefánika 178	OXO Connect	96
34	**Trenčín,** Jilemnického 3760	OXE R12.4	151
35	**Trnava,** Vladimíra Clementisa 24/A	OXE R12.4	200
36	**Veľký Krtíš**, SNP 28	OXO Connect	112
37	**Vranov nad Topľou**, Rázusová 128	OXO Connect	112
38	**Zvolen**, Š.Moyzesa 1369/52	OXO Connect	88
39	**Zvolen**, Námestie SNP č. 35/48	OXO Connect	48
40	**Žiar nad Hronom**, Sládkovičova 17	OXO Connect	112
41	**Žilina**, Nám. L. Štúra	OXO Connect	184

Tabuľka č.2 - Zoznam vysunutých pracovísk bez telekomunikačných systémov, využívajúcich IP telefóny z centrálneho uzla (ul.29.augusta č.10, Bratislava)

č.	Lokalita	Typ lokality	# users
42	Čadca - vysunuté prac., Fraňa Kráľa 1054	Vysunuté pracovisko	12
43	Galanta, Z. Kodálya 1629/48	Vysunuté pracovisko	55
44	Kysucké Nové Mesto, Belanského 1345	Vysunuté pracovisko	7
45	Malacky, Bernolákova 1/A	Vysunuté pracovisko	44
46	Myjava, nám. M. R. Štefánika 561	Vysunuté pracovisko	9
47	Pezinok, Radničné námestie 9	Vysunuté pracovisko	37
48	Prievidza, Matice slovenskej 10	Vysunuté pracovisko	122
49	Revúca, Komenského 40	Vysunuté pracovisko	4
50	Ružomberok, Podhora 9	Vysunuté pracovisko	31
51	Senec Brezova	Vysunuté pracovisko	37

Príloha č. 2 TECHNICKÁ ŠPECIFIKÁCIA PREDMETU ZMLUVY

Predmetom zmluvy je poskytovanie služieb pre call centra, komunikačné systémy a servisné služby Sociálnej poisťovne (ďalej len "SP") spojené telekomunikačnou technikou a sieťami. Komunikačnými systémami sa rozumejú hlasové komunikačné systémy (IPPBX a prislúchajúce koncové zariadenia), informačno-poradenské centrum (IPC) a s ním spojené služby, telekomunikačné siete (fyzické siete na pracoviskách a súvisiace LAN komponenty), opravy a výmeny vadných komponentov a zmenové požiadavky podľa požiadaviek SP.

Predmetom zmluvy je kombinácia paušálnych služieb a prevádzkových potrieb udržania chodu a rozvoja telekomunikačného prostredia SP.

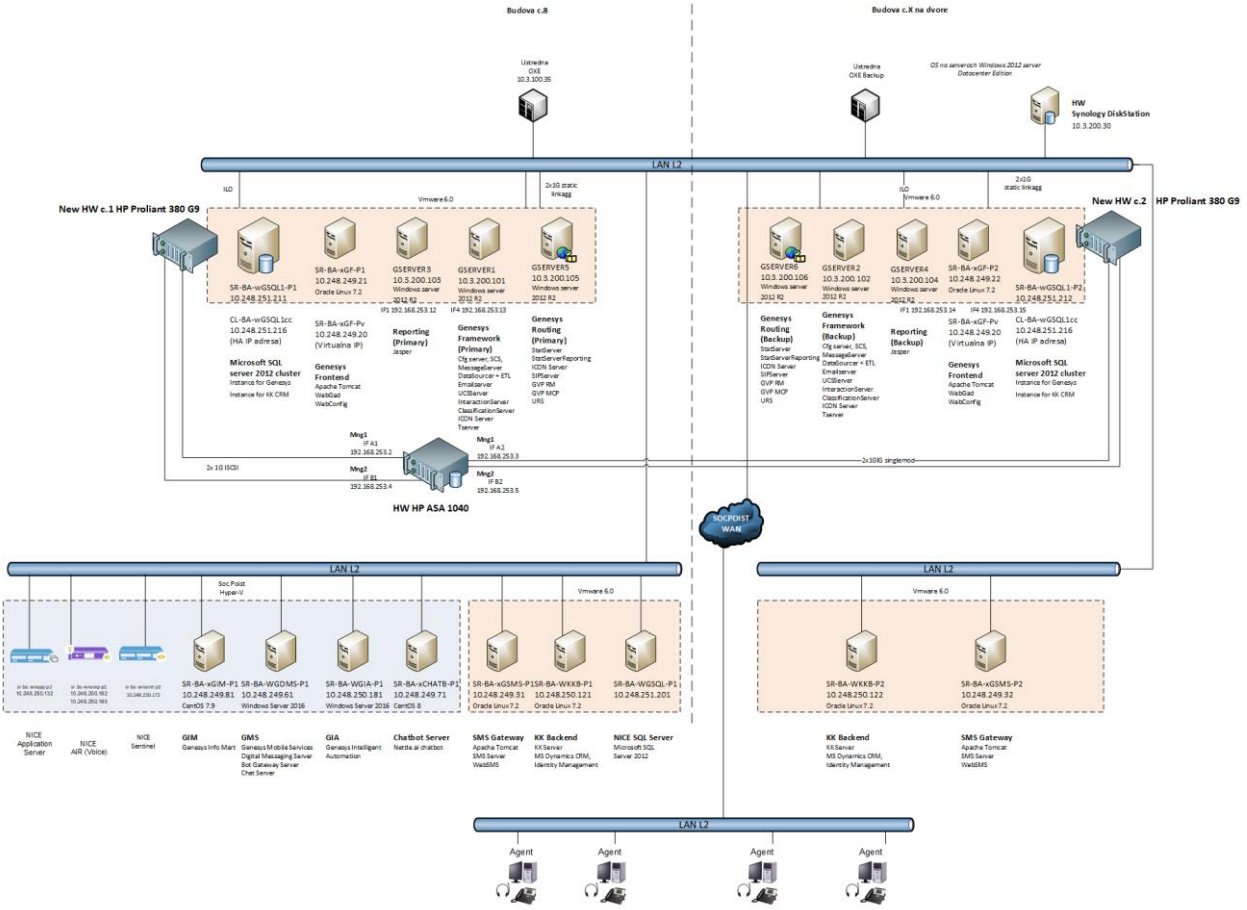
Popis aktuálneho stavu

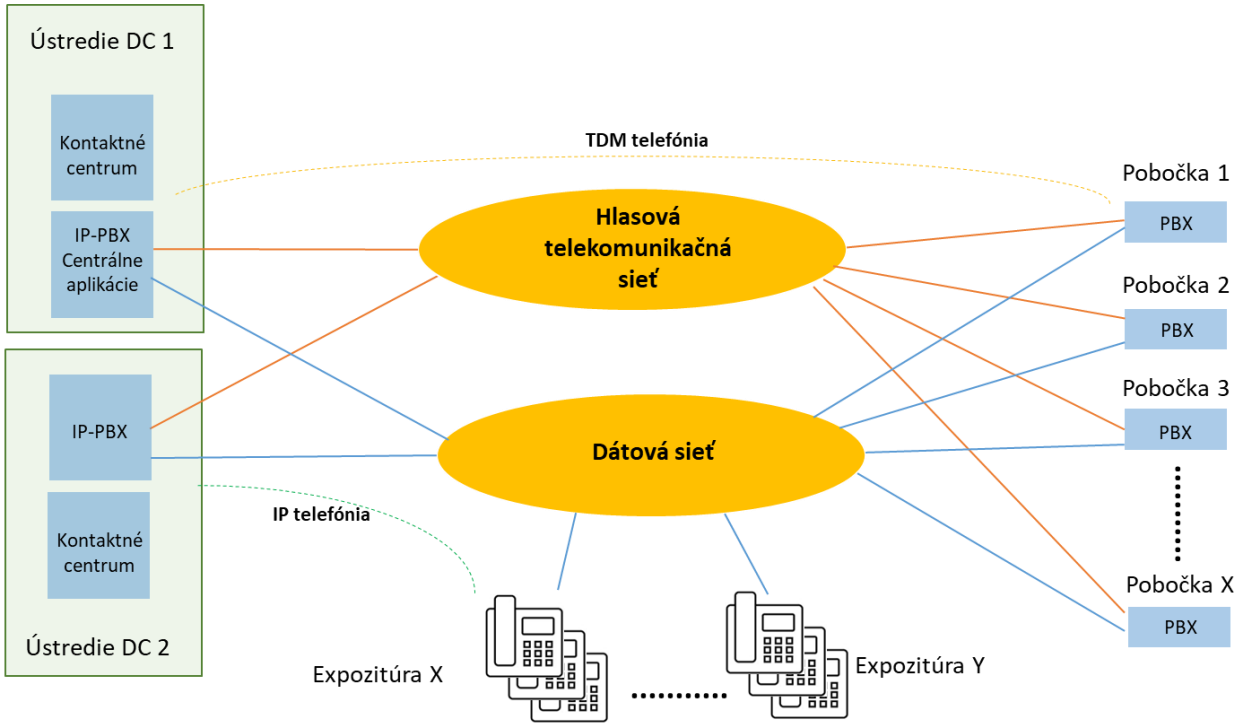
Priama denná komunikácia s klientom (mimo osobnej návštevy) prebieha:

- telefonicky volaním na pobočku (volania klient – pracovník vybraného pracoviska)
- e-mailom na pracovníka pobočky
- volaním na informačno-poradenské (IPC)
- elektronicky vyplnením web formulára na webe SP a následná komunikácia s IPC (komunikáciu prichádzajúcu z web stánky zabezpečuje primárne IPC)
- súčasťou komunikácie je aj komunikácia cez SMS kanál

Na komunikáciu pobočiek s klientom SP má v prevádzke 41 telekomunikačných systémov Alcatel-Lucent pokrývajúcich ústredie, pobočky, vysunuté pracoviská. Malé pobočky a vysunuté pracoviská sú pokryté IP telefónmi registrovanými na systém ústredia. Aktuálne je centralizovaných (obsluhovaných centrálnou IPPBX) približne 40% užívateľov siete SP. Zatiaľ nie je splnený predpoklad na úplnú centralizáciu telefónie – dostatočne prestupná WAN s QoS pre telefóniu.

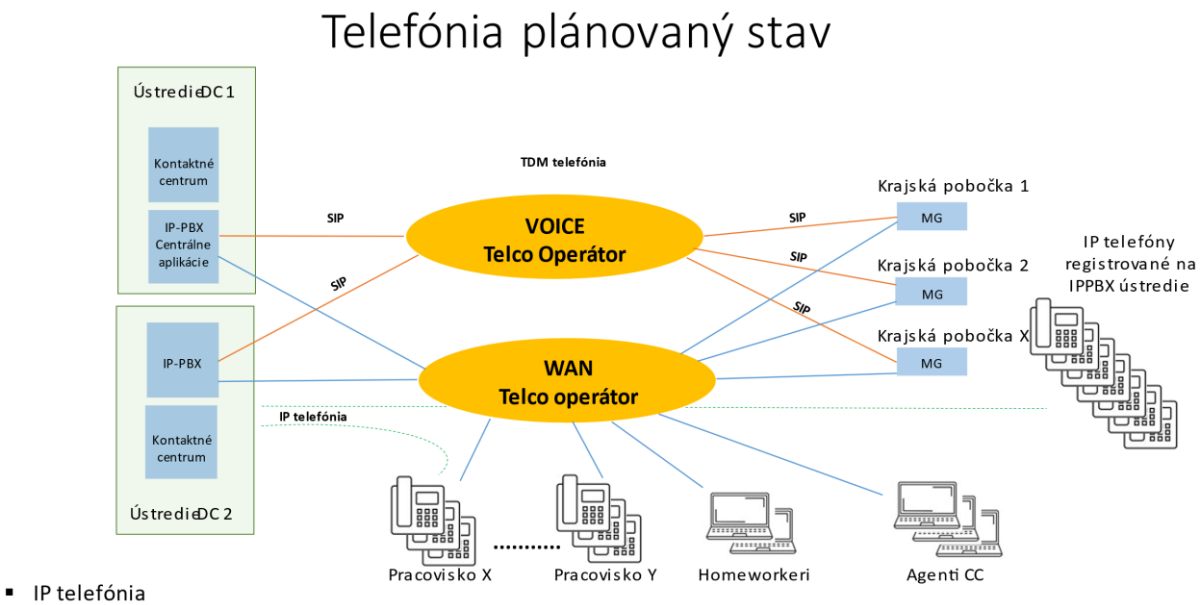
Základná topológia informačno-poradenského centra (IPC)





- Duálna telefónia – TDM a IP
  - Centralizované ISDN pripojenie do siete telekomunikačného operátora
  - Prepojenie pobočiek na ústredie cez TDM Q-Sig Hlas
  - Vysunuté pracoviská a menšie pobočky IP telefónia cez sieť WAN

Cieľový stav, ktorý zjednoduší servisnú náročnosť bude plne centralizované riešenie postavené na systéme ústredia – centralizované prístupy k telekomunikačným operátorom, centrálne riadenie, manažment, monitoring, centrálne služby, centrálne integračné rozhrania na API pre integráciu s ostatnými systémami SP so zdvojeným riadením (dnes už v prevádzke) dislokovaným v dvoch dátových centrách. Vybrané pracoviská (krajské mestá, prípadne veľké okresné pobočky) budú mať lokálny prestup na telekomunikačného operátora a záložné riadenie pre prípad výpadku WAN siete.



- IP telefónia
  - CentralizovanéSIP pripojenie do siete Voice Telco operátora
  - Všetci klienti v sieti sú IP/SIP
  - Lokálne SIP prestupy do siete Voice operátora / MG umožní standalone prevádzku vybranej lokality v prípade výpadku WAN

Centrálny systém dnes pokrýva ústredie na ul. 29.Augusta vzdialené IP telefóny a jednotlivé pracoviská SP v Bratislave a pobočky/ vysunuté pracoviská v rámci SR a je hlavným prestupným bodom k operátorom. Bežná prevádzková doba na ústredí, pobočkách a vysunutých pracoviskách objednávateľa v pracovných dňoch v čase od 06.00 -18.00 hod.

Nadstavbou nad týmto systémom je technológia pre IPC – informačno-poradenské centrum, Genesys a recording NICE. Tieto technológie pre IPC sú schopné pokryť požiadavky na kontaktné centrum pre všetky lokality v SR, call centrum pre komunikáciu s klientami/Ticketing, IVR/hlasová samoobslužná zóna, kampaňový manažment pre emailovú komunikáciu a súčasť riešenia IPC je aj SMS gateway slúžiaca primárne na SMS kampane na klientov SP. Ďalším komponentom IPC je aj CHATBOT platforma a BOT orchestration server (očakáva sa zapojenie ďalších kanálov – VoiceBot, MailBot).

Súčasťou telekomunikačného prostredia sú aj lokálne siete pracovísk – kabeláže systémy, racky, telekomunikačné UPS a batérie, koncové LAN switche s PoE pre napájanie IP telefónov.

Popis žiadaného stavu

Všetky vyššie spomínané telekomunikačné technológie (telefónia, siete / kontaktné centrum / nice recording – ostatné komunikačné kanály) vyžadujú z pohľadu servisu potrebu:

- **paušálneho servisu**
  - L3 servis/support – vendor maintenance/subscription na špecializovaný software tretích strán – možnosť otvárať servisné požiadavky na vendora, bug a security patche, updates a dostupné upgrade verzie – potrebné pre kompatibilitu s operačnými systémami a databázami podporovanými SP.
  - Servisná starostlivosť - riešenie incidentov, dodržiavanie SLA a s tým súvisiaca dostupnosť náhradných komponentov, pravidelná profylaxia a pravidelné nasadzovanie opravných patchov, updatov a upgradov
- **servisu na vyžiadanie**
  - riešenie požiadaviek na úrovni konfigurácií systémov a užívateľských nastavení, prípadne mimoriadnych požiadaviek na update/upgrade systémov vyvolaných treťou stranou (inými dotknutými systémami, mimoriadnymi security opatreniami ap.)
  - fyzické zásahy na mieste, výmeny hardware v prípade potreby, presuny a zmeny na mieste v lokalitách SP.

Základné požiadavky na poskytovanie servisu

1. Paušálny servis

   a. L3 servis/support – vendor maintenance/subscription na software tretích strán

   - Maintenance a Subscription pre SW tretích strán (uvedený v tabuľke č. 1)
     - Dostupnosť helpdesku a možnosť otvárať servisné požiadavky u dodávateľa/vendora a podpora supportného teamu vendora (riešiť servisné požiadavky u vendora bude dodávateľ servisných služieb v mene SP)
     - Dostupnosť opravných verzií/patch/service packs
     - Dostupnosť upgrade verzií
     - Informovanie a dostupnosti up-date verzií SW
     - Informovanie a dostupnosť upgrade verzií SW

   b. Servisná starostlivosť

   Servisná starostlivosť v rozsahu :

   - integrácia so servisdeskom IBM Control Desk 7.6, nahlasovanie požiadaviek v režime 24 x 7, riešenie požiadaviek v súlade s definovanými SLA
   - Tel. hotline dodávateľa pre nahlasovanie požiadaviek v režime 24 x 7, riešenie požiadaviek v súlade s definovanými SLA
   - Starostlivosť o softvér tretích strán (Genesys, Nice, ALE)

- Poskytovanie a nasadzovanie opravných verzií/patch/service packs podľa doporučení výrobcu
- Informovanie o up-date verziách (nových patchoch) a ich poskytovania a nasadzovanie
- Informovanie o upgrade verzií (nových verzií) a ich poskytovanie (nasadzovanie upgrade verzií je predmetom plateného zmenového konania CR)
- Minimálne 1 x ročne nasadzovanie upgrade software verzií pre telekomunikačné systémy (IP telefónia)
- Minimálne 1 x ročne update software verzií pre kontaktné centrum, Genesys, Nice, a dodané / spravované systémy nutné na ich bezproblémovú prevádzku.

- Incident management – Remote
  - Diaľková analýza a diagnostika incidentov
  - Diaľkové obnovenie prevádzky a vyriešenie komunikačných problémov
  - Spustenie on-site diagnostiky, ak je potrebné
- Incident management - On-site
  - Hardwarové problémy riešené výmenou chybného komponentu (náhradné diely s výnimkou batérií a zdrojov napájania sú zakalkulované v cene servisu)
  - On-site diagnostika na základe požiadavky prevádzkového centra
- profylaxia pre jednotlivé systémy v definovanom rozsahu
  - telekomunikačné systémy (IP telefónia)
    - 4 x ročne (3 x remote a 1 x on-site) centrálny systém (tel. ústredňa a servery vrátane HA)
    - 1 x ročne vzdialené lokality on-site návšteva (samostatné systémy, mediagatewaye mimo ústredia SP)
      - Minimálny rozsah
        - kontrola logov SW a HW anomálií
        - kontrola užívateľskej databázy
        - kontrola zálohovania konfiguračných databáz všetkých systémov
        - kontrola verzií software a opatchovanie verzie podľa doporučení výrobcu
        - kontrola stavu HW, napájačov, batérií, ventilátorov
        - výstupná sumárna správa z profylaxie s doporučeniami na potrebné úpravy, upgrady, výmeny opotrebovaného HW
  - systémy IPC (informačno-poradenské centrum)
    - 4 x ročne (3 x remote a 1 x on-site)
      - Minimálny rozsah
        - kontrola logov SW
        - kontrola databáz
        - kontrola zálohovania databáz

- kontrola verzií software a opatchovanie podľa doporučení výrobcu
- kontrola stavu HW, napájačov, batérií, ventilátorov
- výstupná sumárna správa z profylaxie s odporučeniami na potrebné úpravy, upgrady, výmeny opotrebovaného HW

- business continuity testy centrálneho uzla telefónie a IPC – 1 x ročne (plánované výpadky lokalít v mimopracovnej dobe/víkend)
- Dostupnosť služieb (požiadavka na SLA)
  - dostupnosť systému na ústredí 99,8% (IP telefónia a kontaktné centrum)
  - dostupnosť systémov na pobočkách a vysunutých pracoviskách 98%
  - Service Level management - detailné evidovanie úloh (prijatie, pridelenie, stav, riešenie, uzatvorenie) a vyhodnocovanie dodržiavania požiadaviek SLA

Pravidelné reportovanie stavu úloh za definované obdobie (raz za ¼ rok ku 10. dňu po ukončení predchádzajúceho kalendárneho štvrťroka vyhodnocovací meeting s objednávateľom). Reportovanie vykoná poverený pracovník dodávateľa vedúcemu oddelenia správy technickej a komunikačnej infraštruktúry objednávateľa.

za dodávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

za objednávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Definícia dostupnosti systémov

Tabuľka č.3 - Požadovanú dostupnosť systémov musí dodávateľ služby garantovať nasledovne:

Systém	Dostupnosť (%)	Prevádzková doba	Maximálny jednorázový výpadok (H)
Centrálny telefónny systém	99,8	7 x 24	2
Informačno-poradenské centrum (IPC)	99,8	7 x 24	2 (voice) 8 (ostatné media)
Telefónne systémy pobočiek	98,0	5 x 24	6

Dostupnosť systému bude počítaná podľa nasledovného vzorca:

$$\left(1 - \frac{\sum_{i=1}^{k} n_i t_i}{N_d T_d}\right) \bullet 100[\%]$$

n_i = počet jednotiek: užívateľov / zariadení / pracovných staníc, týkajúcich sa i-tého incidentu

t_i = doba trvania i-tého incidentu

k = počet incidentov za sledované obdobie (mesiac)

N_d = celkový počet jednotiek: užívateľov / zariadení / pracovných staníc, kde je poskytovaná služba

T_d = dohodnutá doba, počas ktorej je dostupnosť služby meraná

Tabuľka č.4 - Definícia kategórií technických porúch/ incidentov

Definícia technickej poruchy / incidentu	**Definície kategórií závažnosti poruchy**
Kategória A / Kritická	Dodané IS/ICT riešenie nie je funkčné vo svojich základných funkciách, alebo sa vyskytuje kritická funkčná vada znemožňujúca jeho činnosť a zakladajúca možnosť vzniku škody Systém je pre zabezpečenie činnosti objednávateľov nepoužiteľný. Funkčnosť systému je degradovaná s dopadom na kvalitu poskytovanej služby s majoritným dopadom na zákazníkov. Vada sa vždy považuje za kritickú, ak viac ako 29% trunkov alebo užívateľov je mimo prevádzky alebo ak dáta spracúvané objednávateľom sú nedostupné.
Kategória B / Závažná	Funkčnosť dodaného IS/ICT riešenia je vo svojich funkciách znížená tak, že tento stav obmedzuje alebo ohrozuje bežnú prevádzku Funkčnosť systému je degradovaná s dopadom na kvalitu poskytovanej služby s minoritným dopadom na zákazníkov. Vada sa vždy považuje za závažnú, ak 10% až 29 % trunkov alebo užívateľov je mimo prevádzky)
Kategória C / Bežná	Ostatné drobné vady dodaného IS/ICT riešenia, ktoré nespadajú do kategórie vád A a B

	Funkčnosť systému je degradovaná bez dopadu na kvalitu poskytovanej služby

Po nahlásení požiadavky/ technickej poruchy/incidentu sú dodávateľom vykonávané požiadavky/opravy nasledovne:

Tabuľka č.5 - Systémy s prevádzkovou dobou 7 x 24 Pondelok-Nedeľa

Kategória technickej poruchy/incidentu	RT	FT voice	FT total
A	1 hod	2 hod	8 hod
B	1 hod	4 hod	24 hod
C	1 hod		48 hod

Tabuľka č.6 - Systémy s prevádzkovou dobou 5 x 24 Pondelok-Piatok

Kategória technickej poruchy/incidentu	RT (7:00-21:00)	FT voice (7:00-21:00)	FT total
A	1 hod	2 hod	8 hod
B	1 hod	4 hod	24 hod
C	1 hod		48 hod

Vysvetlenie:

RT – response time – čas reakcie dodávateľa od nahlásenia technickej poruchy /požiadavky zo strany SP
FT voice - fix time voice - čas na obnovu minimálne hlasovej prevádzky od nahlásenia technickej poruchy zo strany SP
FT total – fix time total – čas na úplné odstránenie technickej poruchy od nahlásenia technickej poruchy/požiadavky zo strany SP

Servis na vyžiadanie

Prevádzka telekomunikačných systémov (základná fyzická telekomunikačná infraštruktúra, fixná telefónia / IP telefónia, kontaktné call centrum) prináša systémové a funkčné požiadavky spojené so zavádzaním nových služieb pre klientov, organizačnými zmenami a podobne. Za systémové zmeny/požiadavky menšieho rozsahu objednávateľ považuje zmeny, ktorých prácnosť pre dodanie nepresiahne 30 človekodní. Systémové zmeny väšieho rozsahu objednávateľ považuje také zmeny, pri ktorých lehota na dodanie presiahne 30 človekodní. Pre ich realizáciu verejný obstarávateľ požaduje:

- riešenie požiadaviek na úrovni konfigurácií systémov a užívateľských nastavení, prípadne mimoriadnych požiadaviek na update/upgrade systémov vyvolaných treťou stranou (inými dotknutými systémami, mimoriadnymi security opatreniami ap.)

- Poziadavky na úpravy systému budú zadávať poverení pracovníci oddelenia správy technickej a komunikačnej infraštruktúry Sociálnej poisťovne prostredníctvom Service Desku. Dodávateľ sa zaväzuje vyriešiť požiadavky na úpravu systému menšieho rozsahu v lehote do 10 pracovných dní odo dňa ich objednania.
- Pri systémových zmenách väčšieho rozsahu, sa dodávateľ zaväzuje dodať riešenie do 30 pracovných dní odo dňa ich objednania.
- podpora business užívateľov – podpora kampaní
- fyzické zásahy na mieste, výmeny hardware v prípade potreby, presuny a zmeny na mieste v lokalite

Vyššie spomenuté služby možno kvantifikovať nasledujúcimi aktivitami:

- Základné montážne práce – fyzická inštalácia na pracovisku SP – koncové zariadenia, telefóne-komunikačné zariadenia, patch panely a zásuvky, POE sieťové komponenty napr. typu LAN switch, zdroje, úpravy RACKov, úpravy štruktúrovanej kabeláže
- Základná správa systému - Inštalácia updatov, bugfixov, security updatov s minoritným dopadom na produkčnú prevádzku
- Pokročilá správa systému - Inštalácie upgradov a migrácií spojených s prechodom na nový hardware, operačné systémy, databázy, ktoré majú zásadný vplyv na produkčné prostredie
- Analýza a návrh - špecifikácia nových prevádzkových požiadaviek užívateľa a technicko-funkčný návrh riešenia pre potreby schválenia zadávateľom)
- Konfigurácia systému - Konfigurovanie nových služieb/agentských skupín/reportov, úpravy aktuálnej konfigurácie
- Softwarový vývoj - vývoj špeciálneho software pre integráciu Genesys/NICE/Alcatel na iné systémy, vývoj plug-inov do jestvujúcich aplikácií, vývoj nových aplikácií
- Testovanie - testovanie nových funkčností, ktoré nevie obstarávateľ testovať samostatne, záťažové testy.

Výstupné správy z Profylaxie budú so zodpovednými pracovníkmi SP rozpracované podľa dôležitosti/kritickosti a v prípade, že SP pristúpi na návrhy, budú tieto realizované ako servis na vyžiadanie z položiek cenníka.

Príloha č. 3 k zmluve č. 37640-8/2023-BA

PREBERACÍ PROTOKOL (VZOR)

Objednávateľ (preberajúci):	
Dodávateľ (odovzdávajúci):	
Objednávka č.:	**Protokol vypracoval:**
Strana: 1/1	**Dátum:**

Preberajúci týmto potvrdzuje prevzatie nasledovného predmetu dodania od odovzdávajúceho:

Termín*	Názov prdmetu dodania*	Položka z cenníka (Príloha č.1)*	Riešiteľ*	Merná Jednotka	Počet MJ*/Prácnosť v ČD*

Bez výhrad*:

S výhradou*:

Popis výhrady:	

Preberajúci týmto potvrdzuje prevzatie nasledovného predmetu dodania, ktorým je tovar:

Zariadenie (typové označenie)*	Sériové číslo*	Miesto inštalácie/Adresa lokality	Počet ks*

Za odovzdávajúceho: **.....** **Meno a Priezvisko**		**Za preberajúceho:** **.....** **Meno a Priezvisko**
..... **Pečiatka, podpis**		**.....** **Pečiatka, podpis**
..... **Dátum odovzdania**		**.....** **Dátum prevzatia**
Poznámka:		

*** Nehodiace sa škrtnúť**

Príloha č. 4 k zmluve č. 37640-8/2023-BA

ZOZNAM SUBDODÁVATEĽOV

Obchodné meno uchádzača: ALCASYS Slovakia, a.s.

Adresa/sídlo uchádzača: Staré grunty 36, 841 04 Bratislava

IČO uchádzača: 35 879 335

Na uskutočnení plnenia Zmluvy o poskytovaní služieb správy a rozvoja call centra a telekomuikačného prostredia v Sociálnej poisťovni č. 37640-8/2023-BA

a) sa nebudú podieľať subdodávatelia a celý predmet zmluvy uskutočníme vlastnými kapacitami.*

~~b) sa budú podieľať nasledovní subdodávatelia:*~~

P. č.	Meno a priezvisko alebo obchodné meno alebo názov subdodávateľa Adresa sídla alebo miesta podnikania	Identifikačné číslo alebo dátum narodenia, ak nebolo pridelené identifikačné číslo	Meno a priezvisko, adresa pobytu a dátum narodenia osoby oprávnenej konať za subdodávateľa	IČO	Podiel plnenia zmluvy v %	Predmet subdodávok
1.						
2.						
3.						

V Bratislave, dňa

.....
Ing. Ján Kostka
predseda predstavenstva
ALCASYS Slovakia, a.s.

*Nehodiace sa prečiarknite

Príloha č. 5 k zmluve č. 37640-8/2023-BA

ZÁPIS

O ZMENE PRÍLOHY Č. X „ZOZNAM XXX“

k Zmluve o poskytovaní služieb pre call centrá a komunikačné systémy a servisných služieb spojených s telekomunikačnou technikou a sieťami č. 37640-8/2023-BA

uzatvorenej podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

(ďalej len „zmluva“) medzi:

dodávateľom ALCASYS Slovakia, a.s., Staré grunty 36, 841 04 Bratislava,

IČO: 35 879 335 (ďalej len „dodávateľ“)

a

objednávateľom Sociálna poisťovňa, Ul. 29. augusta 8 a 10, 813 63 Bratislava,

IČO: 30807484 (ďalej len „objednávateľ“)

V súlade s čl. XX bodom XX zmluvy, v ktorom sa zmluvné strany dohodli o spôsobe zmeny Prílohy č. X k zmluve „Zoznam XXX“, zmluvné strany v zastúpení ich oprávnenými zástupcami podpisujú tento zápis, ktorým sa mení Príloha č. X k zmluve „Zoznam XXX“, ktorá tvorí prílohu k tomuto zápisu.

Dôvod potreby uskutočnenia zmeny Prílohy č. X k zmluve „Zoznam XXX“:

.....
...
.....
..
.....

Tento zápis je neoddeliteľnou súčasťou zmluvy.

Tento zápis nadobúda platnosť dňom jeho podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.

Nadobudnutím účinnosti tohto zápisu sa v celom rozsahu mení znenie Prílohy č. X k zmluve „Zoznam XXX“.

Za dodávateľa:	Za objednávateľa:
....., dňa	Bratislava, dňa
.....	.....
oprávnená osoba	oprávnená osoba

Príloha:

Príloha č. X k zmluve „Zoznam XXX“

Príloha č. 6 k zmluve č. 37640-8/2023-BA

Zoznam expertov

Poradové číslo experta	Meno a priezvisko experta
1.	[redacted]
2.	[redacted]
3.	[redacted]
4.	[redacted]
5.	[redacted]

Príloha č. 7 k zmluve č. 37640-8/2023-BA

Sprostredkovateľská zmluva č. 37640-9/2023-BA

uzatvorená podľa čl. 28 ods. 3 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 osobných údajov) a podľa § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Zmluvné strany

Prevádzkovateľ

Názov:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Ilko generálny riaditeľ Sociálnej poisťovne
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA
IČO:	308 07 484
DIČ:	2020592332

(ďalej len „**prevádzkovateľ**“)

a

Sprostredkovateľ

Obchodné meno:	**ALCASYS Slovakia, a.s.**
Sídlo:	Staré grunty 36 841 04 Bratislava
Štatutárny orgán:	Ing. Ján Kostka predseda predstavenstva
Bankové spojenie:	[redacted]
IBAN:	[redacted]
IČO:	35 879 335
DIČ:	2021805764
IČ DPH:	SK2021805764

Zapísaný v Obchodnom registri Mestského súdu Bratislava III, oddiel Sa, vložka č. 3296/B.

(ďalej len „**sprostredkovateľ**“)

(spolu ďalej ako „**zmluvné strany**“)

Preambula

Zmluvné strany spolu uzatvárajú Zmluvu č. 37640-8/2023-BA o poskytovaní služieb správy a rozvoja call centra a telekomunikačného prostredia v Sociálnej poisťovni, podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „zmluva o poskytovaní služieb“).

Sprostredkovateľ vystupuje v tejto zmluve ako poskytovateľ týchto služieb, pričom nie je vylúčené, že v rámci plnenia predmetu zmluvy sa dostane priamo k spracovaniu osobných údajov dotknutých osôb, aj keď takéto spracovanie nie je predmetom zmluvy. Vzhľadom na vyššie uvedenú možnosť spracovania osobných údajov prevádzkovateľa sprostredkovateľom, zmluvné strany uzatvárajú podľa čl. 28 ods. 3 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 osobných údajov) (ďalej len „GDPR“) a podľa § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „ZOOU“) túto sprostredkovateľskú zmluvu (ďalej len „zmluva“).

Článok I.
Vymedzenie pojmov

Dotknutá osoba je identifikovaná, alebo identifikovateľná fyzická osoba, ktorej sa spracúvané osobné údaje týkajú – dotknutí zamestnanci a klienti Prevádzkovateľa.

Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Prevádzkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

Sprostredkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

Spracúvanie – je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Čl. II
Predmet zmluvy

1. Predmetom tejto zmluvy je poverenie sprostredkovateľa na spracovanie osobných údajov dotknutých osôb v mene prevádzkovateľa a podľa pokynov prevádzkovateľa v rozsahu osobných údajov, spracúvanie ktorých je potrebné pre plnenie účelu zmluvy o poskytovaní služieb.
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje po splnení povinností uvedených v tejto zmluve.
3. Účel spracúvania osobných údajov je vymedzený v zákone č. 461/2003 Z. z. o sociálnom poistení, v Nariadení (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, v Nariadení (ES) Európskeho parlamentu a Rady č. 987/2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, podľa ktorých je prevádzkovateľ oprávnený spracúvať osobné údaje dotknutých osôb za účelom výkonu sociálneho poistenia.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje výhradne pre poskytovanie služieb prevádzkovateľovi, a to na základe pokynov prevádzkovateľa podľa podmienok stanovených v tejto zmluve v súlade so všeobecne záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov. Za pokyny prevádzkovateľa sa považujú pokyny uvedené v tejto zmluve, v servisnej zmluve, prípadne iné písomne zdokumentované pokyny alebo požiadavky prevádzkovateľa na poskytnutie služby v zmysle servisnej zmluvy.
5. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou zmluvy o poskytovaní služieb a to na účel:
    - Účelom spracúvania osobných údajov poskytovateľom je systém poskytovania komplexných komunikačných služieb virtuálnej privátnej siete.
6. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu zmluvy o poskytovaní služieb je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom konkrétu zákonnú povinnosť ustanovuje zmluva o poskytovaní služieb osobitne a § 78 ods. 3 ZOOU.

Čl. III
Zoznam osobných údajov a okruh dotknutých osôb

1. Zmluva, v rámci plnenia predmetu ktorej je sprostredkovateľ poverený spracúvať osobné údaje dotknutých osôb:
   Zmluva č. 37640-8/2023-BA o poskytovaní služieb podľa § 84 a nasl. zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.
2. Zoznam osobných údajov, ktoré môžu byť v prípade realizácie predmetu zmluvy o poskytovaní služieb predmetom spracúvania:
   - meno, priezvisko, titul, adresa bydliska, dátum narodenia, rodné číslo, číslo občianskeho preukazu
   - osobné údaje nevyhnutné na výkon úrazového poistenia
   - osobné údaje nevyhnutné na výkon garančného poistenia

- osobné údaje nevyhnutné na výkon starobného dôchodkového sporenia
- osobné údaje nevyhnutné na výkon lekárskej posudkovej činnosti
- adresné, číslo bankového účtu
- audiozáznam telefonického rozhovoru do IPC (Informačno-poradenské centrum)
- mzdové náležitosti, miesto výkonu práce, pracovisko, údaje o odpracovanom čase, tel. číslo, e-mail, číslo bankového účtu FO,
- identifikačné a kontaktné údaje
- telefónne číslo, e-mail

3. Spracúvané osobné údaje sú typu:
   adresné, zamestnanecké, ekonomické, sociálne, elektronické,

   Iné osobné údaje v rozsahu bodu 2 tohto článku.

Čl. IV
Spôsob výkonu a oprávnenia sprostredkovateľa

1. Osobné údaje o dotknutých osobách prevádzkovateľ spracúva v súlade so zákonom o sociálnom poistení, s Nariadením (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, s Nariadením (ES) Európskeho parlamentu a Rady č. 987/2009 za účelom výkonu sociálneho poistenia a vedenia ekonomickej, prevádzkovej, personálnej a mzdovej agendy Sociálnej poisťovne.
2. Na spracúvanie osobných údajov sprostredkovateľom sa v zmysle § 34 ods. 1 ZOOU nevyžaduje súhlas dotknutej osoby.
3. Sprostredkovateľ má v rámci spracúvania osobných údajov podľa tejto zmluvy povolené operácie s osobnými údajmi v rozsahu najmä:
   a) zaznamenávanie
   b) usporadúvanie,
   c) štruktúrovanie,
   d) uchovávanie,
   e) zmena,
   f) vyhľadávanie,
   g) prehľadávanie,
   h) vymazanie alebo likvidácia,
   i) zálohovanie,
   j) poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb po dobu trvania účelu spracúvania, resp. po dobu platnosti a účinnosti zmluvy o poskytovaní služieb a po dobu platnosti a účinnosti tejto zmluvy.

Čl. V
Vyhlásenie prevádzkovateľa

1. Prevádzkovateľ vyhlasuje, že pri výbere sprostredkovateľa dbal na odbornú, technickú, organizačnú a personálnu spôsobilosť sprostredkovateľa a jeho schopnosť zaručiť ochranu práv dotknutých osôb.
2. Prevádzkovateľ prehlasuje, že
   a) osobné údaje sa spracúvajú na základe primeraného právneho dôvodu v súlade s GDPR a ZOOU,

b) osobné údaje sa spracúvajú v súlade s jasne definovaným účelom spracúvania,
c) osobné údaje, ktoré sprostredkovateľ spracúva na základe tejto zmluvy sú aktuálne, úplné a primerané vzhľadom na účel spracúvania.

Čl. VI
Vyhlásenie sprostredkovateľa

1. Sprostredkovateľ vyhlasuje, že pri činnosti spracovania nedochádza k odovzdaniu osobných údajov do tretej krajiny alebo medzinárodnej organizácii ani iným organizáciám v SR, ak prevádzkovateľ neprejavil s takýmto úkonom vopred písomný súhlas.
2. Sprostredkovateľ vyhlasuje, že prijal také opatrenia organizačného a technického rázu, aby nemohlo dôjsť k neoprávnenému alebo náhodnému prístupu k osobným údajom, k ich zmene, zničeniu či strate, neoprávneným prenosom, k ich inému neoprávnenému spracovaniu, ako aj k inému zneužitiu osobných údajov. Sprostredkovateľ je povinný prijať organizačné a technické opatrenia na prevenciu rizík pre práva a slobody fyzických osôb, vyvolaných spracovaním, v maximálnej miere, akú dovoľujú súčasný stav techniky, náklady a ďalšie ovplyvniteľné okolnosti. Táto povinnosť platí aj po ukončení spracovávania osobných údajov ukončením tejto zmluvy až do okamihu protokolárnej úplnej likvidácie osobných údajov.
3. Sprostredkovateľ vyhlasuje, že zabezpečí, aby všetky ním určené oprávnené osoby boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti.

Čl. VII
Povinnosti sprostredkovateľa

1. Sprostredkovateľ sa pri spracúvaní osobných údajov podľa tejto zmluvy zaväzuje najmä:
   a) postupovať s náležitou starostlivosťou a v súlade s GDPR, ZOOU a súvisiacimi všeobecne záväznými právnymi predpismi Slovenskej republiky, dodržiavať povinnosti vyplývajúce z tejto zmluvy a pokynov prevádzkovateľa, a dodržiavať zásady ochrany osobných údajov zverejnené Prevádzkovateľom,
   b) akékoľvek spracúvanie osobných údajov vykonávať len za účelom plnenia predmetu tejto zmluvy a servisnej zmluvy a len v rozsahu nevyhnutnom na jej plnenie,
   c) údaje dotknutých osôb nezverejňovať, nešíriť či neodovzdávať ďalším osobám,
   d) zaistiť, aby jeho zamestnanci a ďalšie osoby, ktoré využije na plnenie podľa tejto zmluvy, dodržiavali podmienky stanovené GDPR, vnútroštátnymi predpismi a touto zmluvou a boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti,
   e) ak všeobecne záväzné právne predpisy neustanovujú inak, osobné údaje, s ktorými sa dostal do styku v súvislosti s realizáciou zmluvy o poskytovaní služieb nezverejňovať, neposkytovať a nesprístupňovať tretím stranám,
   f) zachovávať mlčanlivosť a zabezpečiť diskrétnosť pri akomkoľvek spracúvaní osobných údajov,
   g) ak zmluva alebo všeobecne záväzný právny predpis neustanovuje inak, nevyhotovovať kópie akýchkoľvek nosičov obsahujúcich osobné údaje a ani z nich nevyhotovovať výpisy alebo odpisy, ktoré by obsahovali osobné údaje,

h) ak všeobecne záväzné právne predpisy upravujúce problematiku archívov a registratúr neustanovujú inak, bezodkladne odovzdávať prevádzkovateľovi všetky získané materiály obsahujúce osobné údaje, ktoré už pre realizáciu zmluvy nepotrebuje, resp. všetky osobné údaje, ktoré bude spracúvať v súvislosti s plnením zmluvy o poskytovaní služieb, bezodkladne po tom, čo pominie dôvod na ich spracúvanie podľa zmluvy, zmazať zo všetkých elektronických, hmotných alebo iných nosičov informácii (napr. pevné disky počítačov, USB kľúče, CD, DVD, dokumenty v papierovej podobe) alebo tieto nosiče zlikvidovať tak, aby nedošlo k úniku týchto údajov,

i) poučiť svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby“), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných údajov, ako aj o iných právach a povinnostiach sprostredkovateľa upravených zmluvou alebo ustanovených všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov, o zodpovednosti za ich porušenie, a to všetko pred uskutočnením prvej operácie s osobnými údajmi,

j) zachovávať mlčanlivosť o osobných údajoch dotknutých osôb a o bezpečnostných opatreniach prijatých na zabezpečenie ochrany osobných údajov, a to aj po skončení tohto zmluvného vzťahu,

k) je povinný nakladať s údajmi ako s informáciami dôvernými v zmysle Zákona 513/1991 Zb. (Obchodný zákonník) a jeho následných novelizácií a je povinný zaviazať týmito povinnosťami aj osoby, ktoré by dojednal na činnosti na plnenie podľa tejto zmluvy (zamestnancov či iných pracovníkov),

l) plniť predmet zmluvy len prostredníctvom riadne a preukázateľne poučených alebo vyškolených oprávnených osôb pre účel plnenia predmetu zmluvy a z nej vyplývajúceho rozsahu a podmienok spracúvania osobných údajov,

m) spracúvať osobné údaje oprávnenými osobami konajúcimi za sprostredkovateľa len v rozsahu pokynov prevádzkovateľa v zmysle čl. 32 GDPR vrátane prípadnej pseudonymizácie a šifrovania s ohľadom na okolnosti konkrétneho prípadu a v rozsahu nevyhnutnom na dosiahnutie účelu spracúvania osobných údajov, ako je uvedené v čl. II tejto zmluvy a pokynu prevádzkovateľa udeleného osobou oprávnenou konať v danom rozsahu za prevádzkovateľa, alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,

n) v prípade sťažností alebo sporu týkajúceho sa spracúvania osobných údajov pri plnení predmetu zmluvy, bezodkladne informovať prevádzkovateľa o tejto skutočnosti a spolupracovať pri riešení sťažnosti alebo sporu s prevádzkovateľom,

o) nepoužiť spracúvané osobné údaje v mene prevádzkovateľa pre vlastnú potrebu, pokiaľ všeobecne záväzné platné právne predpisy neustanovujú inak,

p) zabrániť neoprávneným osobám v prístupe k osobným údajom a k prostriedkom na ich spracovanie, zabrániť neoprávnenému čítaniu, vytváraniu, kopírovaniu, prenosu, úprave či vymazaniu záznamov obsahujúcich osobné údaje a zabezpečiť opatrenia, ktoré umožnia určiť a overiť, komu/kým a akým spôsobom boli osobné údaje odovzdané, resp. kým boli prevzaté a spracúvané.

2. Sprostredkovateľ je pri spracúvaní osobných údajov podľa tejto zmluvy ďalej povinný bezodkladne informovať prevádzkovateľa o

a) poskytnutí a sprístupnení osobných údajov tretej strane spolu s odôvodnením a určením všeobecne záväzného právneho predpisu, ktorý sprostredkovateľovi ukladá

povinnosť poskytnúť, sprístupniť alebo zverejniť osobné údaje dotknutých osôb spracúvaných v mene prevádzkovateľa,

b) skutočnostiach zabraňujúcich plneniu povinností podľa tejto zmluvy,

c) akomkoľvek porušení povinností podľa zmluvy alebo porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov,

d) akomkoľvek porušení ochrany osobných údajov,

e) akomkoľvek porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov zo strany prevádzkovateľa, ak sa podľa názoru sprostredkovateľa pokynom prevádzkovateľa tieto predpisy porušujú.

3. V prípade, ak sprostredkovateľ obdržal žiadosť dotknutej osoby, ktorá si uplatňuje voči prevádzkovateľovi svoje práva podľa článkov 15 až 22 GDPR a § 21 až § 28 ZOOU (napr. právo na prístup k údajom, právo na výmaz alebo opravu osobných údajov), je povinný bezodkladne, najneskôr však do troch pracovných dní od jej prijatia, takúto žiadosť zaslať prevádzkovateľovi prostredníctvom emailovej adresy: zodpovedna.osoba@socpoist.sk, spolu so žiadosťou je sprostredkovateľ povinný prevádzkovateľovi zaslať aj ďalšie relevantné informácie týkajúce sa predmetnej žiadosti, ktoré by mohli mať vplyv na postup vybavenia žiadosti dotknutej osoby zo strany prevádzkovateľa.

4. Sprostredkovateľ je povinný pomáhať prevádzkovateľovi pri zabezpečení plnenia povinností prevádzkovateľa v oblasti bezpečnosti spracúvania, zisťovania porušení ochrany osobných údajov, posudzovania vplyvu na ochranu osobných údajov a poskytovať informácie, ktoré sú mu dostupné.

5. Sprostredkovateľ je povinný dôsledne chrániť spracúvané osobné údaje podľa svojho najlepšieho vedomia, v súlade s ustanoveniami GDPR a ZOOU.

6. Oprávnené osoby sprostredkovateľa resp. subdodávateľa, ktoré budú mať prístup k osobným údajom sú viazaní povinnosťou mlčanlivosti o týchto údajoch a to aj po zániku štátnozamestnaneckého pomeru, pracovného pomeru uzatvoreného v súlade so zákonníkom práce resp. v súlade so zákonom o výkone práce vo verejnom záujme alebo dohody o práci vykonávanej mimo pracovného pomeru v súlade so zákonníkom práce.

7. Oprávnené osoby sprostredkovateľa sú oboznámené so spôsobom oznamovania podozrení z bezpečnostných incidentov v súvislosti s informačným systémom a spracúvanými osobnými údajmi. Oprávnené osoby sprostredkovateľa sú poučené, aby bezodkladne oznamovali určenej osobe prevádzkovateľa akékoľvek podozrenie z bezpečnostného incidentu, ktoré by mohlo mať dopad na bezpečnosť informačného systému s osobnými údajmi. Sprostredkovateľ je povinný bezodkladne prijať relevantné opatrenia k náprave, o bezpečnostnom incidente informovať zodpovednú osobu prevádzkovateľa a e-mailom na adresu: zodpovedna.osoba@socpoist.sk.

8. Sprostredkovateľ je povinný spracovať a dokumentovať prijaté a vykonané technicko-organizačné opatrenia na zaistenie ochrany osobných údajov v súlade s právnymi predpismi EÚ a Slovenskej republiky, k tomu sa vzťahujúcimi. Sprostredkovateľ je povinný spolupracovať s Prevádzkovateľom a byť mu nápomocný pri zaisťovaní plnenia jeho povinností pri prevencii rizík a ďalších povinností Prevádzkovateľa podľa ustanovení čl. 32 – 36 GDPR. K vyžiadaniu Prevádzkovateľa je mu nápomocný technickými a organizačnými prostriedkami pri plnení povinností Prevádzkovateľa reagovať na žiadosti o výkon práv Dotknutej osoby stanovených v kapitole III. GDPR (informácie a prístup k osobným údajom, oprava a výmaz, právo na obmedzenie spracovania atď.)

9. Sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na doloženie toho, že boli splnené povinnosti sprostredkovateľa a stanovené ustanoveniami GDPR a umožní audity, vrátane inšpekcií, vykonávané prevádzkovateľom alebo iným audítorom, ktorého prevádzkovateľ poveril. Pri vykonávaní auditov bude spolupracovať s prevádzkovateľom alebo ním určeným audítorom. Prevádzkovateľ je oprávnený vykonať inšpekciu plnenia povinností sprostredkovateľa a audit bez predchádzajúceho upozornenia. Nespolupráca sprostredkovateľa bude považovaná za podstatné porušenie tejto Zmluvy s možnosťou odstúpenia zo strany prevádzkovateľa, resp. vyvodením zodpovednosti za prípadnú škodu.
10. Po ukončení poskytovania služieb spojených so spracovaním sprostredkovateľ v súlade s rozhodnutím prevádzkovateľa všetky osobné údaje buď vymaže, alebo ich vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo členského štátu nepožaduje uloženie daných osobných údajov. Dojednáva sa, že takýto pokyn bude sprostredkovateľovi daný písomne.
11. Ak sprostredkovateľ poruší GDPR a túto zmluvu tým, že bez pokynu prevádzkovateľa sám určí účely a prostriedky spracovania osobných údajov, stane sa vo vzťahu k týmto údajom a ich spracovaniu prevádzkovateľom so všetkými dôsledkami z toho vyplývajúcimi.

Čl. VIII
Podmienky spracúvania osobných údajov

1. Sprostredkovateľ vyhlasuje, že spracúvanie osobných údajov bude vykonávať sám. Prevádzkovateľ so spracúvaním osobných údajov uvedenými subdodávateľmi súhlasí. Subdodávatelia budú spracúvať osobné údaje na zodpovednosť sprostredkovateľa v rozsahu a za podmienok stanovených v tejto zmluve.
2. Sprostredkovateľ nezapojí do spracovania žiadneho ďalšieho sprostredkovateľa bez predchádzajúceho konkrétneho písomného súhlasu prevádzkovateľa. Náležitosti žiadosti o poskytnutie súhlasu sú uvedené v bode 4 tohto článku zmluvy.
3. Sprostredkovateľ nesmie zveriť spracúvanie osobných údajov subdodávateľovi, ak by tým mohli byť ohrozené práva a právom chránené záujmy dotknutých osôb. Pri zapojení ďalšieho sprostredkovateľa do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa je mu sprostredkovateľ povinný uložiť rovnaké povinnosti týkajúce sa ochrany osobných údajov, ako má on sám.
4. Žiadosť o poskytnutie súhlasu musí obsahovať aspoň nasledovné náležitosti:
   a. označenie subdodávateľa obchodným menom, identifikačnými údajmi a zápisom v obchodnom registri,
   b. odôvodnenie jeho poverenia spracúvaním osobných údajov dotknutých osôb,
   c. vyhlásenie sprostredkovateľa, že subdodávateľ poskytuje dostatočné záruky na vykonanie primeraných technických a organizačných opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov a zmluvy,
   d. vyhlásenie sprostredkovateľa, že subdodávateľ nevykonáva prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii ani iným organizáciám v SR, ktorá nezaručuje primeranú úroveň ochrany osobných údajov,
   e. vyhlásenie sprostredkovateľa, že subdodávateľ poučí svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby“), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných

údajov ako aj o iných právach a povinnostiach sprostredkovateľa upravených touto zmluvou alebo ustanovených všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov.

5. Zmluvné strany sa dohodli, že sprostredkovateľ po obdŕžaní súhlasu na spracúvanie osobných údajov podľa tejto zmluvy prostredníctvom subdodávateľa písomne poverí subdodávateľa spracúvaním osobných údajov podľa zmluvy za podmienok, za akých je oprávnený/povinný ich spracúvať sprostredkovateľ a len v rozsahu nevyhnutnom pre realizáciu zmluvy v záujme prevádzkovateľa, resp. jeho dotknutých osôb. Sprostredkovateľ je povinný predložiť kópiu zmluvy so subdodávateľom do 5 pracovných dni od jej vyžiadania prevádzkovateľovi.
6. Subdodávateľ spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa. Ak subdodávateľ nesplní svoje povinnosti pri spracúvaní osobných údajov dotknutých osôb, sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný za plnenie týchto povinnosti subdodávateľom. Sprostredkovateľ sa nemôže zbaviť zodpovednosti za porušenie povinnosti subdodávateľom tvrdením, že tieto povinnosti porušil subdodávateľ sprostredkovateľa. Ustanovenia GDPR o sprostredkovateľovi, vrátane ustanovení zmluvy upravujúcich povinnosti a podmienky spracúvania osobných údajov zo strany sprostredkovateľa sa vzťahujú aj na subdodávateľa.
7. Sprostredkovateľ je povinný oznámiť prevádzkovateľovi ukončenie spracúvania osobných údajov dotknutých osôb prostredníctvom subdodávateľa, a to bezodkladne, najneskôr však do piatich pracovných dní od ukončenia takéhoto spracúvania. Toto oznámenie musí o. i. obsahovať aj popis spôsobu splnenia povinnosti sprostredkovateľa vo vzťahu k tomuto subdodávateľovi.

Čl. IX
Ostatné dohodnuté podmienky

1. Sprostredkovateľ postupuje pri spracúvaní osobných údajov podľa GDPR a podľa ZOOU.
2. Sprostredkovateľ sa zaväzuje nahradiť prevádzkovateľovi v plnom rozsahu všetky škody, ktoré mu vzniknú v súvislosti s nedodržaním tejto zmluvy zo strany sprostredkovateľa a ktorá prevádzkovateľovi vznikne porušením alebo nesplnením povinností subdodávateľa sprostredkovateľa pri spracúvaní a ochrane osobných údajov vyplývajúcich z ustanovení zmluvy a všeobecne záväzných právnych predpisov.
3. Ochrana osobných údajov podľa zmluvy trvá aj po ukončení zmluvného vzťahu založeného touto zmluvou a zaväzuje aj právnych nástupcov zmluvných strán. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá prevádzkovateľovi vznikla porušením povinností sprostredkovateľa.
4. Sprostredkovateľ je poverený spracúvať osobné údaje po dobu platnosti tejto zmluvy. Okamihom skončenia jej platnosti už sprostredkovateľ nesmie disponovať žiadnymi osobnými údajmi. Sprostredkovateľ je povinný vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje, v prípade že ich spracovával, po ukončení poskytovania služieb týkajúcich sa plnenia zmluvy o poskytovaní služieb a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov, o čom vyhotoví písomné vyhlásenie, ktoré je povinný doručiť prevádzkovateľovi najneskôr do dvoch pracovných dní od skončenia platnosti zmluvy.

5. Kontakt na zástupcu prevádzkovateľa zodpovedného za ochranu osobných údajov: zodpovedna.osoba@socpoist.sk
6. Kontakt na zástupcu sprostredkovateľa: [redacted] .

Čl. X
Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Sprostredkovateľ berie na vedomie povinnosť prevádzkovateľa zverejniť túto zmluvu a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy v plnom rozsahu.
2. Táto zmluva nadobúda platnosť podpisom oprávnených zástupcov zmluvných strán a účinnosť dňom nasledujúcim deň po dni zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Táto zmluva sa uzatvára na dobu určitú, do dňa skončenia platnosti a účinnosti zmluvy o poskytovaní služieb č. 37640-8/2023-BA.
4. Počas platnosti zmluvy o poskytovaní služieb je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane.
5. Práva a povinnosti neupravené touto zmluvou sa budú riadiť príslušnými ustanoveniami právnych predpisov platných na území SR.
6. Zmluvné strany štandardne komunikujú prostredníctvom elektronickej pošty. V prípadoch, keď to vyžaduje zmluva, všeobecne záväzný právny predpis alebo jedna zo zmluvných strán, doručí sa aj listinná podoba požiadavky, súhlasu a pod.
7. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.
8. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k zmluve.
9. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.

10. 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 Bratislave, dňa

Za prevádzkovateľa:

_____

Ing. Michal Ilko
generálny riaditeľ Sociálnej poisťovne

V Bratislave, dňa

Za sprostredkovateľa:

_____

Ing. Ján Kostka
predseda predstavenstva ALCASYS Slovakia, a.s.

Príloha č. 8 k zmluve č. 37640-8/2023-BA

Zmluva č. 37640-10/2023-BA
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

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

Čl. I
Zmluvné strany

Prevádzkovateľ

Názov:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Ilko, generálny riaditeľ Sociálnej poisťovne
IČO:	308 07 484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA

(ďalej len „**prevádzkovateľ**“)

a

Obchodné meno:	**ALCASYS Slovakia, a.s.**
Sídlo:	Staré grunty 36 841 04 Bratislava
Štatutárny orgán:	Ing. Ján Kostka predseda predstavenstva ALCASYS Slovakia, a.s.
Zápis v registri:	Obchodný register Mestského súdu Bratislava III, oddiel Sa, vložka č. 3296/B
IČO:	35 879 335
DIČ:	2021805764
IČ pre DPH:	SK2021805764
Bankové spojenie:	[redacted]
IBAN:	

(ďalej len „**dodávateľ**“)

(spolu ďalej ako „**zmluvné strany**“)

Čl. II
Preambula

1. Prevádzkovateľ je podľa § 3 písm. l) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“) prevádzkovateľom základnej služby podľa § 3 písm. k) body 2 a 3 zákona o kybernetickej bezpečnosti. Dodávateľ je podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom, ktorý na základe zmluvy na výkon činností poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa, ako prevádzkovateľa základnej služby.

2. Zmluvné strany spolu uzatvárajú Zmluvu č. 37640-8/2023-BA o poskytovaní služieb správy a rozvoja call centra a telekomunikačného prostredia v Sociálnej poisťovni, (ďalej len „zmluva o poskytovaní služieb“).

3. Zmluvné strany uzatvárajú za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a podľa § 8 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška“) túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „zmluva“).

Čl. III
Predmet zmluvy

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť pri prevádzke sietí a informačných systémov prevádzkovateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom (ďalej len „kybernetický incident“), ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania sietí a informačných systémov prevádzkovateľa, s prevádzkou ktorých priamo súvisí výkon činností dodávateľa na základe zmluvy na výkon činností.

2. Výkon činností, ktoré priamo súvisia s realizáciou zmluvy na výkon činnosti.

Čl. IV
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné politiky prevádzkovateľa, ktoré tvoria prílohu č. 1 k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami prevádzkovateľa.

2. Dodávateľ súhlasí s tým, že bezpečnostné politiky prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov prevádzkovateľa.

3. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú súčasťou bezpečnostnej politiky prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a bezpečnostných politikách prevádzkovateľa. Dodávateľ

vyhlasuje, že s bezpečnostnými opatreniami súhlasí.

4. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti.

5. Dodávateľ je povinný chrániť všetky informácie ku ktorým má prístup na základe zmluvy na výkon činností alebo tejto zmluvy, alebo ktoré mu boli poskytnuté zo strany prevádzkovateľa s tým, že všetci dotknutí zamestnanci dodávateľa jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých dodávateľ poskytuje služby podľa zmluvy na výkon činnosti (ďalej len „tretia osoba“) sú povinní podpísať vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

6. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá je aktuálna a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi.

7. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy minimálne v oblastiach podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, § 10, §12, §14 a § 15 vyhlášky a v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa.

8. Dodávateľ je povinný doručiť prevádzkovateľovi zoznam zamestnancov dodávateľa subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa zmluvy na výkon činností a tejto zmluvy a ktorí budú mať prístup k informáciám prevádzkovateľa (ďalej len „zoznam osôb“). Dodávateľ je povinný oznámiť prevádzkovateľovi každú zmenu v zozname zamestnancov podľa tohto bodu a to elektronicky prostredníctvom Ústredného portálu verejnej správy (ďalej „UPVS“). Dodávateľ je povinný zabezpečiť, aby každá osoba uvedená v zozname osôb, schválená odborom bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa podpísala vyhlásenie o mlčanlivosti a zúčastnila sa na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností. Po podpísaní vyhlásenia o mlčanlivosti budú týmto osobám sprístupnené bezpečnostné politiky prevádzkovateľa.

9. Dodávateľ je povinný písomne informovať prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom na účely plnenia tejto zmluvy.

10. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Čl. V
Okolnosti plnenia zmluvy

1. Pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto zmluvy a 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.

3. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa podľa zmluvy na výkon činností. Dodávateľ je povinný

plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania zmluvy na výkon činností.

4. Odplata za plnenie povinností dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom dodávateľovi podľa zmluvy na výkon činností a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Čl. VI
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

Dodávateľ je povinný v rámci prevencie kybernetických incidentov, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa, a tým na činnosť prevádzkovateľa:

a. zabezpečiť vlastnú kybernetickú bezpečnosť, aby pri poskytovaní elektronických komunikačných služieb a sietí cez siete a informačné systémy dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa,
b. 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 informáciám prevádzkovateľa,
c. sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
d. sledovať hrozby týkajúce sa dodávateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
e. predchádzať hrozbe vzniku kybernetických incidentov,
f. v prípade vzniku kybernetických incidentov, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
g. prijímať od prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
h. zasielať prevádzkovateľovi 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 sietí a informačných systémov prevádzkovateľa.

Čl. VII
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident prevádzkovateľovi, ktorý by mohol mať vplyv na bezpečnosť dát prevádzkovateľa spôsobom určeným prevádzkovateľom, ktorý je uvedený v bezpečnostnej politike, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto

hlásenie doplní.

2. Dodávateľ je povinný riešiť kybernetický incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení kybernetického incidentu na mieste, reakciou na kybernetický incident a podporou reakcií na kybernetický incident.
3. Pri riešení kybernetických incidentov je dodávateľ povinný na žiadosť prevádzkovateľa spolupracovať s prevádzkovateľom, Národným bezpečnostným úradom a Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického incidentu.
4. Dodávateľ je povinný oznámiť prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ je povinný v čase kybernetického incidentu zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho prevádzkovateľovi.
6. Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.
7. Po vyriešení kybernetického incidentu je dodávateľ na výzvu prevádzkovateľa v určenej lehote povinný predložiť prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „ochranné opatrenie“) na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom na návrhu nového ochranného opatrenia.
8. Po schválení ochranného opatrenia prevádzkovateľom je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť prevádzkovateľovi.
9. Dodávateľ je povinný informovať prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to elektronicky prostredníctvom ÚPVS.

Čl. VIII
Mlčanlivosť

1. Dodávateľ 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. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí.
2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.
3. Dodávateľ 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.

Čl. IX
Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u dodávateľa 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 na základe zákona o kybernetickej bezpečnosti a tejto zmluvy.
2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
3. Prevádzkovateľ môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti prevádzkovateľa pri výkone auditu realizuje prevádzkovateľom poverená tretia osoba.
4. Dodávateľ je pri audite povinný spolupracovať s prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
5. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh a úseku kybernetickej bezpečnosti podľa tejto zmluvy.
6. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer vykonať u dodávateľa audit.
8. Vykonanie alebo nevykonanie auditu prevádzkovateľom nezbavuje zodpovednosti dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.
9. Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

Čl. X
Osobitné ustanovenia

1. Dodávateľ 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 Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, 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 riešenie kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú

službu prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania kybernetických incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa mu predložiť uvedenú dokumentáciu.
4. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy odo dňa jej účinnosti.
5. V prípade, ak dodávateľ plní prevádzkovú zmluvu prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s poskytovaním elektronických komunikačných služieb alebo sietí v súvislosti s prevádzkou sietí a informačných systémov prevádzkovateľa, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby prevádzkovateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subdodávateľov.
6. Všetky informácie, ktoré majú vplyv na plnenie práv a povinností uvedených v tejto zmluve sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na adresy uvedené v záhlaví tejto zmluvy, a zároveň elektronicky prostredníctvom UPVS.
7. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, dodávateľ zodpovedá za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky a za dôsledky a škodu vzniknutú 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, v celom rozsahu. Prevádzkovateľ má nárok na preukázanú náhradu škody, pokuty alebo iné náklady, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov dodávateľa.
8. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.
9. Po ukončení tejto zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

Čl. XI
Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom UPVS, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti je: riaditeľ odboru bezpečnosti informačných systémov.

3. Kontaktná osoba dodávateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je: Ing. František Veľký.
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: [redacted] .
5. Kontakt na zástupcu sprostredkovateľa na úseku kybernetickej bezpečnosti je: [redacted] .
6. Kontaktné osoby podľa bodov 2. a 3. tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme na adresu zmluvnej strany uvedenú v záhlaví tejto zmluvy alebo elektronicky prostredníctvom UPVS.

Čl. XII
Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií) a v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
2. Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády SR.
3. Táto zmluva sa uzatvára na dobu určitú po dobu platnosti a účinnosti zmluvy na výkon činnosti definovanej v článku II - Zmluva č. 37640-8/2023-BA o poskytovaní služieb správy a rozvoja call centra a telekomunikačného prostredia v Sociálnej poisťovni.
4. Počas platnosti a účinnosti zmluvy na výkon činností je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane. Skončenie tejto zmluvy sa netýka tých ustanovení, 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.
5. 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.
6. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.
7. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve.
8. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane nezákonným, 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 nezákonného, neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.
9. Neoddeliteľnou súčasťou tejto zmluvy je

a. Príloha č. 1 – Bezpečnostné politiky
b. Príloha č. 2 – Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni.

10. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.
11. 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 Bratislave, dňa	V Bratislave, dňa
Za prevádzkovateľa:	Za dodávateľa:
_____	_____
Ing. Michal Ilko generálny riaditeľ Sociálnej poisťovne	Ing. Ján Kostka predseda predstavenstva ALCASYS Slovakia, a.s.

Príloha č. 1 k Prílohe č. 8- zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Bezpečnostné politiky

1. Všeobecné ustanovenia

(1) Dodávateľ sa zaväzuje pri plnení zmluvy dodržiavať platné a účinné všeobecne záväzné právne predpisy Slovenskej republiky ako aj právne akty Európskej únie (ďalej „EÚ").

(2) Vstup a pohyb zamestnancov dodávateľa, resp. jeho subdodávateľa, prípadne iných tretích osôb, prostredníctvom ktorých dodávateľ poskytuje služby (ďalej len „tretia osoba“) do priestorov prevádzkovateľa v súvislosti splnením predmetu zmluvy s prevádzkovateľom je možný iba v sprievode na to určeného zamestnanca prevádzkovateľa.

2. Mobilné zariadenia a práca na diaľku

2.1 Politika pre mobilné zariadenia

(1) Spracúvať osobné údaje a iné citlivé údaje prostredníctvom mobilného telefónu je možné len za predpokladu, že citlivé údaje sú uchovávané v zašifrovanej forme a sieťové pripojenie je zabezpečené šifrovaním.

(2) Spracúvať osobné údaje prostredníctvom notebooku je možné len za predpokladu, že osobné údaje sú uchovávané v pseudonymizovanej alebo v zašifrovanej forme a sieťové pripojenie je zabezpečené šifrovaním.

2.2 Práca na diaľku

(1) Vzdialený prístup zamestnancov dodávateľa, resp. jeho subdodávateľa, prípadne inej tretej osoby do informačných systémov a ostatného softvéru prevádzkovateľa nie je možný. Prístup je možné povoliť iba v odôvodniteľných prípadoch, a to iba s dohľadom na to určeného zodpovedného zamestnanca dodávateľa, ak sa dodávateľ s prevádzkovateľom písomne nedohodne inak.

(2) Práca na diaľku sa povoľuje len pre určitý okruh zamestnancov dodávateľa, iba pre určité druhy práce, a musí byť adekvátne zabezpečený aj priestor pracoviska, z ktorého je vykonávaná.

(3) Práca nesmie prebiehať na prostriedkoch v súkromnom vlastníctve, ktoré nie sú pod kontrolou dodávateľa.

(4) Zamestnanec dodávateľa, jeho subdodávateľa, prípadne tretia osoba musia byť adekvátne poučený a zmluvne zaviazaný neporušiť pravidlá na zabezpečenie ochrany, odcudzenia alebo vyzradenia chránených údajov.

(5) Fyzická bezpečnosť musí byť odkontrolovaná na mieste výkonu práce. Kontrolu zabezpečí dodávateľom určený zamestnanec, o čom sa vyhotoví záznam, pričom prevádzkovateľ si vyhradzuje právo kontroly priestorov dodávateľa, resp. jeho subdodávateľa, alebo tretej osoby, z ktorých sa práca na diaľku uskutočňuje.

(6) Žiadosť o zriadenie vzdialeného prístupu pre zamestnanca dodávateľa, resp. jeho subdodávateľa, alebo tretiu osobu postúpi príslušný zmluvný kontakt prevádzkovateľa oddeleniu centrálneho dispečingu a monitorovania služieb IS SP. V žiadosti špecifikuje

rozsah prístupových oprávnení. Po schválení žiadosti riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa a po doručení záznamu o vykonaní kontroly fyzickej bezpečnosti na mieste výkonu práce, zrealizuje požiadavku príslušný administrátor.

2.3 Klasifikácia informácií

(1) Pre potrebu ochrany informácií platí ich nasledovná klasifikačná schéma
   a) citlivé,
   b) interné,
   c) verejné.

(2) Citlivé - sú chránené informácie, a to
   a) osobné údaje poistencov,
   b) osobné údaje zamestnancov,
   c) osobné údaje tretích strán,
   d) mzdové náležitosti zamestnancov,
   e) vymeriavacie základy poistencov,
   f) informácie dôležité pre ochranu osobných údajov v rozsahu: analýza rizík, posúdenie vplyvu na ochranu údajov, bezpečnostný incident, bezpečnostný monitoring, bezpečnostný audit,
   g) údaje zhromaždené v IS prevádzkovateľa (ďalej len „IS SP“).

(3) Interné - sú chránené informácie, kam patria všetky informácie, ktoré nie sú klasifikované ako citlivé alebo verejné, a ktoré
   a) vznikajú v súvislosti s plnením pracovných činností zamestnancov a nie sú určené pre zverejnenie,
   b) boli poskytnuté externým subjektom a nie sú určené pre zverejnenie.

(4) Verejné - nie sú chránené informácie. Patria sem informácie už zverejnené alebo určené na zverejnenie v zmysle platných právnych predpisov a vnútorných predpisov.

2.4 Zaobchádzanie s aktívami

K citlivým informáciám je obmedzený prístup. Prístup k nim majú len oprávnené osoby, ktoré citlivé údaje spracúvajú, alebo len úzky okruh určených osôb prostredníctvom, ktorých dodávateľ plní predmet zmluvy, schválených riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa.

2.5 Zmluvy o dôvernosti alebo utajení

Dohody o zachovaní dôvernosti sú súčasťou zmlúv prevádzkovateľa s dodávateľom. Každá zmluva je pred podpisom odkontrolovaná odborom bezpečnosti informačných systémov na bezpečnostný súlad. Ak sú súčasťou zmluvy osobné údaje, k špecifikácii opatrení na ochranu osobných údajov v oblasti technickej a organizačnej zaujme stanovisko zodpovedná osoba prevádzkovateľa, ktorá vykonáva dohľad nad ochranou osobných údajov u prevádzkovateľa v zmysle GDPR a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zodpovedná osoba“).

2.6 Ochrana testovacích údajov

Ak je na účely testovania dodávateľom nevyhnutné použiť prevádzkové údaje, môže byť

použitá iba ich pseudonymizovaná kópia na základe súhlasu riaditeľa odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa. Kópia prevádzkových údajov musí byť bezpečne vymazaná ihneď po skončení testovania. Dozor vykonáva zodpovedná osoba prevádzkovateľa.

3. Riadenie vzťahov s dodávateľom

3.1 Informačná bezpečnosť vo vzťahoch s dodávateľom

Cieľom je zabezpečiť ochranu aktív prevádzkovateľa, ku ktorým má prístup dodávateľ samostatne, prostredníctvom subdodávateľa alebo prostredníctvom tretej osoby.

3.1.1 Politika informačnej bezpečnosti na vzťahy s dodávateľom

(1) Predtým, než sa dodávateľovi, prípadne jeho subdodávateľovi, alebo tretej osobe povolí prístup k chráneným informáciám prevádzkovateľa, musí byť vykonaná identifikácia rizík informačnej bezpečnosti a implementované vhodné opatrenia na pokrytie identifikovaných rizík na strane dodávateľa, prípadne jeho subdodávateľa, alebo tretej osoby. Uvedené posúdenie rizík informačnej bezpečnosti musí byť v písomnej alebo elektronickej forme dodané prevádzkovateľovi v dostatočnom časovom predstihu pred podpisom zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností na jeho preštudovanie.

(2) Prístup zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osoby k chráneným informáciám prevádzkovateľa nesmie byť dovolený skôr, ako je podpísaná zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s dodávateľom a ako sú realizované primerané bezpečnostné opatrenia na ochranu aktív prevádzkovateľa.

(3) Zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osoby sa zriaďuje prístup na dobu najdlhšie jeden rok. Po uplynutí jedného roka sa potreba prístupu prehodnocuje.

(4) Zriadenie prístupu zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osobe za účelom testovania môže byť zriadené len do testovacieho prostredia prevádzkovateľa. Nasadenie vývojovej verzie APV sa musí uskutočniť výhradne v prostredí prevádzkovateľa za prítomnosti určeného zamestnanca sekcie informatiky. Tieto činnosti musia byť zdokumentované.

3.1.2 Ošetrenie bezpečnosti v zmluvách s dodávateľom

(1) Zmluvy na výkon činností s dodávateľom musia pokrývať všetky významné bezpečnostné požiadavky. Zmluvy na výkon činností obsahujú samostatné ustanovenia alebo klauzuly, ktoré vyplývajú z bezpečnostne relevantnej legislatívy SR, zo slovenských technických noriem a z najlepších skúseností.

(2) Pred spracúvaním osobných údajov k časti bezpečnostných formulácií v návrhu zmluvy na výkon činností zaujme stanovisko zodpovedná osoba prevádzkovateľa, ktorá posúdi dostatočnosť a primeranosť špecifikovaných technických a organizačných opatrení na ochranu osobných údajov.

(3) K bezpečnostným formuláciám v návrhu zmluvy na výkon činností s dodávateľom zaujme stanovisko riaditeľ odboru bezpečnosti informačných systémov, ktorý posúdi dostatočnosť bezpečnostných opatrení a notifikačných povinností, ktoré musia platiť počas celej doby platnosti zmluvy na výkon činností pre zaistenie kybernetickej bezpečnosti.

(4) Nie je prípustné v zmluve na výkon činností špecifikovať bližšie neurčených subdodávateľov alebo tretiu osobu a tým následne zriaďovať prístup pre zamestnancov subdodávateľa alebo tretiu osobu.

3.1.3 Monitorovanie a preskúmanie dodávateľských služieb

(1) Služby a záznamy poskytované dodávateľom sú priebežne kontrolované osobou zodpovednou za výkon zmluvy na výkon činností, a sú monitorované vnútornou kontrolou, bezpečnostným monitoringom, interným auditom alebo externým auditom, tak ako je to zmluvne dohodnuté. Cieľom je overenie, že opatrenia na zaistenie informačnej bezpečnosti sú dodržiavané, že sú dostatočné a že vzniknuté bezpečnostné incidenty sú riešené adekvátnym spôsobom.

(2) V prípade osobných údajov spracúvaných dodávateľom, jeho subdodávateľom alebo treťou osobou túto kontrolu vykonáva aj zodpovedná osoba prevádzkovateľa.

3.1.4 Riadenie zmien v službách dodávateľa

Zmeny v službách poskytovaných dodávateľom sú závislé od systémov a procesov a sú súčasťou hodnotenia rizík.

3.1.5 Zodpovednosť, postupy a informovanie o udalostiach informačnej bezpečnosti

(1) Udalosť, ktorá je považovaná za podozrenie z bezpečnostného incidentu, môže byť spôsobená objektívnymi príčinami (napr. technickou poruchou, priemyselnou haváriou), konaním fyzických osôb (napr. nedbalosť, krádež, prepad, teroristický čin) alebo živelnou pohromou (napr. zemetrasenie, povodeň).

(2) Každé podozrenie z bezpečnostného incidentu musí byť nahlásené a posúdené.

(3) Každý zamestnanec dodávateľa, jeho subdodávateľa alebo tretia osoba, ktorý má podozrenie, že odhalil slabé miesto, alebo zistil podozrenie z bezpečnostného incidentu, je povinný to bezodkladne oznámiť. Oznámenie vykoná nasledovne:

a) e-mailom odboru bezpečnosti informačných systémov prevádzkovateľa na adresu [redacted] a,

b) e-mailom oddeleniu centrálneho dispečingu a monitorovania služieb IS SP na adresu [redacted] a v kópii tomu zamestnancovi prevádzkovateľa, ktorému oznámil podozrenie ústne alebo telefonicky.

3.1.6 Informovanie o slabinách informačnej bezpečnosti

Každý zamestnanec prevádzkovateľa môže informovať o odhalení slabého miesta osobne, telefonicky, emailom alebo interným listom. Informáciu môže odovzdať ľubovoľnému zamestnancovi odboru bezpečnosti, alebo emailom zaslať oddeleniu centrálneho dispečingu a monitorovania služieb IS SP na adresu [redacted].

3.1.6.1 Hlavné kategórie bezpečnostných incidentov

(1) V oblasti ochrany zdravia zamestnancov a klientov

a) registrovaný pracovný úraz, ktorým bola spôsobená pracovná neschopnosť zamestnanca trvajúca viac ako tri dni alebo smrť zamestnanca, ku ktorej došlo následkom pracovného úrazu,
b) technický stav majetku a zariadení (napr. výťah, varič, nevykonávané dezinfekcie klimatizácií, nevykonávané tepovanie kobercov aspoň raz za dva roky a pod.) ohrozujúci zdravie zamestnancov a klientov,
c) technický stav elektrických, plynových a iných rozvodov ohrozujúci zdravie

zamestnancov a klientov,

d) konanie tretích osôb v priestoroch prevádzkovateľa ohrozujúce zdravie zamestnancov a klientov.

(2) V oblasti majetku prevádzkovateľa

a) poškodenie majetku (napr. havária vodovodného potrubia spojená so zatopením prostriedkov informačnej komunikačnej infraštruktúry prevádzkovateľa, prašnosť a pod.),
b) odcudzenie majetku, napr. notebook, osobný počítač a pod.,
c) pokus a narušenie jednotlivých prvkov zabezpečovacieho systému,
d) neoprávnený pobyt v objektoch prevádzkovateľa,
e) násilné vniknutie do budovy, do zariadení (serverovňa, pokladňa, technologická miestnosť), prípadne do automobilov (s následkom odcudzenia spisov, dát a zariadení, ktoré obsahujú informácie, ktorých stratou, zneužitím prípadne zničením by došlo k obmedzeniu služieb poistencom, porušením dôvernosti, finančným stratám),
f) poškodenie a zničenie majetku (časti majetku, napr. klimatizačná jednotka, UPS),
g) následky havárií (prasknutie potrubia, výpadok náhradného zdroja, požiar, zatopenie, zatečenie),
h) odcudzenie (strata) dokladov o poistencovi prevádzkovateľa,
i) podvod, sprenevera,
j) preukázané použitie násilia alebo hrozby bezprostredného násilia v úmysle zmocniť sa aktív prevádzkovateľa.

(3) V oblasti informačnej bezpečnosti prevádzkovateľa

a) zverejnenie hesla používateľa,
b) zmena alebo resetovanie hesla na účte alebo zariadení neoprávnenou osobou,
c) diskreditácia bezpečnostného predmetu (GRID karty, tokenu, prvkov PKI),
d) prístup neoprávnenej (cudzia osoba, nevyškolená obsluha a pod.) osoby do IS SP,
e) vírusová infiltrácia do IS SP, zasielanie nežiadúceho obsahu, škodlivý kód,
f) prienik do IS alebo pokus o prienik,
g) kybernetický bezpečnostný incident,
h) inštalácie neschváleného hardvéru a softvéru na komponentoch IS SP,
i) neoprávnené premiestnenie technických komponentov IS SP,
j) používateľom vykonané zmeny hardvérovej konfigurácie počítača, servera, siete, komunikačných prvkov a pod.,
k) nevykonávanie záloh na serveroch zaradených do systému centralizovaných záloh alebo serverov s inak definovanou zálohovacou stratégiou,
l) zničenie alebo odcudzenie médií, na ktorých sú bezpečnostné zálohy serverov,
m) prepisovanie auditných záznamov,
n) krádež hardvéru alebo softwaru, ktorá ovplyvňuje prevádzky schopnosť IS SP,
o) krádež a deštrukcia dát IS SP,
p) zámerné zneužitie prístupu k zariadeniam IS SP,
q) neplánovaný výpadok elektrického prúdu,
r) poskytnutie, sprístupnenie, alebo zverejnenie osobných údajov konaním

osoby alebo technickou poruchou IS v rozpore s pravidlami platných vnútorných predpisov prevádzkovateľa,

s) neoprávnené použitie vstupno-výstupných zariadení nepatriacich do vlastníctva prevádzkovateľa, spôsobujúce hrozbu nebezpečnej infiltrácie,

t) spracúvanie osobných údajov inou ako oprávnenou osobou,

u) porušenie bezpečnostných vnútorných predpisov prevádzkovateľa majúce za následok nedostupnosť služieb pre klientov alebo partnerov prevádzkovateľa,

v) porušenie vnútorných predpisov prevádzkovateľa s kontrolovateľným až katastrofálnym dopadom pre prevádzkovateľa.

3.1.7 Poučenie a záväzok mlčanlivosti

(1) Vstupné poučenie o ochrane osobných údajov musí absolvovať každý zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba pri nástupe na výkon zmluvných činností na základe zmluvy na výkon činností, pretože z charakteru činností prevádzkovateľa je zrejmé, že každý zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba by mohli aj náhodne prísť do styku s osobnými údajmi. Za zabezpečenie poučenia zamestnanca dodávateľa, resp. subdodávateľa a/alebo tretej osoby je zodpovedný odbor bezpečnosti informačných systémov prevádzkovateľa a to vo vzťahu ku všetkým zamestnancom dodávateľa, prípadne zamestnancom subdodávateľa a/alebo tretej osobe uvedených v Zozname osôb podľa čl. IV ods. 8 tejto zmluvy, ktoré boli riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky schválené ako osoby, prostredníctvom ktorých dodávateľ plní predmet zmluvy na výkon činností. Absolvovaním tohto vstupného poučenia sa zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba nestáva oprávnenou osobou na spracúvanie osobných údajov. Dodávateľ zabezpečí, aby každý zamestnanec dodávateľa, jeho subdodávateľa a/alebo tretia osoba, ktorý majú plniť povinnosti dodávateľa, podpísal pred začatím prác u prevádzkovateľa vyhlásenie o mlčanlivosti.

(2) Za nahlásenie a zabezpečenie účasti zamestnanca dodávateľa, resp. subdodávateľa a/alebo tretej osoby na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností je zodpovedný dodávateľ. Nahlásenie vykoná kontaktná osoba dodávateľa u príslušného zmluvného kontaktu prevádzkovateľa.

Príloha č. 2 k Prílohe č. 8- zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Kyberbezpečnostný štandard

pre projekty a IT v Sociálnej poisťovni

Obsah

Úvod

Informačné systémy, technológie a prostriedky používané v Sociálnej Poisťovni – SP musia byť zabezpečené takým spôsobom, aby sťažovali kompromitáciu infraštruktúry a aby v prípade kompromitácie služby alebo systému boli dôsledky incidentu minimalizované. To znamená, že ak útočník kompromituje časť infraštruktúry, je pre neho zložité dostať sa ďalej a kompromitovať ďalšiu časť infraštruktúry – to znamená je obmedzená možnosť pivotingu. Je nutné implementovať viacúrovňovú hĺbkovú ochranu – to znamená že bude bezpečnostná kontrola na viacerých miestach a prelomením jednej úrovne nedôjde priamo ku kompromitácii dát.
Vzhľadom na neustále sa vyvíjajúce a meniace techniky útokov a obrany je táto metodika žijúcim dokumentom.

Cieľ dokumentu

Tento dokument vyberá a sumarizuje minimálne bezpečnostné zásady a opatrenia potrebné na zabezpečenie informačných systémov, technológií a infraštruktúry SP ako aj pre novovznikajúce či existujúce projekty, procesy, zmeny a ostatné aktivity majúce vplyv na bezpečnosť informačných systémov (BIS) v SP tak aby platili princípy uvedené v úvode.
V dokumente sa používajú kľúčové slová „musí“, „malo by byť“, „odporúča sa“. Tieto sú ohodnotením dôležitosti daného opatrenia s ohľadom na jeho implementačnú náročnosť.
Dokument vznikol na základe podkladov z originálu Metodiky zabezpečenia IKT verejnej správy v oblasti informačnej bezpečnosti, ktorého autorom je CSIRT.SK (*MetodikaZabezpeceniaIKT_v2.1.pdf (gov.sk)*) ako aj zo Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe, a zo Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, z Vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy a aj z Vyhlášky č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
Dokument neobsahuje podrobné implementačné detaily jednotlivých opatrení. Podrobné implementačné detaily budú musieť byť vypracované v projektovej dokumentácii, zmenovej dokumentácii a ostatných podkladových materiálov, ktoré spracujú zadávatelia projektov spolu s IT analytikmi, IT architektami, PM a internými či externými dodávateľmi a následne ich predložia odboru BIS na validáciu.

Obmedzenia

Dokument sa v tejto verzii nezaoberá špecifickými požiadavkami na: fyzickú bezpečnosť infraštruktúry, bezpečnosť mobilných zariadení, bezpečnosť Internetu vecí (IoT – Internet of Things), bezpečnosť ICS systémov (Industrial Control Systems), zabezpečenie služieb využívajúcich IPv4 multicast, zabezpečenie webových služieb (web services).

1 Štandardy implementácie

Bezpečnosť životného cyklu

Pri vývoji riešenia je potrebné myslieť na bezpečnosť už od začiatku a prispôsobiť tomu návrh aj implementáciu samotného riešenia počas jednotlivých fáz.

Návrh riešenia

1) Navrhnuté riešenie musí mať modulárnu štruktúru, pričom
   a) pri návrhu jednotlivých komponentov riešenia musí byť splnený princíp least privilege a všetky entity (t.j. používatelia aj systémy) musia mať prístup iba k údajom / aktívam, ktoré pre svoju činnosť nevyhnutne potrebujú,
   b) architektúra riešenia by mala byť trojvrstvová – mala by pozostávať z prezentačných serverov, aplikačných serverov a databázových serverov,
   c) odporúčané je použitie overených návrhových vzorov, napr. MVC, resp. MVP.
2) Musia byť identifikované všetky súčasti (interné aj externé), od ktorých závisí riešenie. Pre jednotlivé súčasti musia byť identifikované zraniteľnosti, ktoré sa v nich môžu vyskytnúť a vyhodnotiť riziká zneužitia týchto zraniteľností na základe:
   a) prístupového vektoru útočníka (lokálny prístup/sieť),
   b) náročnosti získania prístupu,
   c) potreby autentifikácie,
   d) dopadov úspešného útoku na dostupnosť, integritu a dôvernosť riešenia a údajov v ňom spracovávaných.
3) Na základe analýzy rizík musia byť navrhnuté opatrenia, ako predchádzať možným incidentom a ako postupovať v prípade vzniku incidentu. Tieto opatrenia musia byť zapracované v návrhu riešenia.

Implementácia riešenia

1) Riešenie musí byť vyvíjané v bezpečnom vývojovom prostredí.
2) Pri implementácii by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky / knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb.
3) V prípade, že implementované riešenie potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.

4) Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie, pričom:
   a) jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
   b) commity by mali mať zmysluplné popisy,
   c) mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commite.
5) Nemali by byť použité funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v súčasnej dobe zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.
6) Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však:
   a) zapnuté všetky varovania a ochrany vývojových nástrojov,
   b) varovania vývojového prostredia.
7) Všetky varovania z predchádzajúceho bodu by mali byť opravené.
8) Počas vývoja musí byť vedená vývojárska dokumentácia:
   a) dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii,

b) v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená objednávateľom.

9) Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávateľovi spolu so samotným riešením.
10) Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje:
    a) autentifikačné údaje musia byť uložené iba v podobe osolených hashov (salted hash), pričom použitá hashovacia funkcia by mala byť minimálne sha256,
    b) ostatné osobné údaje (adresy, čísla platobných kariet, čísla občianskych preukazov,...) je odporúčané neukladať v čistej podobe, ale chránené šifrovaním.
11) Musí byť implementované logovanie a logy by mali zaznamenávať minimálne:
    a) (úspešné aj neúspešné) prihlásenie a odhlásenie,
    b) (úspešné aj neúspešné) vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny,
    c) (úspešné aj neúspešné) pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie),
    d) (úspešné aj neúspešné) pokusy o kritické operácie,
    e) zaznamenávajú sa úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
    f) zaznamenávajú sa úspešné a neúspešné prístupy k log súborom,
    g) zaznamenávajú sa úspešné a neúspešné prístupy k systémovým zdrojom,
    h) zaznamenáva sa vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
    i) zaznamenávajú sa zmeny v prístupových oprávneniach,
    j) zaznamenáva sa aktivácia a deaktivácia bezpečnostných mechanizmov,
    k) zaznamenáva sa spustenie a zastavenie procesov,
    l) zaznamenávajú sa konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
    m) zaznamenáva sa spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
    n) zaznamenávajú sa významné aktivity v sieťovej komunikácii,
    o) zaznamenáva sa požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
    p) zaznamenávajú sa IP adresy pridelené prostredníctvom služby DHCP,
    q) záznamy v log súboroch obsahujú ku každej udalosti (ak je k dispozícii) čas a dátum udalosti,
    r) záznamy v log súboroch obsahujú ku každej udalosti identifikáciu používateľa,
    s) záznamy v log súboroch obsahujú ku každej udalosti identifikáciu zariadenia,
    t) záznamy v log súboroch obsahujú ku každej udalosti informáciu týkajúcu sa udalosti,
    u) záznamy v log súboroch obsahujú ku každej udalosti indikáciu úspešnosti, alebo zlyhania operácie,
    v) záznamy v log súboroch obsahujú ku každej udalosti pri sieťových službách zdrojovú IP adresa, cieľovú IP adresa, protokol, zdrojový port, cieľový port,
    w) na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja,
    x) záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
12) Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov.
13) Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server.

Testovanie a verifikácia riešenia

1) Po ukončení vývoja musí prejsť aplikácia testovaním a verifikáciou:
    a) vývojári by mali overiť aspoň pomocou automatizovaných nástrojov štandardné

zraniteľnosti. Malo by prebehnúť minimálne testovanie vstupov (fuzzing) a kontrola práce s pamäťou (memory leaky, memory corruption),
b) vývojári musia zabezpečiť realizáciu opatrení vyplývajúcich z analýzy rizík vypracovanej pri návrhu riešenia,
c) musí byť vykonané penetračné testovanie externou organizáciou,
d) zraniteľnosti a problémy zistené na základe testovania musia byť odstránené a ich oprava musí byť potvrdená opakovaným testovaním.

Nasadenie a prevádzka riešenia

1) Hotové riešenie s odstránenými nájdenými zraniteľnosťami musí byť nasadené v prostredí zabezpečenom na základe odporúčaní v kapitolách o zabezpečení služieb a infraštruktúry.
2) Musí byť zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami. Aplikovanie týchto záplat musí podliehať opatreniam uvedeným v smernici pre riadenie záplat.

Bezpečný návrh – Webové aplikácie

1) Webová stránka by mala pozostávať z verejných a neverejných zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.
2) Citlivé informácie by mali byť uchovávané v zašifrovanej podobe.
3) Validácia vstupov musí byť vykonávaná na strane servera a odporúča sa, aby bola vykonávaná aj na strane klienta.

4) Prezentačný server musí byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby. Aplikačný a databázový server by mali byť umiestnené v internej sieti neprístupnej z Internetu.
5) Kód musí byť udržiavaný, prehľadný a dokumentovaný.
6) Prezentačná vrstva musí byť oddelená od aplikačnej a databázovej vrstvy.

2 Konfigurácia webového servera

Systém

1) Systém, nainštalované aplikácie a frameworky musia byť pravidelne aktualizované z pohľadu bezpečnosti.
2) Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.
3) Počas doby, kedy prebieha údržba, rozsiahlejšia alebo mimoriadna aktualizácia OS/SW a/alebo nasadzovanie bezpečnostných záplat, by mali byť webové servery oddelené od zvyšku siete organizácie alebo byť umiestnené v izolovaných sieťach.
4) Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.
5) Na serveri musia byť zatvorené všetky nepotrebné porty.
6) Autentifikácia používateľov na OS servera musí zodpovedať nasledujúcim požiadavkám:
    a) nepotrebné implicitné účty musia byť odstránené alebo zneplatnené,
    b) neaktívne kontá musia byť zneplatnené.
7) Na serveri by mali byť nakonfigurované používateľské skupiny, kontrola prístupu a udeľovanie privilégií by mali byť pre konkrétnych používateľov riadené ich zaradením do týchto skupín.
8) Heslo ku kontu musí zodpovedať požiadavkám organizácie na komplexnosť hesiel a má byť znemožnený útok hádaním či hrubou silou, viď príloha dokumentu.
9) Právo na vykonávanie systémových úkonov musí byť obmedzené na poverených administrátorov. Tí by sa navyše vzdialene mali prihlasovať iba v restricted režime, ak sa

používa RDP (RDP restricted admin).

10) Lokálny administrátor webservera musí byť unikátny pre každý webový server.
11) Servery s OS Windows buď nesmú byť v doméne alebo musia byť spravované RO doménovým radičom (RODC – read-only domain controller).

Webový server

1) Pri inštalácií webového servera a bezprostredne po nej by mali byť vykonané nasledovné kontroly a akcie:
   a) sw webového servera má byť inštalovaný na dedikovanom hostiteľskom zariadení alebo na dedikovanom virtualizovanom OS,
   b) musia byť aplikované dostupné záplaty a aktualizácie na eliminovanie známych zraniteľností,
   c) pre webový obsah by mal byť vytvorený dedikovaný fyzický disk alebo logická partícia (separátne od OS a SW webového servera),
   d) všetky služby inštalované popri webovom serveri, ktoré nie sú potrebné (napr. FTP server alebo služba vzdialenej administrácie) musia byť vypnuté alebo odstránené,
   e) nepotrebné východzie účty vytvorené pri inštalácií by mali byť odstránené alebo vypnuté,
   f) z webového servera majú byť odstránené testovacie a ukážkové súbory vrátane vykonateľných súborov a skriptov a dokumentácia výrobcu,
   g) odporúčame na server aplikovať hardenovací skript alebo bezpečnostnú šablónu, vhodný pre daný OS a webový server. Info možno čerpať z príručiek dostupných na webstránke CSIRT.SK,
   h) banner HTTP služby by mal byť rekonfigurovaný, podľa potreby aj s ďalšími bannermi tak, aby nereportovali typ a verziu webového servera a podkladového OS.
2) Webový server by mal podporovať iba HTTP metódy POST a GET.
3) Webový server nesmú podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
4) Webový server musí byť odolný voči SlowHTTP DoS útokom (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty, implementácia loadbalancerov).
5) Z webového servera musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy, ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.
6) Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.
7) Na serveri musí byť nakonfigurovaný defaultný virtuálny host na obsluhu prístupu na webserver prostredníctvom IP adresy (cez prehliadač). Nesmie byť zobrazovaná defaultná stránka použitého frameworku a pod.
8) Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.
9) Webový server by nemal podporovať funkcionalitu listovania adresára (Directory listing, Microsoft IIS tilde directory enumeration).
10) Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).
11) Webový server by mal byť chránený WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:
   a) detekcia a prevencia známych útokov (Code injection – SQL, XSS, Command, XPATH, ...),
   b) kontrola používateľských vstupov prostredníctvom whitelistingu a ich prekódovanie do HTML entít alebo podobných bezpečných náhrad.
12) Webový server s aplikáciou spracúvajúcou citlivé údajov a/alebo klasifikované informácie, musí byť chránený WAF, ktorého konfigurácia musí byť reštriktívna (kontrola business logiky a pod).
13) Na zvýšenie dostupnosti webového servera odporúčame použiť load balancery. Podľa možnosti môžu byť rozšírené o web cache. V prípade podpory web cache nesmú byť cacheované administrátorské stránky, prístupové údaje a podobné citlivé informácie.

14) Na zvýšenie dostupnosti webového servera môžu byť ako bezpečnostné brány použité reverzné proxy. Podľa možnosti môžu byť rozšírené o funkcie akcelerácie šifrovania, používateľskej autentifikácie alebo filtrovania obsahu.
15) Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov (kvôli DoS útoku).
16) Webový server musí dodržiavať negociačný postup negociácie TLS spojenia, popísaný v RFC 5746, kvôli zraniteľnosti Insecure renegociation a riziku útoku typu MitM.
17) Webový server by mal podporovať bezpečnú renegociáciu (Secure renegotiation).
18) V prípade viacerých virtuálnych hostov musí byť oddelené úložisko cookies minimálne na úrovni adresárov.

Administrácia, logovanie a zálohovanie

1) Správcovské rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).
2) Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.
3) Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.
4) Webové správcovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.
5) Na serveri musí byť aktívne logovanie:
   a) malo by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent,
   b) pre každý virtuálny host na fyzickom webserveri by mal existovať separátny log,
   c) v logoch musia byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná,
   d) logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii,
   e) na uchovávanie logov musí byť vyhradená dostatočná kapacita,
   f) logy by mali byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov,
   g) logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie, minimálne však raz týždenne. V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva organizácie, by mali byť logy kontrolované denne.
6) Webový server musí byť pravidelne zálohovaný nasledovným spôsobom:
   a) zálohovanie servera má byť upravené organizačnými opatreniami organizácie,
   b) archívna záloha musí byť vytvorená minimálne raz ročne,
   c) diferenciálna alebo zmenová záloha webového servera má byť vytvorená na dennej až týždennej báze,
   d) plný backup webového servera by mal byť vytváraný v týždňových až mesačných intervaloch,
   e) zálohy servera by mali byť periodicky archivované na externé médiá,
   f) mala by byť uchovávaná autoritatívna kópia webovej stránky/stránok.

Kontrola prístupu OS a webového servera

1) Proces webového servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.
2) Webový server by mal byť konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné na čítanie, no nie na zápis. Procesy webového servera by nemali mať právo zápisu do priečinkov, kde je uchovávaný verejný webový obsah (web content).

3) OS by mal byť nakonfigurovaný tak, aby proces webového servera mohol vytvárať log záznamy, no nemohol ich čítať.
4) OS by mal byť podľa možnosti nakonfigurovaný, aby dočasné súbory vytvorené procesmi webového servera boli obmedzené na určený a vhodne zabezpečený priečinok. Ak je to možné, prístup k dočasným súborom by mal byť obmedzený na procesy, ktoré ich vytvorili.
5) Webový obsah a všetky logy ním vytvárané by mali byť umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server.
6) Odporúča sa webový server izolovať od iných procesov použitím prostriedkov ako napríklad chroot, kontajnery, virtualizácia a pod.
7) Pre externé skripty a programy, vykonávané ako časť obsahu webového servera by mal byť vytvorený samostatný priečinok (napr. JavaScript knižnice a pod).
8) Mal by byť stanovený maximálny počet procesov webového servera a/alebo sieťových spojení, ktoré by server mal povoliť.
9) Spúšťanie skriptov, ktoré nie sú výlučne pod kontrolou administratívneho konta, malo by byť zakázané (napr. vytvorením a kontrolou prístupu k separátnemu priečinku, obsahujúcom autorizované skripty).
10) Použitie symbolických linkov by malo byť pre procesy webového servera zakázané.
11) Odporúčame vytvoriť kompletnú maticu prístupov k webovému obsahu (access matrix). V nej by malo byť definované, ktoré súbory a priečinky majú byť prístupné a pre koho.
12) V odôvodnených prípadoch odporúčame zaviesť kontrolu proti botom (napr. CAPTCHA, nofollow, filtrovanie kľúčových slov).

HTTP hlavičky a cookies

1) Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security. Nastavené by mali byť direktívy:
   a) max-age=<číslo> – počet sekúnd, počas ktorých má prehliadač automaticky konvertovať všetky HTTP požiadavky do HTTPS,
   b) includeSubDomains – indikuje, že všetky subdomény aplikácie musia používať HTTPS.
2) V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.).
3) V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.
4) Server by mal používať hlavičky:
   a) X-Frame-Options: SAMEORIGIN (alebo DENY),
   b) X-XSS-Protection: 1,
   c) X-Content-Type-Options: nosniff,
   d) Strict-Transport-Security.
5) V odpovediach webového servera by sa nemali nachádzať hlavičky X-Forwarded-For a HTTP_PROXY.

Aplikácia (webový portál)

1) Aplikácia musí ošetrovať všetky chyby a výnimky.
2) Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.
3) V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.
4) Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).
5) Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.
6) Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.
7) Aplikácia nesmie ukladať citlivé údaje (napríklad identifikátor relácie) v URL adrese. V prípade zakázania cookies v prehliadači musí stránka zobraziť hlásenie o nutnosti použitia cookies (ak sa používajú).
8) Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy na SR).

9) Aplikácie nesmie používať odkazy na nedôveryhodné externé zdroje.
10) Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).
11) Aplikácia nesmie používať funkciu eval() alebo jej alternatívy.
12) Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

Autentifikácia a autorizácia

1) Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).
2) Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token).
3) Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.
4) Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.
5) Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.
6) Pre webové aplikácie, ku ktorým je na prístup nutná autentifikácia, je nutné zabezpečiť, aby žiadna webová stránka, ktorá má byť prístupné až po autentifikácii, nebola dostupná bez vykonania kompletného procesu autentifikácie.
7) Autentifikácia musí prebiehať prostredníctvom protokolu HTTPS.
8) Aplikácia musí vyžadovať používanie silných hesiel.
9) V prípade použitia iniciálnych náhodne generovaných hesiel pre nového používateľa musí aplikácia pri prvom prihlásení vyžadovať zmenu tohto hesla, v súlade s definovanými pravidlami pre tvorbu hesiel.
10) Aplikácia musí umožňovať administrátorom i používateľom zmeniť ich heslo.
11) Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.
12) Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.
13) Aplikácia musí pri zmene hesla vyžadovať opakované zadanie nového hesla (2 krát), pričom nové zadané heslá sa musia zhodovať.
14) Odporúčame pri zmene hesla používať viacfaktorové potvrdenie, napríklad Out-Of-Band kanálom (mail, SMS, KeyCloak, ...).
15) Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.
16) Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.
17) Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať soľ (angl. salt).
18) Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti. Funkcia odhlásenia má byť jednoducho identifikovateľná a dostupná z každej stránky, prístupnej po autentifikácii.
19) Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.
20) Odporúča sa, aby aplikácia podporovala simultánne paralelné prihlásenie k jednému účtu iba z jednej verejnej IP adresy. Odporúča sa, aby aplikácia pri zmene verejnej IP adresy prihláseného používateľa požadovala reautentifikáciu.
21) Odporúča sa naviazanie relácie na parameter User-Agent.
22) Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lockout) po istom počte neúspešných pokusov (maximálne 5) o prihlásenie.
23) Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie musí trvať aspoň 10 minút.
24) Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie do kritického systému by malo trvať aspoň hodinu.
25) Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out,

neúspešný log-in, lockout konta, žiadosť o zmenu hesla).

26) V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.
27) Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať (napr. štandardné loginy ako admin, administrator, user a pod, názov alebo typ aplikácie, kombinácie uvedených a pod.).
28) Aplikácia nesmie pre kritické systémy umožniť funkcionalitu zapamätania si hesla.
29) Používateľské kontá by mali byť po určitej dobe nečinnosti znefunkčnené.
30) Používateľské kontá, ktoré neboli použité do 3 mesiacov od ich vytvorenia (používateľ sa počas danej doby nikdy neprihlásil), by mali byť deaktivované.
31) Každý používateľ a administrátor musia mať jedinečné ID.
32) Aplikácia nesmie umožniť vytváranie účtov s používateľským menom podobným administrátorským či servisným kontám. (admin, administrator, helpdesk, support a pod.).
33) Aplikácia musí korektne inštruovať prehliadač, aby neukladal citlivé informácie, prenášané prostredníctvom HTTPS, do cache (a aby neboli bez kontroly opäť prístupné z histórie prehliadania) minimálne v rozsahu:
    a) Server musí nastavovať vo svojich odpovediach hlavičky:
        - Cache-Control: no-cache, no-store, private, must-re-validate, max-age=0, no-transform,
        - Expires: 0,
        - Pragma: no-cache.

Používateľské vstupy

1) Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.
2) Aplikácia musí brať ako vstupy a primerane ošetrovať všetky používateľom ovplyvniteľné časti dopytu, vrátane HTTP hlavičiek, URL, Cookies a pod. Bez ošetrenia nesmú byť reflektované v odpovedi servera. Napríklad:
    a) aplikácia musí byť odolná voči HTTP Spitting/Smuggling útokom,
    b) aplikácia by mala byť odolná voči HTTP Parameter Pollution (HPP) útokom,
    c) aplikácia/webový server musí byť odolný voči Host Header útoku.
3) Aplikácia by mala používať parametrizované SQL požiadavky (queries), tzv. prepared statements.
4) Aplikácia nesmie na tvorenie SQL dotazov využívať používateľské vstupy bez ich dôkladnej kontroly a ošetrenia.
5) Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím. Minimálne:
    a) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek,
    b) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dopyte alebo parametri príkazu operačného systému,
    c) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML,
    d) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript,
    e) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte REST API,
    f) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch,
    g) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query),
    h) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets,
    i) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI (Server-Side Inclusion statements) príkazoch, ak je použitie SSI nutné a povolené,
    j) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách,
    k) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch,
    l) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách,
    m) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych

výrazoch,
n) aplikácia musí ošetrovať vstupy/dátové prúdy prechádzajúce medzi modulmi aplikácie.

Relácie

1) Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.
2) Aplikácia by nemala povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.
3) Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.
4) Na generovanie CSRF tokenov musí aplikácia používať kryptograficky silný generátor pseudonáhodných čísel.
5) Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie. Identifikátor predchádzajúcej neautentifikovanej relácie musí byť zneplatnený.
6) Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia znovu vygenerovať identifikátor relácie.
7) Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia zneplatniť ostatné relácie príslušného používateľa.
8) Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.
9) Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.
10) Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.
11) Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).
12) Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.
13) Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.
14) Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.
15) Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.

Nahrávanie súborov

1) Aplikácia musí nahrávané súbory ukladať mimo koreňového súboru pre dokumenty (document root) na separátnu partíciu disku (inú, ako je vyhradené na zápis logov), kde súčasne nesmie byť možnosť listovania adresára a nesmie byť možnosť interpretovať nahraté súbory ako napríklad skripty (PHP, ASP, JSP, ...).
2) Aplikácia nesmie spúšťať a vyhodnocovať (evaluate) nahraté súbory.
3) Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.
4) Aplikácia by mala obmedzovať počet súborov nahraných za hodinu.
5) Aplikácia musí umožniť nahrávanie iba špecifických typov súborov a kontrolovať nielen ich príponu, ale aj MIME typ.
6) Aplikácia by mala nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.
7) Nahrávané súbory by sa nemali ukladať pod pôvodným názvom.

Obsah

1) Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.
2) Aplikácia by mala pre všetky poskytované stránky definovať „character set“.
3) Zabezpečenie aktívneho obsahu (skripty, spustiteľné súbory):
    a) právo na čítanie a zápis do súborového systému by malo byť limitované alebo zakázané,
    b) mala by byť povolená žiadna alebo len limitovaná interakcia s inými programami,
    c) nemala by byť potrebná žiadna akcia so SUID privilégiami (OS UNIX/Linux),
    d) skripty by pri spúšťaní externých programov mali používať absolútne cesty alebo nepoužívať žiadne cesty a spoliehať sa na premennú PATH, pričom tá musí obsahovať len bezpečné adresáre,
    e) žiadne priečinky nesmú mať súčasne práva na zápis a vykonávanie,

f) spustiteľné súbory by mali byť umiestnené vo vyhradených priečinkoch,
g) SSI (Server-Side Inclusion) by mali byť zakázané, resp. nie je možné ich spúšťať.

4) Spracovanie XML
   a) aplikácia nesmie podporovať XML External entity expansion,
   b) aplikácia nesmie podporovať parsovanie XML External DTD,
   c) aplikácia nesmie podporovať všetky nadbytočné alebo nebezpečné XML rozšírenia,
   d) aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.

Rôzne

1) Aplikácia by nemala podporovať presmerovanie na používateľom poskytnuté externé umiestnenia.
2) Aplikácia by mala obmedziť (krížový) prístup k (cudzím) doménam prostredníctvom whitelistingu.
   a) ak je na riadenie prístupu medzi doménami používané CORS (Cross Origin Resource Sharing), konfigurácia by mala byť obmedzená na dôveryhodné domény. Napr. nemala by byť použitá direktíva Access-Control-Allow-Origin:*,
   b) ak aplikácia používa na kontrolu prístupu k zdrojom na externých doménach súbory crossdomain.xml a/alebo clientaccesspolicy.xml, obsah by mal mať obmedzený na nutné domény, porty a protokoly. Nemali by byť používané nadmerne voľné pravidlá s „*“. Crossdomain.xml a clientaccesspolicy.xml nesmú byť prístupné koncovému používateľovi.
3) Aplikácia by mala pre všetky emailové funkcionality implementovať rate limiting.
4) Aplikácia by mala pre všetky funkcionality vyžadujúce veľa zdrojov (napríklad CPU čas) implementovať rate limiting.
5) Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.

3 Interná infraštruktúra a vývojové prostredie

Interná infraštruktúra riešenia

1) Jednotlivé vrstvy (databázová, aplikačná, prezentačná) by mali byť umiestnené v separátnych segmentoch a komunikácia medzi nimi musí byť filtrovaná.
2) Jednotlivé servery musia byť hardenované minimálne v rozsahu:
   a) vypnuté všetky nepotrebné procesy a služby,
   b) implementovaný host-based firewall, ktorý kontroluje všetku komunikáciu IN aj OUT a je nakonfigurovaný na princípe „least privilege“,
   c) všetky administrátorské účty spĺňajú politiku hesiel pre administrátorské účty,
   d) servery a všetok softvér je aktualizovaný minimálne raz za 6 (šesť) mesiacov, odporúča sa aktualizovať aspoň raz za mesiac,
   e) na serveroch by malo byť implementované anti-malware riešenie, ktoré je centrálne spravované a centrálne logované,
   f) všetky servery majú nastavené lokálny NTP server ako autoritatívny zdroj času a pre preklad doménových mien na IP adresy používajú lokálne DNS servery,
   g) všetky zariadenia musia byť hardenované podľa odporúčaní výrobcu.

Vývojové prostredie

1) Vo vývojovom prostredí musia byť použité iba nástroje spĺňajúce nasledovné:
   a) musia byť získané legálnym spôsobom z dôveryhodných zdrojov,
   b) musia byť stále podporované výrobcom (t.j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané,

c) musia byť aktualizované minimálne raz za 6 (šesť) mesiacov a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.

2) Vo vývojovom prostredí (vývojárske nástroje a podporné informačné systémy vrátane použitých knižníc tretích strán), v ktorom bude vyvíjané riešenie, musia byť implementované tieto opatrenia:
   a) musia byť implementované príslušné opatrenia na zabezpečenie integrity vyvíjaného riešenia na základe najvyššej požadovanej úrovne ochrany dôvernosti, integrity a dostupnosti informácií, ktoré budú spracovávané vo vyvíjanom riešení,
   b) ak samotné vyvíjané riešenie obsahuje informácie, ktoré je potrebné chrániť z hľadiska dôvernosti, musia byť vo vývojovom prostredí implementované opatrenia na zaistenie dôvernosti na základe požadovanej úrovne ochrany dôvernosti týchto údajov.

4 Štandardy prepojenia

Sieťové protokoly

1) Štandardom sieťových protokolov je
   a) pre informačné systémy a ich komponenty, ktoré sú zavedené po 1. septembri 2009, používanie sieťového protokolu Internet Protocol vo verzii 6 (IPv6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),
   b) pre informačné systémy a ich komponenty, ktoré sú zavedené do 31. augusta 2009 podpora sieťového protokolu Internet Protocol vo verzii 4 (IPv4) s podporou sieťovej technológie Dual stack spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP) pre informačné systémy alebo sieťového protokolu Internet Protocol vo verzii 6 (IPv6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),
   c) používanie skupiny protokolov Internet Procotol Security (IPSEC) na zabezpečenie sieťových protokolov.

Prenos dát

1) Štandardom prenosu dát je

   a) používanie protokolu File Transfer Protocol (FTP) alebo protokolu Hypertext Transfer Protocol (HTTP) a

   b) podpora chráneného prenosu dát cez kryptografický protokol Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group.

2) Špecifikácie prepojenia pomocou sieťových služieb

Štandardom špecifikácie prepojenia pomocou sieťových služieb je používanie Domain Name Services (DNS) ako hierarchickej služby name servera v centrálnych bodoch internetu.

3) Sieťová a komunikačná bezpečnosť

   a) aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov,
   b) na prenos informácií k tretím stranám uzatvorenie zmluvy o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami,
   c) 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,

d) 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,
e) vzdialený prístup do vnútornej siete SP musí podliehať autentifikácii a autorizácii, vyžaduje sa použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
f) zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a ich uchovávanie aspoň 4 (štyri) mesiace,
g) na všetkých serveroch podporujúcich základné služby informačných technológií SP sa implementujú sondy detekcie a prevencie prieniku technológia HIPS,
h) všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom,
i) implementácia druhého sieťového firewallu od iného výrobcu tak, aby interné servery a klientske stanice boli vo vzťahu k externým sieťam chránené dvomi sieťovými firewallmi,
j) implementácia Web Application Firewallu (WAF) na všetkých verejne dostupných a kritických webových aplikáciách,
k) implementácia manažmentu logov,
l) implementácia DNSSEC a jeho využitie pre všetky externe dostupné služby,
m) konfigurácia a izolovanie klientskych portov na prístupových switchoch tak, aby pracovné stanice spolu nemohli priamo komunikovať(technológia PVLAN). Táto požiadavka nahrádza požiadavku zo Z2-Fl) o maximálnom počte MAC adries,
n) zabezpečenie prístupu používateľov k Internetu a k službám mimo siete SP cez proxy server a uchovávanie prístupových logov aspoň 6 (šesť) mesiacov,
o) používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 (štyri) mesiace,
p) uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 6 (šesť) mesiacov,
q) rozdelenie siete do jednotlivých segmentov podľa účelu, pričom v rovnakých segmentoch môžu byť len zariadenia s rovnakými požiadavkami na úroveň zabezpečenia,
r) zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 (šesť) mesiacov.

5 **Prenos elektronickej pošty**

5.1 Prenos elektronickej pošty

1) Štandardom prenosu elektronickej pošty je
   a) používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronických poštových správ,
   b) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group na zabezpečenie prenosu elektronických poštových správ.
2) SMTP banner by nemal obsahovať informácie o použitom softvéri ani iné citlivé informácie. Nesmie byť možné zistiť verziu použitého softvéru prostredníctvom help príkazov.
3) Mailové správy odchádzajúce z organizácie by nemali obsahovať informácie o infraštruktúre organizácie (napríklad privátne IP adresy v hlavičke Received-From).

4) Odpoveď na príkaz VRFY by nemala obsahovať informáciu o existencií adresy alebo používateľského mena. Odporúča sa odpovedať kódom 252 s generickou hláškou.
5) Nemala by byť povolená metóda EXPN.
6) SMTP server by nemal preposlať e-mail, ktorý neobsahuje zdrojovú hlavičkovú e-mailovú adresu.
7) SMTP server musí prijímať správy na doručenie z externých sietí len pre spravované domény.
8) SMTP server musí prijímať správy na preposlanie len od autentifikovaných používateľov alebo z určených SMTP serverov.
9) Server by mal detegovať a blokovať pokusy o rozoslanie veľkého množstva e-mailov.
10) SMTP server musí kontrolovať správy pomocou anti-spam filtra.
11) SMTP server musí kontrolovať správy na prítomnosť škodlivého kódu.
12) SMTP server musí logovať všetky detegované anomálie.
13) SMTP server musí logovať informácie o spracovávaných e-mailoch a tieto informácie by mali byť uchovávané aspoň 6 (šesť) mesiacov. Musia byť uchovávané aspoň 3 (tri) mesiace.
14) Prístup k e-mailovým účtom musí byť možný len prostredníctvom šifrovaného kanála.
15) Odporúča sa na prístup k e-mailovej schránke nepoužívať proprietárne protokoly.
16) Z externých sietí by sa malo pristupovať na e-mail len prostredníctvom HTTPS alebo použitím štandardných protokolov POP3S alebo IMAPS. Odporúča sa autentifikovať klienta aj na základe certifikátu alebo vyžadovať použitie VPN. V prípade použitia iných protokolov by sa malo pristupovať prostredníctvom VPN pripojenia.

5.2 Prístup k elektronickej poštovej schránke

1) Štandardom prístupu k elektronickej poštovej schránke je
   a) používanie protokolu Post Office Protocol vo verzii 3 (POP3) alebo protokolu Internet Message Access Protocol v revidovanej verzii 4.1 (IMAP4rev1) pre prístup k verejným elektronickým poštovým službám,

   b) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group pri chránenom prístupe k verejným elektronickým poštovým službám. Formát elektronických poštových správ.

2) Štandardom formátu elektronických poštových správ je používanie formátu
   a) Multipurpose Internet Mail Extensions (MIME) pri prenose elektronických poštových správ,
   b) Secure/Multipurpose Internet Mail Extensions (S/MIME) pri chránenom prenose elektronických poštových správ.

6 Štandardy prístupu k elektronickým službám

6.1 Aplikačné protokoly elektronických služieb

1) Štandardom aplikačných protokolov elektronických služieb je
   a) používanie protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 s prenosom dát vo formáte Extensible HyperText Markup Language (XHTML) vo verzii 1.0 na komunikáciu medzi klientom a webovým serverom,
   b) podpora protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 a Hypertext Transfer Protocol (HTTP) vo verzii 1.0 pri webových serveroch,
   c) používanie mechanizmu Hypertext Transfer Protocol State Management Mechanism (HTTP Management Mechanism) na Hypertext Transfer Protocol Session Management (HTTP Session Management) a cookies,
   d) používanie protokolu Hypertext Transfer Protocol (HTTP) s Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group na

zabezpečenie prenosu dát medzi klientom a webovým serverom a medzi webovými servermi,

e) používanie protokolu HTTP Strict Transport Security (HSTS) pri poskytovaní elektronických služieb a rozhraní prostredníctvom modulu procesnej integrácie a integrácie údajov.

6.2 Adresárové služby

1) Štandardom adresárovej služby je
   a) používanie aplikačného protokolu Lightweighted Directory Access Protocol vo verzii 3 (LDAP v3) na verejný prístup k adresárovým službám,
   b) používanie jazyka Directory Services Markup Language v2 (DSML v2),
   c) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group pri chránenom verejnom prístupe k adresárovým službám.

7 Štandardy webovej služby

7.1 Middleware protokoly sieťovej komunikácie

1) Štandardom middleware protokolov sieťovej komunikácie je používanie

   a) protokolu Simple Object Access Protocol (SOAP) najmenej vo verzii 1.2 alebo protokolu Representational State Transfer (REST) pri komunikácii medzi servermi v rámci jednej správy a komunikácii medzi klientom a serverom; pri poskytovaní elektronických služieb potrebných na spracovanie elektronických podaní alebo úspešné vyplnenie a prípravu elektronického podania prostredníctvom modulu procesnej integrácie a integrácie údajov sa používa protokol Representational State Transfer (REST) a kódovanie UTF-8,
   b) webových služieb na prístup klientskych aplikácií prostredníctvom internetu na serverové aplikácie správy,
   c) protokolu Hypertext Transfer Protocol (HTTP) na poskytnutie vrstvy webovej služby pre existujúcu serverovú aplikáciu a komunikáciu na aplikačnej úrovni,
   d) jazyka Web Services Description Language (WSDL) na definíciu webovej služby,
   e) registra Universal Description, Discovery and Integration (UDDI) najmenej vo verzii 1.0 na komunikáciu medzi klientom a serverom,
   f) špecifikácií podľa Open Geospatial Consortium (OGC) mapových služieb pod OpenGIS,
      1. WebMap Service (WMS),
      2. Web Feature Service (WFS),
      3. Web Coverage Service (WCS),
      4. Web Processing Service (WPS),
      5. Catalog Service for Web (CSW),
      6. Web Map Tile Service (WMTS).
   g) schémy správ Sk-Talk najmenej vo verzii 3.0 pre asynchrónnu komunikáciu s ústredným portálom verejnej správy podľa aktuálne platnej osobitnej špecifikácie zverejnenej po dohode s orgánom vedenia podľa § 24 ods. 5 Zákona č. 95/2019 na ústrednom portáli verejnej správy,
   h) špecifikácie OpenAPI Specification najmenej vo verzii 3.0 na definíciu webovej služby pri použití protokolu Representational State Transfer (REST),
   i) špecifikácie OpenID Connect podľa OpenID Foundation s OAuth2 podľa osobitnej špecifikácie RFC 6749, ak sa pri použití protokolu Representational State Transfer (REST) vyžaduje autentifikácia a určenie rozsahu oprávnení.

8 Štandardy integrácie dát

8.1 Opisný jazyk dátových prvkov

1) Štandardom opisného jazyku dátových prvkov je používanie jazyka Extensible Markup Language (XML) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pre dátové prvky pri vstupe na rozhranie informačného systému verejnej správy.

8.2 Prenos dátových prvkov

1) Štandardom prenosu dátových prvkov je používanie
   a) jazyka schém XML Schema Definition (.xsd) najmenej vo verzii 1.0 podľa World Wide Web Consortium (W3C) na výmenu dátových prvkov medzi všetkými informačnými systémami verejnej správy,
   b) jazyka Extensible Markup Language (.xml) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pri výmene dátových prvkov, a to s hodnotou atribútu pre deklaráciu menného priestoru spravidla v tvare referencovateľného identifikátora, pričom ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov, je možné namiesto Extensible Markup Language použiť dátový model Resource Description Framework (RDF) opísaný formátmi RDF/XML podľa World Wide Web Consortium (W3C) alebo JSON-LD; pri otvorených údajoch je možné použiť aj formát CSV podľa Vyhlášky č. 78/2020, § 24 písm. e) alebo formát JavaScript Object Notation (JSON),
   c) znakovej sady Unicode Character Set (UCS) podľa technickej normy v 8 bitovom kódovaní UTF-8,
   d) transformačného jazyka XSL Transformations (XSLT) podľa World Wide Web Consortium (W3C) pri transformácii dátových prvkov,
   e) formátu Geography Markup Language (GML) pri výmene priestorových dátových prvkov alebo ak sa na tom zasielateľ a prijímateľ dohodnú jeden z formátov uvedených v štandardoch poskytovania otvorených údajov Vyhlášky č. 78/2020 Z. z. § 40 písm. i),
   f) jazyka Web Ontology Language (OWL) pre ontológie, ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov,
   g) jazyka Shapes Constraint Language (SHACL) podľa World Wide Web Consortium (W3C) pre validáciu dátového modelu Resource Description Framework (RDF) v Centrálnom modeli údajov.

9 Formáty kompresie súborov

1) Štandardom formátov kompresie súborov je
   a) prijímanie a čítanie všetkých doručených formátov kompresie súborov, ktorými sú:
      1. ZIP (.zip) vo verzii 2.0,
      2. TAR (.tar),
      3. GZIP (.gz),
      4. TAR kombinovaný s GZIP (.tgz, .tar.gz).

10 Dátové štandardy

10.1 Výmena údajov

1) Štandardom výmeny údajov je
   a) pri výmene obsahovo príslušných informácií použitie dátových prvkov uvedených v Centrálnom modeli údajov, pričom ak neexistujú obsahovo vhodné dátové prvky v Centrálnom modeli údajov použijú sa dátové prvky uvedené v Prílohe č. 3 Vyhlášky č.

78/2020 Z. z.; v ostatných prípadoch sa použijú vlastné dátové prvky,
b) používanie technických parametrov dátových prvkov podľa dátových štruktúr vo formáte Extensible Markup Language Schema Definition (XSD) zverejnených na webovom sídle orgánu vedenia pri tvorbe definície vlastných dátových štruktúr vo formáte Extensible Markup Language Schema Definition (XSD),
c) rozširovanie typov dátových prvkov na osobitné dátové typy Centrálneho modelu údajov, ak je to potrebné,
d) použitie vlastných dátových prvkov podľa písmena a) spravidla tak, že referenčné údaje určené na automatizované spracovanie a tvoriace súčasť dátového obsahu sú v dátovej štruktúre uvedené ako samostatné dátové prvky na automatizované spracovanie,
e) Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou,
f) Informácie v transakciách informačných technológií alebo medzi informačnými technológiami sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti) certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.

11 Šifrovanie

1) Webový portál musí byť prístupný prostredníctvom protokolu HTTPS.
2) K webovému portálu by sa nemalo pristupovať prostredníctvom HTTP.
3) Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu na ktorej je dostupný webový portál.
4) Identita webového portálu by mala byť zabezpečená certifikátom s Extended Validation.
5) Webový portál nesmie používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.
6) Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.
7) Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.
8) Webový portál by nemal ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.
9) Webový portál by nemal vkladať nešifrované zdroje bez SSL/TLS do stránok používajúcich SSL/ TLS.
10) Pri informačných technológiách s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.
11) Pri informačných technológiách s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä elektronických dokumentov a technológií v nasledujúcich riadkoch:
    a) šifrovanie dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
    b) šifrovanie emailovej komunikácie prostredníctvom PGP alebo S/MIME,
    c) šifrovanie komunikačných kanálov na výmenu nešifrovaných dát,
    d) šifrovanie centrálnych úložísk,
    e) šifrovanie záloh.

12 Šifrovacie kľúče a protokoly

1) Webový server nesmie podporovať protokoly SSLv2, SSLv3, TLS 1.0 a TLS 1.1.
2) Webový server musí podporovať TLS 1.2.
3) Webový server by mal podporovať TLS 1.3.
4) Webový server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64bitov.
5) Webový server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.
6) Webový server nesmie podporovať tzv. Export (EXP) šifry.
7) Použité šifry a protokoly SSL/TLS by mali byť odolné voči známym typom útokov, ako napríklad: FREAK, BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES), BREACH (Pri SSL/TLS musí byť vypnutá http kompresia), POODLE, LOGJAM, TLS Crime (TLS kompresia by mala byť vypnutá).
8) Dĺžka kľúča asymetrickej šifry RSA, DSA v X.509 certifikáte musí byť aspoň 2048 bitov. Toto neplatí pre ECDSA, kedy na dosiahnutie vysokej bezpečnosti postačujú kratšie kľúče – napríklad 256 bitov.
9) X.509 certifikáty musia byť hashované bezpečnými hashovacími funkciami (napr. kvôli možnosti kolíznych útokov nesmie byť použitý algoritmus MD5).
10) Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).
11) Webový server by nemal podporovať RC4, DES a 3DES.
12) Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi. Pri použití CBC šifier je potrebné použiť ďalšiu autentifikáciu, napríklad HMAC (hashovaný autentifikačný kód správ).
13) Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.
14) Konfiguráciu odporúčame otestovať v SSL/TLS teste.
15) Pri správe SSL/TLS je nutné sledovať a v konfigurácii reflektovať aktuálne odporúčania. V prípade použitia WAF/FW pre SSL/TLS preň platia všetky vyššie uvedené požiadavky.

13 Firewall

1) Všetky prepoje medzi segmentami a externými sieťami musia byť chránené firewallom a všetky spojenia (IN aj OUT) musia byť povoľované iba na princípe least privilege.
2) Smerom do vnútra musia byť povolené len špecifikované služby umiestnené v DMZ (politika "default deny").
3) Smerom do externých sieti by mala byť povolená len špecifikovaná komunikácia (pre interné siete by to malo byť len HTTP a HTTPS).
4) Všetky spojenia do externých sietí musia byť smerované cez dedikovaný sieťový firewall. Všetky spojenia do externých sietí okrem VoIP by mali byť smerované aj cez IPS (ak je IPS použité) - výnimkou je VoIP, pre ktoré sa toto odporúča ak to výkon a funkcionalita IPS dovoľuje.
5) Musí byť obmedzená táto komunikácia:
   a) DNS požiadavky smerom do externých sietí (dport UDP/TCP 53) môžu iniciovať len autorizované rekurzívne DNS servery,
   b) SMTP správy smerom do externých sietí (dport TCP 25) môžu posielať len autorizované (t.j. na to určené) SMTP servery,
   c) SMTP smerom do externých sietí môžu iniciovať len autorizované SMTP servery,
   d) Odporúča sa nepovoľovať smerom do externých sietí komunikáciu na TCP/445 (SMB), TCP/6697 (IRC).

14 Zabezpečenie iných služieb

1) Pre prístup k neštandardným službám, ktoré nie je možné hardenovať a zabezpečiť štandardným spôsobom (napr. TLS) sa odporúča využiť prístup cez VPN.

15 Požiadavky z pohľadu BIS vo vzťahoch s tretími stranami

1) V zmluve s dodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa BIS. Môže byť uvedený odkaz na zákon, vyhlášku alebo na osobitný predpis.
2) Požiadavky v oblasti BIS sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií SP.
3) Zmluvné požiadavky na BIS obsahujú najmenej záväzok:
   a) plnenia určených požiadaviek a kritérií pre oblasť BIS pri dodávke predmetu zmluvy,
   b) ochrany informácií, ku ktorým je poskytnutý prístup,
   c) oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa BIS a ďalších opatrení a postupov BIS špecifických na plnenie predmetu zmluvy,
   d) riadenia a monitorovania prístupov do informačných technológií SP vrátane spôsobu a mechanizmu,
   e) možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
   f) oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií SP zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,
   g) spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
   h) zachovania úrovne BIS pri významných zmenách vrátane spôsobu a formy prechodu k inému dodávateľovi.
4) Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká BIS a posúdia sa najmä:
   a) kritické komponenty a prvky služby,
   b) možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
   c) možné riziká BIS vo vzťahoch medzi dodávateľmi a subdodávateľmi,
   d) ďalšie možné riziká BIS vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému dodávateľovi.
5) Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti.
6) Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia BIS v SP.
7) Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.
8) Pre informačné technológie SP, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.
9) Zamedzenie prístupu tretích strán ku všetkým údajom v IT SP, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom len na základe zmluvy tak, aby nebola narušená bezpečnosť IT SP a bezpečnostná politika SP.

Dodatky

Vysvetlenie skratiek
ACL - Access Control List
AP - Access Point
BIS – Bezpečnosť informačných systémov
CSRF - Cross-Site Request Forgery
DHCP - Dynamic Host Configuration Protocol
DMZ - Demilitarized Zone - VLAN, v ktorej sú umiestnené servery poskytujúce služby do externej siete, ktorá je logicky oddelená od internej siete (komunikácia je fultrovaná sieťovým firewallom)
DNS - Domain Name System
DoS – Denial of Service
FW – Firewall
IB – Informačná bezpečnosť
ICS - Industrial Control System
MitM útok – Man in the Middle útok
MVC – návrhový vzor Model–View–Controller
MVP - návrhový vzor Model–View–Presenter
NAC – Network Access Control
NAP - Network Access Protection
NDP - Neighbor Discovery Protocol - protokol v IPv6, okrem iného, nahradzujúci ARP z IPv4
NTP - Network Time Protocol
OS - Operačný systém PVLAN – Private VLAN princíp least privilege
RDP - Remote Desktop Protocol
QoS - Quality of Service
Sieťový firewall - firewall umiestnený v sieti filtrujúci komunikáciu viacerých zariadení, prípadne sietí (nie lokálny firewall)
SNMP – Simple Network Management Protocol
SSO – Single Sign-On
Telepresence
UAC – User Access Control
VLAN – Virtual Local Area Network
VPN – Virtual Private Network
VOIP – Voice over IP
WAF – Webaplikačný firewall - špeciálny typ firewallu, prispôsobený na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku.
Whitelisting - metóda kontroly prístupu k službám, ktorá povoľuje prístup iba špecifikovaným klientom a všetkým ostatným ho zakazuje
XSS - Cross-Site Scripting

Zdroje a Legislatívne východiská

- Slov-lex
- Eur-lex
- Sémantický znalostný strom vedomostí Knowww EU portál
- Vláda SR
- Ústredný portál verejnej správy
- Rokovania legislatívnej rady vlády SR
- Zoznam uznesení vlády SR
- Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
- CSIRT
- NASES
- NBÚ
- Interné normy SP
- NIST
- NSA
- OWASP
- IETF
- IAB
- RFC
- Zákon č. **395/2002** Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. **461/2003** Z. z. o sociálnom poistení,
- Zákon č. **215/2004** Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov,
- Trestný zákon č. **300/2005** Z. z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí),
- Zákon č. **45/2011** Z. z. o Kritickej infraštruktúre,
- Zákon č. **305/2013** Z. z. o elektronickej podobe výkonu pôsobnosti OVM a o zmene a doplnení niektorých zákonov (zákon o e-Governmente),
- Zákon č. **272/2016** Z. z. o dôverných službách (elektronický podpis) pre elektronické transakcie na vnútornom trhu (EiDAS) a o zmene a doplnení niektorých zákonov,
- Zákon č. **18/2018** Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a odporúčacích opatrení (zákon o ochrane osobných údajov),
- Zákon č. **69/2018** Z. z., o Kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov,
- Zákon č. **95/2019** Z. z., o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov,
- Zákon č. **452/2021** Z. z. o elektronických komunikáciách (ochrana súkromia a osobných údajov, ochrana sietí a zariadení),
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **179/2020** Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **78/2020** Z. z. o štandardoch pre informačné technológie verejnej správy,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **85/2018** Z. z., ktorou sa ustanovujú podrobnosti o spôsobe vyhotovenia a náležitostiach listinného rovnopisu elektronického úradného dokumentu,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **70/2021** Z. z. o zaručenej konverzii,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **438/2019** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente,

- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy VS,
- Vyhláška Ministerstva vnútra Slovenskej republiky č. **29/2017** Z. z. o alternatívnom autentifikátore,
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **85/2020** Z. z. o riadení projektov v znení neskorších predpisov,
- Vyhláška Národného bezpečnostného úradu č. 48/2019 Z.z., ktorou sa ustanovujú podorbnosti o administratívnej bezpečnosti utajovaných skutočností,
- Vyhláška Národného bezpečnostného úradu č. **164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- Vyhláška Národného bezpečnostného úradu č. **165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov v aktuálne platnom znení,
- Vyhláška Národného bezpečnostného úradu č. **166/2018** Z. z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
- Vyhláška Národného bezpečnostného úradu č. **362/2018** Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- Nariadenie GDPR - 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),
- Nariadenie Európskeho parlamentu a Rady (EÚ) **2018/1725** z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES,
- Nariadenie Európskeho parlamentu a Rady (EÚ) **2019/881** zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti),
- Smernica Európskeho parlamentu a Rady (EÚ) **2016/1148** zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov vÚnii,
- Smernica Európskeho parlamentu a Rady (EÚ) **2016/2102** z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora,
- Smernica Európskeho parlamentu a Rady (EÚ) **2019/1024** z 20. júna 2019 o otvorených dátach a opakovanom použití informácií verejného sektora,
- Smernica č. **7/2019** o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT,
- Metodika Používateľské princípy pre návrh a rozvoj elektronických služieb verejnej správy https://www.mirri.gov.sk/sekcie/oddelenie-behavioralnych-inovacii/index.html,
- Metodika Jednotný dizajn manuál elektronických služieb verejnej správy - Metodické usmernenie UVSR č. 002089/2018/oLŠISVS-7 zo dňa 11.05.2018 https://www.mirri.gov.sk/wp-content/uploads/2018/10/Metodicke-usmernenie-ID-SK-publikovat.pdf,
- Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (Číslo spisu v DKS: 004307/2019/oBI) https://www.mirri.gov.sk/wp-content/uploads/2019/04/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-verejnej-spravy.pdf,
- Metodika riadenia QAMPR https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html,
- Metodický pokyn k zabezpečeniu centrálneho nákupu produktov a služieb spoločnosti ORACLE v rámci Centrálnej rámcovej dohody na poskytovanie licencií a produktov ORACLE a služieb s nimi súvisiacich https://www.mirri.gov.sk/wp-

content/uploads/2020/02/Metodicky_pokyn_ORACLE_CRD_2019.pdf,

- Metodické usmernenie nariadeniu (GDPR) k spracúvaniu osobných údajov (prostredníctvom web stránok) v súlade s požiadavkami Nariadenia Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20190901.html,
- Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT) – aktuálne znenie MetodikaZabezpeceniaIKT_v2.1.pdf (gov.sk).

Klasifikačné stupne informačných aktív

Klasifikačné stupne informačných aktív opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív (ďalej len „informačné aktíva“) z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

Dôvernosť

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako

- **verejné** informačné aktíva určené pre verejnosť, ktoré sú získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie,
- **interné** informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,
- **chránené** informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,
- **prísne** chránené informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

Ak nie je informačné aktívum explicitne klasifikované je považované za interné.

Integrita

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

- **nízka** zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu,
- **stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej

služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

- **vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a reputáciu prevádzkovateľa základnej služby.

Dostupnosť

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako

- **nízka** zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,
- **stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,
- **vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.