Rámcová dohoda o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne

uzatvorenej podľa § 269 odsek 2 zákona č. 513/1991 Zb. Obchodného zákonníka

Čl. I
Účastníci rámcovej dohody

Objednávateľ:	Sociálna poisťovňa
Sídlo:	Ul. 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Tariška generálny riaditeľ Sociálnej poisťovne
IČO:	30807484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
SWIFT:	SPSRSKBA

(ďalej len „objednávateľ“)

a

Poskytovateľ:	DXC Technology Slovakia s.r.o.
Sídlo:	Galvaniho 7, 820 02 Bratislava
Štatutárny orgán:	Ing. Martin Peluha, konateľ
Bankové spojenie:	Všeobecná úverová banka, a.s. Mlynské nivy 1, 829 90 Bratislava 25
IBAN:	XXXXX
SWIFT:	SUBASKBX
IČO	35 785 306
DIČ	2020213393
IČ DPH	SK2020213393

Zapísaný v Obchodnom, resp. živnostenskom registri Mestského súdu Bratislava III oddiel: Sro, vložka č.: 21438/B.

(ďalej len „poskytovateľ“)

(spolu aj ako „účastníci dohody“)

Čl. II
Východiskové podklady

Východiskovým podkladom na uzatvorenie tejto rámcovej dohody o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne (ďalej len „dohoda“) sú súťažné podklady a ponuka poskytovateľa zo dňa 14. 12. 2023 predložená do verejnej súťaže vyhlásenej vo vestníku verejného obstarávania č. 236/2023 dňa 30. 11. 2023 pod značkou 37929-WYS v rámci zadávania zákazky podľa § 112 až 114a 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“) na predmet zákazky „Zabezpečenie poskytovania služieb pre informačný systém Finančného riadenia Sociálnej poisťovne“.

Čl. III
Predmet dohody

3.1 Predmetom tejto dohody je úprava práv a povinností účastníkov dohody v súvislosti so záväzkom poskytovateľa poskytovať objednávateľovi služby pre informačný systém Finančného riadenia Sociálnej poisťovne (ďalej aj ako „služby“) počas trvania rámcovej dohody na základe individuálnych a aktuálnych potrieb objednávateľa v rozsahu:

3.1.1 poskytovanie služieb technickej podpory IS FRSP,

3.1.2 poskytovanie služieb rozvoja IS FRSP,

3.1.3 poskytovanie školení v súvislosti s používaním IS FRSP.

3.2 Charakteristika informačného systému Finančného riadenia Sociálnej poisťovne (ďalej ako „IS FRSP“) a podrobná špecifikácia požadovaných služieb je uvedená v prílohe č. 1 k tejto dohode.

3.3 Poskytovateľ sa zaväzuje poskytovať objednávateľovi služby na základe čiastkových objednávok podľa aktuálnych potrieb objednávateľa riadne a včas v dohodnutej kvalite a množstve a objednávateľ sa zaväzuje za riadne a včas poskytnuté služby zaplatiť dohodnutú cenu v súlade s prílohou č. 2 k tejto dohode.

3.4 Poskytovateľ berie na vedomie, že (i) objednávateľ je oprávnený na základe svojich potrieb určovať rozsah, a že (ii) rozsahy poskytovaných služieb počas platnosti tejto dohody sú maximálne, a nemožno ich považovať za záväzné v žiadnom rozsahu, (iii) objednávateľ nie je povinný objednať celé množstvo podľa tejto dohody, ani vyčerpať celkový finančný limit predmetu dohody. Celkové odobrané množstvo podľa tejto dohody bude závisieť výlučne od potrieb objednávateľa počas platnosti a účinnosti tejto dohody. Pre vylúčenie pochybnosti účastníci dohody berú na vedomie, že objednávateľ nemusí zrealizovať žiadnu objednávku. Neobjednanie služieb objednávateľom v celom rozsahu a množstve nezakladá právo poskytovateľa uplatniť si nárok na náhradu škody a ani od dohody odstúpiť.

Čl. IV
Miesto a termín plnenia, rozsah a spôsob plnenia

4.1 Miestom plnenia je ústredie objednávateľa na Ul. 29. augusta 8 a 10, 813 63 Bratislava a jeho vybrané pobočky na úrovni krajov v rámci SR.

4.2 Poskytovateľ je povinný poskytnúť služby dohodnutým spôsobom a v termíne plnenia stanovenom v čiastkovej písomnej objednávke.

4.3 Poskytovateľ sa zaväzuje realizovať plnenie predmetu dohody na základe písomných čiastkových objednávok prijatých od objednávateľa, pričom poskytovateľ akceptuje ako záväznú objednávku aj objednávku zaslanú elektronickou poštou. Zmena objednávky sa môže uskutočniť iba písomne a so súhlasom oboch účastníkov dohody.

4.4 V objednávke objednávateľ určí termín plnenia spolu s definovaním spôsobu a rozsahu požadovanej služby (podľa prílohy č. 1 k tejto dohode).

4.5 Účastníci dohody sa dohodli, že všetka vzájomná oficiálna komunikácia podľa tejto dohody, bude prebiehať prostredníctvom zodpovedných osôb objednávateľa a poskytovateľa.

Zodpovedná osoba poskytovateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
*XXXXX**	*Projektový manažér*	*DXC Technology Slovakia s.r.o., Galvaniho 7, 820 02 Bratislava*	*XXXXX@dxc.com*	*+421 XXXXX*

*XXXXX**	*Sales manager*	*DXC Technology Slovakia s.r.o., Galvaniho 7, 820 02 Bratislava*	*XXXXX@dxc.com*	*+421 XXXXX*

*každý samostatne

Zodpovedná osoba objednávateľa:

Titul / meno / Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
XXXXX	*Projektový manažér*	*Sociálna poisťovňa – ústredie, ul. 29. augusta 8 a 10, 813 63 Bratislava*	*XXXXX@socpoist.sk*	*+421 XXXXX*

4.6 Osobami zodpovednými za komunikáciu a preberanie výstupov súvisiacich so zabezpečovaním plnenia predmetu dohody na strane objednávateľa sú konkrétne osoby uvedené v bode 4.5 tohto článku dohody. V prípade zmeny osôb poskytovateľ alebo objednávateľ oznámia nové kontaktné osoby v lehote do 3 dní od uskutočnenia zmeny písomnou formou na emailovú adresu uvedenú v bode 4.5 tohto článku dohody.

4.7 Objednávka musí obsahovať:

a) špecifikáciu spôsobu a rozsahu požadovanej služby,

b) požadovaný termín poskytnutia služby,

c) požadované výstupy.

4.8 Objednávateľ je oprávnený zaslať poskytovateľovi objednávku písomne e-mailom na adresu uvedenú v bode 4.5 tohto článku dohody. Poskytovateľ sa zaväzuje potvrdiť prijatie každej objednávky objednávateľa vyhotovenej a doručenej v súlade s touto dohodou, bez zbytočného odkladu, najneskôr však do dvoch (2) pracovných dní odo dňa jej doručenia. Potvrdenie objednávky bude poskytovateľom urobené formou emailu, resp. odpovede na email, ktorým bola konkrétna objednávka doručená s textom „potvrdzujem objednávku číslo....“.

4.9 Prevzatie objednanej a poskytnutej služby poskytovateľovi písomne alebo elektronicky potvrdí zodpovedná osoba objednávateľa uvedená v bode 4.5 na základe protokolu, ktorý môže byť poskytovateľom zaslaný objednávateľovi aj v elektronickej podobe emailom.

4.10 Poskytovateľ je povinný zabezpečiť, aby experti, ktorých použije na plnenie svojich záväzkov podľa tejto dohody:

a) vykonávali svoju profesiu podľa svojho najlepšieho vedomia a schopností, nestranne a bez predsudkov tak, aby bola dosiahnutá najvyššia kvalita poskytovania služieb,

b) mali všeobecnú povinnosť riadiť sa pokynmi objednávateľa, vystupovať korektne voči objednávateľovi,

c) boli povinní vždy a za každých okolností zachovávať mlčanlivosť o všetkých informáciách, ktoré získali alebo o ktorých sa dozvedeli pri výkone alebo v súvislosti s výkonom svojej profesie; povinnosť zachovávať dôvernosť informácií nie je časovo obmedzená a vzťahuje sa aj na informácie, ktoré nie sú označené ako dôverné.

4.11 Poskytovateľ 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. Poskytovateľ 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.

4.12 V prípade zmeny niektorého z expertov, ktorí sú uvedení v prílohe č. 5 k tejto dohode, je poskytovateľ povinný toto písomne oznámiť objednávateľovi najneskôr do 5 pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví dohody, údaje o navrhovanom novom expertovi. Nový expert musí spĺňať podmienky podľa bodu 4.11 tohto článku dohody. Zmena nového experta sa vykoná zápisom o zmene prílohy k dohode, ktorá nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch účastníkov dohody a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky (ďalej len „register“); vzor zápisu o zmene prílohy k dohode tvorí prílohu č. 4 k tejto dohode; osobami oprávnenými konať vo veciach zmeny prílohy č. 5 sú osoby uvedené v bode 4.5 tejto dohody.

Čl. V
Cena

5.1 Cena za plnenie predmetu dohody je stanovená dohodou účastníkov tejto dohody v eurách, v súlade so zákonom Národnej rady Slovenskej republiky č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky Ministerstva financií Slovenskej republiky č. 87/1996 Z. z., ktorou sa vykonáva zákon č. 18/1996 Z. z. o cenách v znení neskorších predpisov.

5.2 Ceny a predpokladané množstvo predmetu dohody sú uvedené v prílohe č. 2 k dohode.

5.3 Celkový finančný limit tejto dohody sumárne počas platnosti dohody je **214 440,00 EUR bez DPH**.

Slovom: dvestoštrnásťtisícštyristoštyridsať EUR bez DPH.

Celkový finančný limit bol určený výškou predpokladanej hodnoty zákazky ako maximálna predpokladaná hodnota všetkých plnení, ktoré sa predpokladajú počas platnosti a účinnosti dohody. Skutočná cena plnenia je daná násobkami jednotkových cien a množstva vykonaných úkonov. Objednávateľ si vyhradzuje právo nevyčerpať celkový finančný limit za predmet dohody a poskytovateľ sa zaväzuje uvedené právo objednávateľa akceptovať.

Poskytovateľ je platcom DPH. DPH bude účtovaná v aktuálnej sadzbe podľa všeobecne záväzných právnych predpisov, platných v čase zdaniteľného plnenia.

5.4 Celkový finančný limit za celé predpokladané množstvo za predmet dohody uvedený v bode 5.3 tohto článku dohody a jednotkové ceny za predmet dohody uvedené v prílohe č. 2 obsahujú všetky náklady poskytovateľa potrebné na zabezpečenie predmetu dohody podľa čl. III a prílohy č. 1 k tejto dohode, a to personálne náklady na expertov, ostatné náklady na expertov vrátane ich prípravného času, náklady na všetky použité pomôcky potrebné na riadne zabezpečenie poskytovania služieb a všetky nešpecifikované náklady súvisiace s realizáciou predmetu dohody a tiež všetky dane, clá, poplatky, licenčné poplatky, platby vyberané v rámci uplatňovania nesadzobných opatrení ustanovené osobitnými predpismi, ako aj iné náklady súvisiace s plnením predmetu dohody.

5.5 Cena za poskytovanie služieb rozvoja IS FRSP podľa čl. III bod 3.1.2 tejto dohody a za poskytovanie školení v súvislosti s používaním IS FRSP podľa čl. III bod 3.1.3 tejto dohody bude účtovaná v súlade s prílohou č. 2 k dohode ako príslušná jednotková cena vynásobená počtom človekodní.

5.6 Poskytovateľovi nevznikne nárok na úhradu dodatočných nákladov, ktoré si nezapočítal do celkového finančného limitu za predmet dohody.

5.7 V prípade, že poskytovateľ nie je schopný poskytnúť služby v požadovanom termíne, je povinný uhradiť náklady spojené s ich realizáciou treťou osobou.

Čl. VI
Platobné podmienky

6.1 Úhrada ceny podľa čl. V bude realizovaná formou bezhotovostného platobného styku bez zálohovej platby na základe čiastkového plnenia predmetu dohody. Poskytovateľ berie na vedomie a súhlasí, že nie je oprávnený požadovať zaplatenie ceny na iný bankový účet než ten, ktorý je uvedený v záhlaví dohody; k zmene bankového účtu, na ktorý bude objednávateľ uhrádzať svoje splatné záväzky z dohody môže dôjsť iba uzavretím dodatku k dohode, predmetom ktorého bude zmena čísla IBAN a/alebo kódu SWIFT (BIC) bankového účtu poskytovateľa v záhlaví dohody.

6.2 Úhrada ceny za jednotlivé čiastkové plnenia predmetu dohody, na základe písomných objednávok, bude realizovaná priebežne na základe samostatného daňového dokladu – faktúry. Poskytovateľovi vznikne právo na vystavenie faktúry dňom riadneho a včasného splnenia predmetu dohody na základe jednotlivých objednávok, odsúhlasených a potvrdených oprávnenými zástupcami oboch účastníkov dohody. Prílohou faktúr budú protokoly vyhotovené podľa čl. IV bod 4.9 tejto dohody.

6.3 Faktúra za jednotlivé čiastkové plnenia bude doručená objednávateľovi najneskôr do 15 dní odo dňa prevzatia predmetu dohody objednávateľom. Lehota splatnosti faktúry je najneskôr do 30 dní odo dňa jej doručenia do podateľne objednávateľa.

6.4 Poskytovateľom vystavená faktúra ako daňový doklad musí byť vyhotovená v súlade s ustanoveniami zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov.

6.5 Poskytovateľ 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 vyhotovení. Takto predložená faktúra nesmie byť vo forme obrázku, ale musí byť strojovo čitateľná. Poskytovateľ 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 a objednávky vyplývajúce z tejto dohody podliehajú povinnosti zverejnenia zo strany objednávateľa.

6.6 V prípade, že faktúra vyhotovená poskytovateľom nebude obsahovať všetky zákonom stanovené náležitosti alebo bude obsahovať nesprávne alebo neúplné údaje, objednávateľ má právo takúto faktúru vrátiť poskytovateľovi na jej doplnenie, resp. opravu a poskytovateľ je povinný podľa charakteru nedostatku vyhotoviť novú, opravenú, resp. doplnenú faktúru s novou lehotou splatnosti. Poskytovateľ je povinný bezodkladne poslať opravenú alebo novú faktúru znovu aj v elektronickej podobe na e-mailovú adresu objednávateľa, ktorá je uvedená v predchádzajúcom bode tohto článku dohody.

6.7 Účastníci dohody sa dohodli, že objednávateľ má právo znížiť cenu/jej časť o hodnotu zmluvnej pokuty dohodnutej v dohode, uplatnenej voči poskytovateľovi.

Čl. VII
Zmluvné pokuty a zodpovednosť za škody

7.1 V prípade, ak poskytovateľ nedodrží termín na poskytnutie plnenia služby uvedenej v objednávke, objednávateľ má právo uplatniť si nárok na zmluvnú pokutu vo výške 500.- EUR, slovom päťsto EUR, za každý, aj začatý deň omeškania, ak sa účastníci dohody nedohodnú inak.

7.2 Ak je poskytovateľ v omeškaní s odstránením nahlásených chýb alebo vád s vysokou prioritou, je objednávateľ oprávnený požadovať za každú začatú hodinu omeškania zmluvnú pokutu vo výške 150,- EUR, slovom jednostopäťdesiat eur. Ak je poskytovateľ v omeškaní s odstránením nahlásených chýb alebo vád s kritickou prioritou, je objednávateľ oprávnený požadovať za každú začatú hodinu omeškania zmluvnú pokutu vo výške 300,- EUR, slovom tristo eur. Toto právo má objednávateľ bez ohľadu na to, či je naplnený zároveň aj bod 7.4 tohto článku.

7.3 V prípade omeškania objednávateľa s úhradou faktúry v dohodnutej lehote je poskytovateľ 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.

7.4 V prípade porušenia niektorej zo zmluvných povinností poskytovateľa zakladajúcej právo objednávateľa odstúpiť od dohody podľa bodu 9.4 článku IX tejto dohody má objednávateľ právo účtovať poskytovateľovi zmluvnú pokutu vo výške 20.000,- EUR, slovom dvadsaťtisíc eur, a to za každé porušenie. Toto právo má objednávateľ bez ohľadu na to, či od dohody odstúpi alebo nie. Zaplatením zmluvnej pokuty nie je dotknuté právo objednávateľa na náhradu škody v plnej výške a to aj nad výšku zaplatenej zmluvnej pokuty.

7.5 Sankcie podľa bodov 7.1 až 7.4 tohto článku sú splatné do pätnásť (15) dní odo dňa doručenia písomnej výzvy druhému účastníkovi dohody.

7.6 Uhradením zmluvných pokút nezaniká nárok objednávateľa na náhradu škody, ktorá prevyšuje výšku zmluvnej pokuty.

7.7 Poskytovateľ a objednávateľ sú povinní uhradiť prípadné škody, ktoré spôsobili porušením povinností uvedených v tejto dohode druhému účastníkovi dohody v súlade s príslušnými ustanoveniami Obchodného zákonníka.

7.8 Účastníci dohody sa dohodli na započítaní vzájomných pohľadávok podľa ustanovenia § 364 Obchodného zákonníka.

7.9 Účastníci dohody sa dohodli, že objednávateľ má právo znížiť dohodnutú cenu o hodnotu zmluvnej pokuty uplatnenej objednávateľom voči poskytovateľovi. Poskytovateľ je v takom prípade povinný vystaviť faktúru, ktorá bude znížená o uplatnenú zmluvnú pokutu.

7.10 Zaplatením zmluvnej pokuty sa poskytovateľ nezbavuje povinnosti nedostatky odstrániť.

7.11 Zodpovednosť za škodu sa riadi podľa príslušných ustanovení Obchodného zákonníka.

7.12 Poskytovateľ zodpovedá za škody spôsobené objednávateľovi na jeho majetku pri plnení dohody zanedbaním svojich povinností alebo v dôsledku okolností, o ktorých poskytovateľ vedel, alebo mal vedieť z titulu svojej činnosti v čase plnenia dohody, alebo ich mohol predvídať.

7.13 Ak poruší jeden z účastníkov dohody svoje povinnosti alebo akýkoľvek záväzok vyplývajúci z tejto dohody, je povinný nahradiť škodu tým spôsobenú druhému účastníkovi dohody. Za škodu sa považuje skutočná škoda a náklady vzniknuté poškodenému účastníkovi dohody v súvislosti so škodovou udalosťou. Za škodu sa nepovažuje nepriama alebo následná škoda, škody na strate zisku (ušlý zisk) alebo tržieb alebo iný druh ekonomických strát.

7.14 Účastník dohody, ktorý porušil svoju povinnosť alebo akýkoľvek záväzok vyplývajúci z tejto dohody, sa môže zbaviť zodpovednosti za náhradu škody, ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku vyplývajúceho z tejto dohody došlo v dôsledku okolností vylučujúcich zodpovednosť. Ak porušenie povinností alebo akéhokoľvek záväzku vyplývajúceho z tejto dohody spôsobila tretia osoba (subdodávateľ), ktorej povinný účastník dohody zveril plnenie svojej povinnosti alebo záväzku, je u povinného účastníka dohody vylúčená zodpovednosť za škodu len v prípade, ak by k vzniku škody došlo v dôsledku okolností vylučujúcich zodpovednosť.

Čl. VIII
Práva a povinnosti účastníkov dohody

8.1 Poskytovateľ sa zaväzuje poskytovať služby podľa požiadaviek objednávateľa v náležitej kvalite.

8.2 V prípade, ak je poskytovateľ povinný v rámci poskytovania služieb vypracovať písomnú dokumentáciu, zaväzuje sa predložiť objednávateľovi na pripomienky a schválenie návrh takejto písomnej dokumentácie, a to v elektronickej podobe jej doručením na stanovenú e-mailovú adresu. Objednávateľ je oprávnený predložiť poskytovateľovi pripomienky a/alebo doplňujúce požiadavky k návrhu písomnej dokumentácie bezodkladne podľa povahy spracúvaného dokumentu, najneskôr však do 10 (desať) pracovných dní odo dňa jej doručenia; v prípade ak takéto pripomienky a/alebo doplňujúce požiadavky v lehote uvedenej pred bodkočiarkou nepredloží, má sa za to, že so znením návrhu písomnej dokumentácie súhlasí.

8.3 Poskytovateľ je povinný posúdiť predložené pripomienky a doplňujúce požiadavky a v prípade, ak tomu nebránia závažné dôvody (napr. nesúlad s právnou úpravou), tieto pripomienky a doplňujúce požiadavky zapracovať do návrhu písomnej dokumentácie a upravený návrh písomnej dokumentácie bezodkladne doručiť objednávateľovi v závislosti od povahy spracúvaného dokumentu, a to najneskôr do 10 (desať) pracovných dní odo dňa predloženia pripomienok a doplňujúcich požiadaviek. V prípade, ak poskytovateľ nezapracuje do návrhu písomnej dokumentácie pripomienky a doplňujúce požiadavky objednávateľa, je v rovnakej lehote povinný túto skutočnosť písomne odôvodniť.

8.4 Ak má objednávateľ výhrady k forme, spôsobu a rozsahu zapracovania pripomienok a doplňujúcich požiadaviek, je oprávnený vrátiť upravený návrh písomnej dokumentácie poskytovateľovi. V prípade, ak nemá objednávateľ (ďalšie) pripomienky a doplňujúce požiadavky k doručenému upravenému návrhu písomnej dokumentácie, oznámi túto skutočnosť poskytovateľovi najneskôr do 10 (desať) pracovných dní odo dňa doručenia upraveného návrhu písomnej dokumentácie; v prípade, že sa objednávateľ v tejto lehote nevyjadrí, má sa za to, že k návrhu písomnej dokumentácie nemá ďalšie pripomienky alebo doplňujúce požiadavky. Poskytovateľ je povinný bez zbytočného odkladu, najneskôr však do 10 (desať) pracovných dní od doručenia oznámenia podľa predchádzajúcej vety, predložiť objednávateľovi finálnu verziu písomnej dokumentácie na prevzatie; dátum, čas a miesto prevzatia si dohodne objednávateľ a poskytovateľ.

8.5 Poskytovateľ je povinný dokumentáciu odovzdať objednávateľovi v elektronickej podobe vo formáte .pdf na jednom nosiči dát s trvalo uchovateľným obsahom (USB resp. flash disk). Poskytovateľ je povinný na základe požiadavky objednávateľa odovzdať objednávateľovi takúto dokumentáciu na základe preberacieho protokolu. Poskytovateľ je povinný dokumentáciu odovzdať najneskôr do 10 (desať) pracovných dní odo dňa jej schválenia.

8.6 Poskytovateľ je povinný oznámiť objednávateľovi všetky okolnosti, ktoré zistil pri plnení svojich záväzkov, a ktoré môžu mať vplyv na zmenu pokynov objednávateľa.

8.7 Poskytovateľ sa zaväzuje chrániť práva a právom chránené záujmy objednávateľa, dôsledne využívať všetky zákonné prostriedky a uplatňovať všetky dostupné možnosti, čo podľa svojich odborných vedomostí a pokynov objednávateľa považuje za účelné.

8.8 Účastníci dohody sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto dohody a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na riadne plnenie tejto dohody.

8.9 Poskytovateľ je oprávnený plniť si svoje povinnosti podľa tejto dohody aj prostredníctvom tretích osôb (najmä prostredníctvom expertov, ktorí nie sú v pracovnoprávnom vzťahu k poskytovateľovi), v takom prípade však zodpovedá voči objednávateľovi, akoby plnil sám.

Čl. IX
Skončenie dohody

9.1 Dohoda môže skončiť:

a) uplynutím doby, na ktorú bola uzatvorená, t. j. 12 mesiacov odo dňa účinnosti dohody, alebo vyčerpaním celkového finančného limitu, dohodnutého v čl. V bode 5.3 tejto dohody, podľa toho, ktorá skutočnosť nastane skôr. V prípade nevyčerpania celkového finančného limitu sú účastníci dohody oprávnení platnosť a účinnosť dohody predĺžiť maximálne o šesť (6) mesiacov alebo do vyčerpania finančného limitu, podľa toho, ktorá skutočnosť nastane skôr a to formou písomného dodatku k dohode,

b) písomnou dohodou účastníkov dohody,

c) výpoveďou ktoréhokoľvek z účastníkov dohody,

d) odstúpením od dohody ktoréhokoľvek z účastníkov dohody

9.2 Dohoda môže byť skončená písomnou výpoveďou ktoréhokoľvek z účastníkov dohody aj bez uvedenia dôvodu. Účastníci dohody sa dohodli na dvojmesačnej výpovednej lehote, ktorá začne plynúť prvým dňom kalendárneho mesiaca nasledujúceho po doručení písomnej výpovede

druhému účastníkovi dohody.

9.3 Vypovedaním dohody nevzniknú objednávateľovi žiadne dodatočné záväzky voči poskytovateľovi.

9.4 Objednávateľ môže od dohody odstúpiť:

9.4.1 v prípade podstatného porušenia tejto dohody poskytovateľom; za podstatné porušenie sa považuje:

a) omeškanie poskytovateľa s plnením predmetu dohody v dohodnutom termíne,

b) ak poskytovateľ neposkytne predmet dohody v dohodnutej kvalite a rozsahu a cene,

c) neakceptovanie objednávky objednávateľa,

9.4.2 v prípade nepodstatného porušenia dohody, len ak poskytovateľ nesplní svoju povinnosť ani v dodatočnej primeranej lehote, ktorá mu na to bola poskytnutá,

9.4.3 v prípade opakovaného porušenia akýchkoľvek povinností poskytovateľom, ktoré vyplývajú z ustanovení tejto dohody alebo z ustanovení všeobecne záväzných právnych predpisov; za opakované porušenie sa považuje preukázateľné porušenie dvakrát a viackrát.

9.4.4 podľa § 19 zákona o verejnom obstarávaní.

Odstúpeniu objednávateľa od dohody musí predchádzať upozornenie poskytovateľa na neplnenie povinností upravených v dohode a na možnosť ukončenia tejto dohody odstúpením.

9.5 Poskytovateľ môže od tejto dohody odstúpiť v prípade, ak je objednávateľ v omeškaní s úhradou riadne vystavenej faktúry podľa tejto dohody po dobu dlhšiu ako 30 dní po lehote jej splatnosti; skončeniu dohody musí predchádzať upozornenie na neplnenie platobných povinností objednávateľa a na možnosť ukončenia tejto dohody odstúpením.

9.6 Odstúpenie od dohody musí byť uskutočnené písomnou formou a účinnosť nadobudne dňom jeho doručenia druhému účastníkovi dohody. Úplná alebo čiastočná zodpovednosť účastníka dohody bude vylúčená v prípadoch zásahu vyššej moci.

9.7 Pri podstatnom porušení povinností vyplývajúcich z dohody, môže oprávnený účastník dohody písomne požadovať od povinného účastníka dohody v súlade so všeobecne záväznými právnymi predpismi náhradu škody, ktorá jeho vinou vznikne.

9.8 Skončením dohody zanikajú všetky práva a povinnosti účastníkov dohody vyplývajúce z dohody s výnimkou ustanovení, ktoré sa týkajú nároku na náhradu škody vzniknutej porušením tejto dohody, nároku na zaplatenie dohodnutej zmluvnej pokuty podľa ustanovení tejto dohody a ďalej ustanovenia tejto dohody, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení dohody, napr. dôvernosť informácií a mlčanlivosť.

Čl. X
Dôvernosť informácií a mlčanlivosť

10.1 Účastníci dohody a ich zamestnanci, ako aj tretie osoby a prípadní subdodávatelia, sú povinní zachovávať v tajnosti všetky dôverné informácie, ktoré sú uvedené v tejto dohode 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 s dohodou alebo s ktorými sa oboznámili počas plnenia dohody, resp. ktoré súvisia s predmetom plnenia, s údajmi, ktoré podliehajú ochrane podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (GDPR) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s údajmi o klientoch a obchodných partneroch objednávateľa a s údajmi získanými v rámci predzmluvných rokovaní, ktoré súvisia s dohodou, s výnimkou nasledujúcich prípadov:

a) ak je poskytnutie informácie od dotknutého účastníka dohody 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 v znení neskorších predpisov),

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

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

d) ak je informácia poskytnutá odborným poradcom dotknutého účastníka dohody (vrátane právnych, účtovných, daňových a iných poradcov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti alebo, ak sa voči dotknutému účastníkovi dohody zaviazali povinnosťou mlčanlivosti,

e) pre účely akéhokoľvek súdneho, rozhodcovského, správneho alebo iného konania, ktorého je dotknutý účastník dohody účastníkom,

f) ak je informácia poskytnutá so súhlasom druhého účastníka dohody.

10.2 Účastníci dohody, ich subdodávatelia a tretie osoby sú povinní zachovávať mlčanlivosť o všetkých dôverných informáciách, ibaže by z tejto dohody alebo z príslušných všeobecne záväzných právnych predpisov vyplývalo inak. Tento záväzok trvá aj po ukončení platnosti a účinnosti tejto dohody.

10.3 Účastníci dohody, ich subdodávatelia a tretie osoby sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhého účastníka dohody nepoužijú 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 účastníkov dohody, audítori alebo právni poradcovia účastníkov dohody, ktorí sú ohľadne im sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.

10.4 Účastníci dohody, ich subdodávatelia a tretie osoby sa zaväzujú, že všetky zúčastnené osoby a subjekty, budú s takto poskytnutými informáciami a zistenými skutočnosťami nakladať ako s dôvernými informáciami.

10.5 Účastníci dohody sa zaväzujú, že upovedomia druhého účastníka dohody o porušení povinnosti mlčanlivosti bez zbytočného odkladu po tom, ako sa o takomto porušení dozvedeli.

10.6 Účastníci dohody sa zaväzujú, že budú ochraňovať dôverné informácie druhého účastníka dohody s rovnakou starostlivosťou ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti.

Čl. XI
Osobitné ustanovenia

11.1 Poskytovateľ (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. 3 k tejto dohode, 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. Objednávateľ neuzatvorí túto dohodu s poskytovateľom, ak v čase uzavretia dohody nebude mať poskytovateľ, 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 poskytovateľovi bude uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní.

11.2 Objednávateľ môže podľa § 19 ods. 3 zákona o verejnom obstarávaní odstúpiť od dohody, ak

poskytovateľ v čase uzatvorenia dohody nebol zapísaný v registri partnerov verejného sektora, ak mu zákon o registri partnerov verejného sektora takúto 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 dohody stala konečným užívateľom výhod poskytovateľa alebo jeho subdodávateľa osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní, môže objednávateľ odstúpiť od dohody po uplynutí 30 dní odo dňa, keď táto skutočnosť nastala, ak táto skutočnosť stále trvá.

11.3 Na plnenie predmetu dohody môže poskytovateľ využiť subdodávateľov. Poskytovateľ je povinný pri uzatvorení dohody uviesť zoznam subdodávateľov, ktorý obsahuje údaje o všetkých známych subdodávateľoch poskytovateľa v čase uzatvorenia tejto dohody a údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Zoznam subdodávateľov tvorí prílohu č. 3 k tejto dohode a obsahuje okrem uvedených údajov aj podiel plnenia z dohody v % a stručný opis časti dohody, ktorá bude predmetom subdodávky.

11.4 Poskytovateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi, ktorý je uvedený v prílohe č. 3 k tejto dohode najneskôr do piatich (5) pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví dohody.

11.5 V prípade zmeny subdodávateľa je poskytovateľ povinný najneskôr tri (3) pracovné dni pred zmenou subdodávateľa 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 č. 3 k dohode, ktorý nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch účastníkov dohody 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 k dohode tvorí prílohu č. 4 k tejto dohode; osobami oprávnenými konať vo veciach zmeny prílohy č. 3 k dohode sú osoby uvedené v bode 4.5 tejto dohody.

11.6 Navrhovaný subdodávateľ musí spĺňal 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.

11.7 Využitím subdodávateľov nie je dotknutá zodpovednosť poskytovateľa za plnenie predmetu dohody. Pri plnení dohody treťou osobou (subdodávateľom) má poskytovateľ zodpovednosť, akoby plnil predmet dohody sám.

11.8 Pod vyššou mocou sa rozumejú okolnosti, ktoré nastanú po uzatvorení dohody ako výsledok nepredvídateľných a účastníkmi dohody neovplyvniteľných prekážok. V prípade, že takáto okolnosť bude brániť v plnení povinností podľa dohody poskytovateľovi alebo objednávateľovi, bude účastník dohody dotknutý vyššou mocou zbavený zodpovednosti za čiastočné alebo úplné nesplnenie záväzkov vyplývajúcich z tejto dohody primerane počas doby, po ktorú pôsobili tieto okolnosti.

11.9 Ak sa poskytovateľ v súvislosti s plnením povinností podľa dohody dostane do súdneho konania s treťou osobou, alebo by takéto súdne konanie hrozilo, bezodkladne o tom vyrozumie objednávateľa. Objednávateľ bude povinný na požiadanie poskytovateľa dať ihneď k dispozícii poskytovateľovi všetky potrebné informácie a podklady. Táto povinnosť vznikne príslušným vyrozumením. Uvedená povinnosť bude platiť recipročne aj pre poskytovateľa, 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 dohody.

11.10 Poskytovateľ 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 dohody. Ďalej je povinný bezodkladne oznámiť objednávateľovi, ak niektorý z veriteľov poskytovateľa podal proti nemu návrh na vyhlásenie konkurzu a návrh na povolenie reštrukturalizácie alebo vstup do likvidácie a jej ukončenie.

11.11 Účastníci dohody sa zaväzujú bezodkladne vzájomne sa informovať o konkrétnom podozrení na

korupciu pri rokovaniach o dohode, uzatváraní dohody alebo počas plnenia tejto dohody.

11.12 Účastníci dohody sa zaväzujú ihneď písomne oznámiť druhému účastníkovi dohody závažné skutočnosti, ktoré nastali po podpísaní dohody a súvisia s predmetom dohody.

11.13 Poskytovateľ vyhlasuje, že ku dňu podpísania tejto dohody má vyrovnané všetky záväzky voči objednávateľovi podľa zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov. Táto skutočnosť je podmienkou na uzatvorenie tejto dohody.

11.14 Poskytovateľ vyhlasuje a potvrdzuje, že v prípade, ak pri poskytovaní plnenia predmetu dohody vznikne dielo, ktoré je predmetom ochrany podľa zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov (ďalej aj len ako "autorské dielo"), jeho dodaním podľa tejto dohody sa objednávateľ stáva výhradným vykonávateľom majetkových práv autora k autorskému dielu, pričom sa na jeho postavenie a práva aplikuje primerane postavenie objednávateľa v zmysle § 91 autorského zákona, a to počas celej doby trvania autorských práv k autorskému dielu, ak z kogentných ustanovení právnych predpisov nevyplýva inak. V uvedenom rozsahu je poskytovateľ povinný strpieť výkon majetkových práv a sám ich nevykonávať. Rovnako platí, že poskytovateľ je povinný zabezpečiť splnenie povinností podľa predchádzajúcej vety tohto bodu vo vzťahu k akýmkoľvek tretím osobám (subdodávateľom), prostredníctvom ktorých vykoná autorské dielo podľa tejto dohody (ak bol na to oprávnený), ak z kogentných ustanovení právnych predpisov nevyplýva inak.

11.15 Poskytovateľ zároveň udeľuje objednávateľovi súhlas na vykonávanie akýchkoľvek a všetkých úprav alebo nadstavieb autorského diela, ako aj jeho spracovanie alebo zahrnutie do iného diela, ktoré sa tak môže stať súčasťou iného diela, a to bez povinnosti akejkoľvek osobitnej odplaty a bez potreby osobitného súhlasu poskytovateľa.

11.16 Poskytovateľ vyhlasuje a zaručuje sa, že vo vzťahu k autorskému dielu, jeho akýmkoľvek súčastiam, výsledkom jeho priebežnej aktualizácie, modernizácie a k jeho akýchkoľvek úpravám podľa tejto dohody, ktoré vznikli v priamej súvislosti s vykonaním autorského diela a vo vzťahu k všetkým a akýmkoľvek právam k nemu udeleným objednávateľovi podľa dohody:

a) vysporiadal alebo vysporiada na svoju zodpovednosť a náklady všetky nároky osôb, ktoré sa podieľali na tvorbe autorského diela (vrátane svojich zamestnancov a prípadných subdodávateľov), resp. predmetov autorského práva obsiahnutých v autorskom diele;

b) zabezpečí všetky potrebné súhlasy a oprávnenia od osôb, ktoré sa podieľali na tvorbe diela, resp. predmetov autorského práva obsiahnutých v autorskom diele, ktoré sa vyžadujú v zmysle autorského zákona a príslušných právnych predpisov;

c) je na základe dohody s autormi autorského diela jediným subjektom oprávneným na výkon majetkových práv k autorskému dielu a je oprávneným vykonávateľom všetkých a akýchkoľvek majetkových práv k predmetom autorského práva, ktoré sú obsiahnuté v autorskom diele;

d) získal predchádzajúci písomný súhlas s postúpením licencie v rozsahu podľa bodu 11.16 písmeno d) tejto dohody; uvedenú skutočnosť ním preukáže;

e) neexistuje žiadna skutočnosť, ktorá by bránila akýmkoľvek spôsobom alebo v akomkoľvek rozsahu poskytnutiu licencie objednávateľovi v rozsahu podľa bodu 11.16 článku dohody a použitiu autorského diela spôsobom predvídaným v tejto dohode alebo z tejto dohody vyplývajúcim a

f) vysporiadal všetky a akékoľvek peňažné a nepeňažné záväzky voči akejkoľvek a každej tretej osobe, týkajúce sa a/alebo spojené s autorským dielom.

11.17 Pre prípad, ak sa z akéhokoľvek dôvodu objednávateľ nestane vo vzťahu k autorskému dielu výhradným vykonávateľom majetkových práv podľa tohto článku dohody, poskytovateľ udeľuje objednávateľovi licenciu k autorskému dielu, a to od momentu odovzdania autorského diela objednávateľovi. Licencia sa udeľuje v nasledovnom rozsahu:

a) spôsob použitia – všetky známe formy použitia diela v čase uzatvorenia tejto dohody;

b) obdobie licencie – počas celej doby trvania výhradných majetkových práv k autorskému dielu podľa autorského zákona;

c) územie – bez územného obmedzenia;

d) objednávateľ je oprávnený udeliť tretej osobe sublicenciu v rozsahu udelenej licencie alebo túto licenciu alebo jej časť postúpiť na tretiu osobu; poskytovateľ týmto zároveň poskytuje objednávateľovi svoj výslovný a neodvolateľný súhlas na udelenie sublicencie tretej osobe, ako aj na postúpenie licencie alebo jej časti. Objednávateľ nie je súčasne povinný výhradnú licenciu použiť.

11.18 Poskytovateľ sa zaväzuje odškodniť objednávateľa v prípade, ak objednávateľovi bude zaviazaný uhradiť akejkoľvek tretej osobe akúkoľvek škodu, bezdôvodné obohatenie, náhradu, kompenzáciu, zmluvnú pokutu alebo inú sankciu, ktorej dôvod spočíval v nevysporiadaní autorských práv alebo práv súvisiacich s autorským právom obsiahnutých v autorskom diele, pričom objednávateľ tento sľub odškodnenia prijíma.

11.19 Poskytovateľ sa vyvaruje akýchkoľvek kontaktov, ktoré by mohli ohroziť jeho nezávislosť. Okrem toho, poskytovateľ je povinný prijať všetky nevyhnutné opatrenia s cieľom predísť akejkoľvek situácii, ktorá by mohla ohroziť nestranné a objektívne plnenie tejto dohody. Konflikt záujmov by mohol vzniknúť najmä v dôsledku ekonomických záujmov, politickej alebo národnej spriaznenosti, rodinných či citových väzieb alebo akýchkoľvek iných vzťahov alebo spoločných záujmov. Každý konflikt záujmov, ktorý vznikne počas plnenia tejto dohody, musí byť bezodkladne písomne oznámený objednávateľovi. V prípade konfliktu záujmov poskytovateľ okamžite prijme všetky opatrenia potrebné na jeho ukončenie. Objednávateľ si vyhradzuje právo overiť, či sú opatrenia uvedené v predchádzajúcom bode tohto článku dohody primerané, a v prípade potreby môže vyžadovať prijatie dodatočných opatrení v lehote, ktorú sám určí. Poskytovateľ zabezpečí, aby sa jeho zamestnanci a subdodávatelia nedostali do situácie, ktorá by mohla viesť ku konfliktu záujmov. Bez toho, aby bol dotknutý bod 11.17 tohto článku dohody, poskytovateľ okamžite a bez akéhokoľvek odškodnenia zo strany objednávateľa nahradí každého svojho zamestnanca a /alebo subdodávateľa, ktorý je takejto situácii vystavený.

11.20 Poskytovateľ vyhlasuje, že je spôsobilý uzatvoriť túto dohodu a riadne plniť záväzky z nej vyplývajúce a že sa oboznámil s podkladmi tvoriacimi zadávanú dokumentáciu, vrátane jej príloh, ktoré ustanovujú požiadavky na predmet plnenia tejto dohody.

11.21 Poskytovateľ vyhlasuje, že disponuje všetkými oprávneniami požadovanými príslušnými orgánmi a v zmysle príslušných právnych predpisov, ako aj kapacitami a odbornými znalosťami nevyhnutnými na riadnu a včasnú realizáciu predmetu tejto dohody.

11.22 Objednávateľ týmto vyhlasuje, že je orgánom verejnej moci zriadený v súlade s právnym poriadkom Slovenskej republiky, spĺňa všetky podmienky a požiadavky stanovené v tejto dohode, je oprávnený a spôsobilý uzatvoriť túto dohodu a riadne plniť záväzky v nej obsiahnuté.

11.23 Objednávateľ podpisom tejto dohody vyhlasuje, že na účely plnenia tejto dohody poskytovateľom má zabezpečené programové vybavenie a IT infraštruktúru, a to takým spôsobom, že plnenie povinností poskytovateľom bude objektívne možné a bude v súlade s dojednaniami tejto dohody vrátane jej príloh.

11.24 V prípade rozporu medzi ustanoveniami tejto dohody a dispozitívnymi ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, platia ustanovenia tejto dohody. V prípade rozporu medzi ustanoveniami tejto dohody a ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, ktoré je možné dohodou účastníkov dohody vylúčiť, platia ustanovenia tejto dohody a uvedené ustanovenia všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky sa považujú za výslovne vylúčené.

11.25 Objednávateľ vyhlasuje, že obsah tejto dohody je v súlade so všetkými predpismi upravujúcimi činnosť objednávateľa, najmä s predpismi týkajúcimi sa verejného obstarávania.

11.26 Poskytovateľ vyhlasuje a zaväzuje sa, že umožní objednávateľovi vykonať audit bezpečnosti Informačného systému na overenie miery dodržiavania bezpečnostných požiadaviek relevantných právnych predpisov a zmluvných požiadaviek.

11.27 Poskytovateľ vyhlasuje a zaväzuje sa, že prijme opatrenia na zabezpečenie nápravy zistení z auditu bezpečnosti Informačného systému.

11.28 Dohodu je možné meniť počas jej trvania bez nového verejného obstarávania v súlade s ustanovením § 18 zákona o verejnom obstarávaní. Zmena dohody musí byť písomná.

11.29 Poskytovateľ vyhlasuje, že ku dňu uzavretia tejto dohody je/nie je závislou osobou voči objednávateľovi v zmysle § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení 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 poskytovateľ povinný objednávateľovi písomne oznámiť a to do 5 dní odo dňa vzniku zmeny.

Čl. XII
Záverečné ustanovenia

12.1 Táto dohoda sa uzatvára na dobu určitú, a to na 12 mesiacov odo dňa jej účinnosti alebo do vyčerpania celkového finančného limitu, dohodnutého v čl. V bode 5.3 tejto dohody, podľa toho, ktorá skutočnosť nastane skôr. V prípade nevyčerpania celkového finančného limitu sú účastníci dohody oprávnení platnosť a účinnosť dohody predĺžiť maximálne o šesť (6) mesiacov alebo do vyčerpania finančného limitu, podľa toho, ktorá skutočnosť nastane skôr, a to formou písomného dodatku k dohode.

12.2 Táto dohoda 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. Poskytovateľ berie na vedomie povinnosť objednávateľa zverejniť túto dohodu ako aj jednotlivé objednávky a faktúry vyplývajúce z tejto dohody, vrátane jej príloh v plnom rozsahu.

12.3 Dohoda nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch účastníkov dohody a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.

12.4 Dohodu je možné meniť alebo dopĺňať iba formou písomných dodatkov, ktoré budú neoddeliteľnou súčasťou dohody, s výnimkou zmeny identifikačných údajov účastníkov dohody, zmeny experta, ktorá sa vykoná podľa čl. IV, bod 4.12 a zmeny subdodávateľa, ktorá sa uskutoční podľa čl. XI bodu 11.5 dohody. Dohodu je možné meniť len v prípade, ak zmeny a doplnenia nebudú v rozpore s ustanovením § 18 zákona o verejnom obstarávaní a európskou legislatívou.

12.5 Účastníci dohody sa v súlade s ustanovením § 262 ods. 1 Obchodného zákonníka dohodli, že záväzkový vzťah založený touto dohodou sa spravuje Obchodným zákonníkom. Vzťahy účastníkov dohody neupravené touto dohodou sa budú riadiť príslušnými ustanoveniami Obchodného zákonníka, zákona o verejnom obstarávaní a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky a európskou legislatívou.

12.6 Objednávateľ podpísaním tejto dohody akceptuje všetkých subdodávateľov poskytovateľa, čo však poskytovateľa nezbavuje zodpovednosti za kvalitu plnenia dohody podľa všeobecne záväzných právnych predpisov a tejto dohody.

12.7 Účastníci dohody sa zaväzujú, že všetky spory, vyplývajúce z tejto dohody, budú riešiť predovšetkým formou dohody. Prípadné spory, o ktorých sa účastníci dohody nedohodnú, budú sa riadiť právnym poriadkom Slovenskej republiky. Prípadné spory, o ktorých sa účastníci dohody nedohodnú, budú postúpené na rozhodnutie vecne a miestne príslušnému súdu.

12.8 Ak niektoré ustanovenia tejto dohody stratili platnosť alebo sú platné len sčasti alebo neskôr stratia platnosť, nie je tým dotknutá platnosť ostatných ustanovení. Na miesto neplatných ustanovení sa použije úprava, ktorá sa čo najviac približuje zmyslu a účelu tejto dohody.

12.9 Neoddeliteľnou súčasťou tejto dohody sú:

príloha č. 1 – Špecifikácia predmetu dohody
príloha č. 2 – Predpokladané množstvo a cena
príloha č. 3 – Zoznam subdodávateľov
príloha č. 4 – Zápis o zmene prílohy č. X „Zoznam XX“

príloha č. 5 – Zoznam expertov
príloha č. 6 – Vzor požiadavky pre hlásenie chýb
príloha č. 7 – Vzor protokolu o paušálnej podpore
príloha č. 8 – Vzor požiadavky na zmeny/úpravy IS FRSP
príloha č. 9 – Vzor akceptačného protokolu
príloha č. 10 – Vzor požiadavky na školenie
príloha č. 11 – Vzor protokolu o vykonanom školení
príloha č. 12 – Rozpis dodávky/zmeny
príloha č. 13 – Sprostredkovateľská zmluva
príloha č. 14 – Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

12.10 Dohoda je vyhotovená v štyroch rovnopisoch, po dva rovnopisy pre každého účastníka dohody.

12.11 Účastníci dohody vyhlasujú, že obsah dohody je prejavom ich slobodnej vôle, dohoda nebola uzatvorená v tiesni a ani za zvlášť nevýhodných podmienok. Súčasne vyhlasujú, že si ju riadne a dôsledne prečítali, jej obsahu a právnym účinkom porozumeli a na znak súhlasu ju vlastnoručne podpísali.

V Bratislave, dňa.....

Za poskytovateľa:

_____

Ing. Martin Peluha
Konateľ
DXC Technology Slovakia s.r.o.

V Bratislave, dňa .....

Za objednávateľa:

_____

Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

Príloha č. 1 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

ŠPECIFIKÁCIA PREDMETU DOHODY

A. Charakteristika systému

Informačný systém Finančného riadenia Sociálnej poisťovne (ďalej len „IS FRSP“) je založený na jednoducho ovládateľnom rozhraní a je vybudovaný na báze produktu SAP. Používa sa ako hlavná firemná ERP (Enterprise Resource Planning) aplikácia, ktorá umožňuje využitie ďalších rozhraní. Je komplexným a univerzálnym riadiacim a administratívnym nástrojom, ktorý využívajú manažéri a ostatní zamestnanci. Riešenie poskytuje všetky bežné administratívne funkcie, ktoré umožňujú upravovať a zálohovať dáta, parametrizovať oprávnenia a prístupy a pristupovať k údajom z produktov tretích strán. Skladá sa z jednotlivých vzájomne integrovaných modulov, ktoré rozširujú schopnosti riešenia IS FRSP, zjednodušujú podnikové procesy a ponúkajú viaceré administratívne funkcie.

Objednávateľ má udelenú výhradnú licenciu na zákaznícke úpravy a zdrojové kódy k zákazníckym úpravám implementovaným od 01.01.2016. Na zákaznícke úpravy a súvisiace zdrojové kódy z predchádzajúcich období, t. j. do 31.12.2015, má objednávateľ udelenú nevýhradnú licenciu na základe Verejnej realizačnej zmluvy o dielo č. 8 zo dňa 3. marca 2008, v znení jej dodatkov č. 1 až 6 a dodatkov č. 8 až 13 poskytovanej spoločnosťou CSC Computer Sciences spol. s r. o. (po zmene obchodného mena DXC Technology Slovakia s. r. o.). Objednávateľ disponuje so zdrojovými kódmi na všetky moduly tvoriace IS FRSP v zmysle vyššie uvedeného a môže s nimi nakladať v súlade s ustanoveniami zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov.

Technická špecifikácia riešenia

IS FRSP je vybudovaný na báze produktu SAP ECC 6.0 s Enhancement Package 3 pracujúci nad databázovým serverom Oracle Database 19.20. Softvér SAP systémov má 64-bitovú architektúru a SAP systémy sú inštalované ako UNICODE. Sú použité nasledujúce softvérové komponenty:

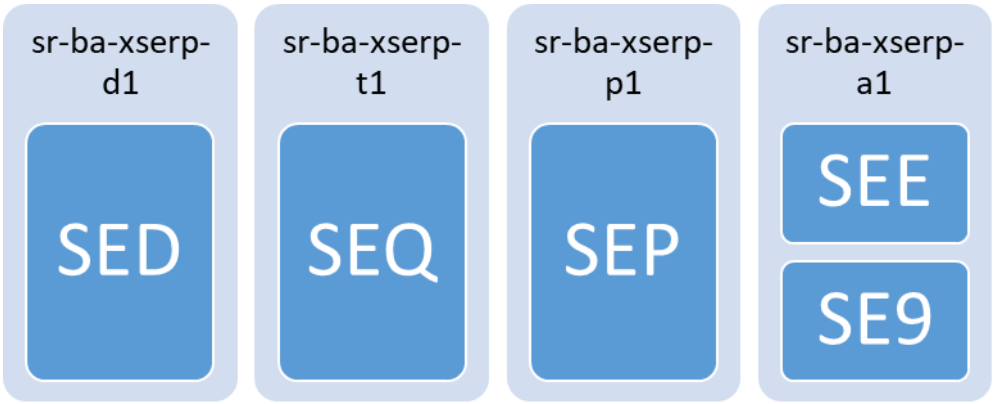
- IBM AIX 7.2, od 12/2023: 7.3 — 64-bitový operačný systém
- Oracle Database 19.20.0.0.0 — databázový server
- SAP Kernel 7.22 EXT 64-bit UNICODE — platforma aplikačného servera
- SAP ECC 6.0 s EhP3, *od 12/2023:* EHP8 — aplikácia

Popis technickej infraštruktúry IS FRSP

Aplikačná vrstva

IS FRSP pozostáva z troch samostatných prostredí – vývojovo-customizačné (**SED**), testovacie (**SEQ**) a produkčné (**SEP**) prostredie. Každé prostredie je realizované samostatným SAP systémom s vlastným databázovým serverom inštalovaným vždy na samostatnom IBM LPARe.

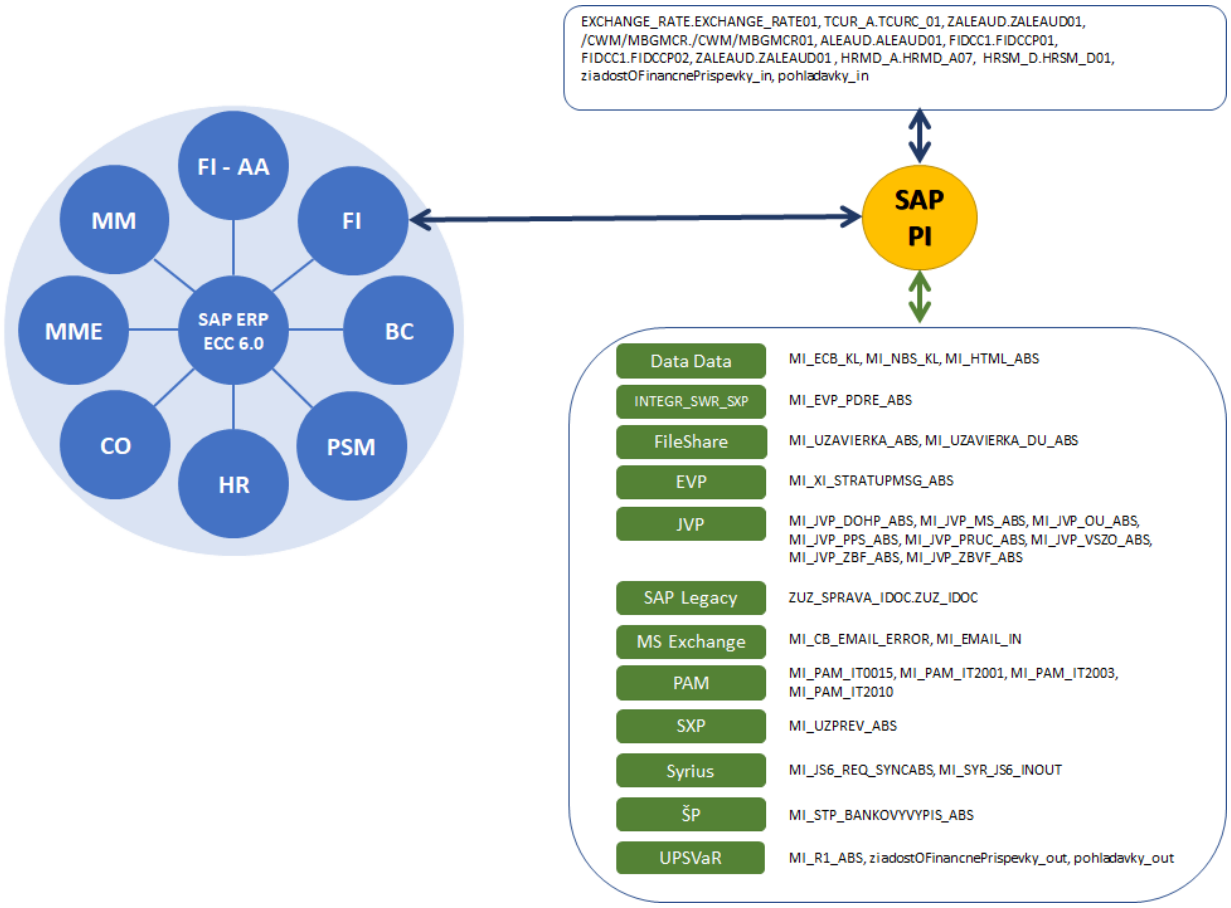
Okrem toho existujú dva archívne systémy – SEE so stavom produkčného systému pred eurokonverziou, teda v mene Slovenská koruna a SE9 po eurokonverzii, so stavom produkčného systému pred implementáciou aplikačných modulov (SAP PSM, SAP FI-AA, SAP-MM/MME, SAP CO) v roku 2009. Oba archívne systémy sú inštalované na spoločnom LPARe.



Databázová vrstva

Jeden SAP systém je inštalovaný na jednej inštancii operačného systému (t. j. na jednom LPARe). Nachádza sa tu teda databázový server Oracle a aj SAP softvérové komponenty (inštancia centrálnych služieb a aplikačný server ABAP).

Architektúra IS FRSP



Moduly

- **SAP-FI:** Finančné účtovníctvo - modul pre podporu procesov účtovania a vedenia účtov v organizácii,
- **SAP-CO:** Controlling - modul pre riadenie nákladov a výnosov a vnútropodnikové účtovníctvo,

- **SAP-PSM:** Rozpočtovníctvo - modul obsahujúci nástroje pokrývajúce celý životný cyklus rozpočtového hospodárenia,
- **SAP-FI-AA:** Majetok - modul umožňujúci viesť komplexnú evidenciu o stave majetku a pokrývajúci procesy životného cyklu majetku,
- **SAP-MM:** Materiálové hospodárstvo a obstarávanie - modul, ktorý poskytuje nástroje pokrývajúce procesy obstarania majetku a materiálu, jeho skladovania a spotreby,
- **SAP-MME:** Rozšírenie modulu SAP MM - Odberateľská fakturácia,
- **SAP-HR:** Personalistika, organizačný manažment a mzdy – modul, ktorý pokrýva procesy riadenia ľudských zdrojov a mzdovú agendu,
- **SAP-BC:** Báza systému SAP,
- **SAP Netweaver PI:** Integračná platforma zabezpečujúca komunikáciu s agendovými (produkčnými) IS Sociálnej poisťovne.

Rozhrania (Interfaces)

- **Vstupné rozhrania – rozhrania, ktorými sa prenášajú dáta do APV SAP**

Rozhranie	Popis	Technológia
Banka	Bankové rozhranie	File transfer SSH
IS NPaLPČ	Online prenos údajov o ND na dennej báze	File transfer SSH
IS JVP	Prenos agregovaných údajov na mesačnej báze	File transfer SSH
IS DAÚP	Prenos agregovaných údajov na mesačnej báze	File transfer SSH
IS PvNGP	Prenos agregovaných údajov na mesačnej báze	File transfer SSH
MPSVaR	Prenos dát – Kurzarbeit	Webservice

- **Výstupné rozhrania – rozhrania, ktorými sa prenášajú dáta smerom von z APV SAP**

Rozhranie	Popis	Technológia
Active	Údaje o zamestnancoch pre MS Active Directory	File transfer SSH
Dovolenky	Prenos stavu dovoleniek zamestnancov do iCard	File transfer SSH
Dochádzka	Údaje o zamestnancoch pre iCard	SAP RFC
Prenos W	Publikovanie objednávok a faktúr na www	File transfer SSH
VRP	Vrátené platby	File transfer SSH
MPSVaR	Prenos odpovede o úspešnom prijatí žiadosti	Webservice

Zákaznícke úpravy

Okrem štandardných transakcií, reportov a procesov, obsahuje IS FRSP veľké množstvo tzv. zákazníckych úprav, ktoré rozširujú funkcionalitu o „na mieru ušité“ riešenia.

Modul FI

- Automatizované preúčtovanie zostatkov účtov pri uzávierkových prácach,
- Prehľad máp pre automatizované preúčtovanie zostatkov účtov pri uzávierkových prácach,
- Spracovanie elektronického bankového výpisu, denné rutinné spracovanie,
- Zobrazenie spracovaného bankového výpisu,
- Nastavenia pre spracovanie elektronického bankového výpisu pre transakciu ZBNK1,
- Výmaz dát bankového výpisu v prípade chyby pri spracovaní,
- Generovanie výplaty miezd za pobočky,
- Spracovanie a zaúčtovanie príjmov a výdajov v pokladni, členenie podľa pobočiek - Pokladňa správneho fondu ústredia – nastavenie možnosti „len fond 132“,
- Pokladňa základných fondov – nastavenie možnosti „len fond 122 a 123“,
- Spracovanie a zaúčtovanie príjmov a výdajov v pokladni, členenie podľa pobočiek,
- Servisný program pre ukončenie práce s pokladňou,
- Zobrazenie dokladov v pokladni,
- Customizing pre nastavenie pokladní: texty, hlavičky, stavy dokladu, polia dokumentu, účtovacie kľúče, atď.,
- Tlač účtovného dokladu zaúčtovaného do 31.12.2012,
- Tlač účtovného dokladu zaúčtovaného od 01.01.2013 do 29.02.2016,
- Tlač účtovného dokladu zaúčtovaného od 01.01.2013 do 31.01.2014,
- Tlač účtovného dokladu zaúčtovaného od 01.01.2013 do 29.02.2016 - hromadná tlač,
- Tlač účtovného dokladu zaúčtovaného od 01.01.2013 do 31.01.2014 - hromadná tlač,
- Tlač účtovného dokladu pre odpisy majetku zaúčtovaného do 02.29.2016,
- Tlač účtovného dokladu pre odpisy majetku zaúčtovaného do 01.03.2016,
- Tlač účtovného dokladu zaúčtovaného od 01.02.2014 do 29.02.2016,
- Tlač účtovného dokladu zaúčtovaného od 01.02.2014 do 29.02.2016 - hromadná tlač,
- Tlač účtovného dokladu zaúčtovaného od 01.03.2016,
- Tlač účtovného dokladu zaúčtovaného od 01.03.2016 - hromadná tlač,
- Tlač likvidačnej doložky ku faktúre,
- Tlač dokladu FI s hlavičkou,
- Modifikácia štandardnej transakcie FBL1N pre pobočky a fondy,
- Modifikácia štandardnej transakcie FBL3N pre pobočky a fondy,

- Modifikácia štandardnej transakcie FBL5N pre pobočky a fondy,
- Modifikácia transakcie FD10N - rozšírenie výberu o pracovný úsek a fond,
- Zaúčtovanie mzdových druhov do FI,
- Customizing pre automatizované účtovanie na fondoch,
- Modifikácia transakcie FS10N - rozšírenie výberu o pracovný úsek a fond,
- Zobrazenie dokladov zaúčtovaných po závierke,
- Modifikácia transakcie FK10N - rozšírenie výberu o pracovný úsek a fond,
- Zobrazenie obratov a zostatkov na účtoch hlavnej knihy,
- Doplnenie účtov dodávateľov vo formáte IBAN do tabuľky TIBAN,
- Tlač zoznamu došlých faktúr podľa dodávateľov,
- Tlač prehľadu nákladov podľa pobočiek a nákladových druhov,
- Nastavenie otvorenia účtovných období za pobočky (rozšírenie štandardu o pracovné úseky),
- Program pre výber faktúr pre platbu, zablokovanie, odblokovanie faktúr pre platbu,
- Tlač reportu Súvaha vo formáte Word,
- Customizing súvahy pre tlač,
- Export súvahy a výsledovky do súboru vo formáte CSV,
- Nastavenie času spustenia a cesty na server pre zverejňované dokumenty,
- Rozhranie pre spúšťanie výkazov SOCP,
- Customizing výsledovky pre tlač,
- Projekt SEPA štandardy – nastavenie a úprava rozhrania bankové výpisy > SAP FI,
- Zmena číselníkov bankových účtov na formáty IBAN,
- Úprava xml štruktúr pre SAP,
- Nastavenia a rozšírenie funkcionality platieb a spracovania bankového výpisu – projekt EESSI,
- Úprava štandardnej funkcionality platobných príkazov pre doklady storna (transakcia F110),
- Nastavenie blokácie účtovania dokladov na deň pracovného pokoja,
- Úprava štandardnej transakcie pokladne správneho fondu,
- Možnosť spracovania viacerým užívateľom,
- Predĺženie časového pásma na opravu dokladov,
- Dopĺňanie mena zodpovedného zamestnanca do formulárov dokladov pokladne,
- Program pre čítanie a filtrovanie kreditných položiek výpisov ÚDP a ÚOP (transakcia ZFIVRP1),
- Program na automatické napĺňanie výkazov SP: ročné výkazy, štatistiky, pohľadávky a výkazy FIN3-04, FIN4-04 a FIN5-04. Vypracovanie užívateľskej dokumentácie k napĺňaniu (výkazy ZVYKSTAT, ZVYKSTAT2, ZKONTAB, ZKONTAB2, ZVYKROC, FIN3-04, FIN4-04 a FIN5-04),
- Novela zákona č. 461/2003 Z. z. o sociálnom poistení: obecní policajti a baníci: úprava účtovných a finančných výkazov, štatistických a úprava vstupného rozhrania – rozhrania, ktorými sa prenášajú dáta do APV SAP z IS JVP (transakcia ZVYKAZY), súvaha, FIN 2-04 a ďalšie výkazy podľa

požiadavky MF SR v súvislosti so štatistickým úradom; ZVYKSTAT, ZVYKSTAT2, ZKONTAB, ZKONTAB2,

- Novela zákona č. 461/2003 Z. z. o sociálnom poistení s preloženou účinnosťou na 1.3.2022; zabezpečenie prepojenia primárnych IS (JVP) do SAP FI prostredníctvom integračnej platformy PI, Vstupné rozhrania – rozhrania, ktorými sa prenášajú dáta do APV SAP z IS JVP pre základný fond poistenia v nezamestnanosti a „výplata dávky Kurzarbeit" – prenos účtovných dát (žiadosti = vznik záväzku voči poskytovateľovi podpory) web servisom do účtovníctva bez zásahu zamestnanca SP a následné spracovanie platobného návrhu pre platbu na zabezpečenie postúpenia finančných prostriedkov poskytovateľom podpory,
- Komunikačné rozhranie – webservice Kurzarbeit v zmysle zákona č. 215/2021 Z. z. zo dňa 4. mája 2021 o podpore v čase skrátenej práce a o zmene a doplnení niektorých zákonov:

  - Predpis záväzku Kurzarbeit a zaslanie platby pre pobočky ÚPSVaR,

  - Vznik pohľadávky,
- Zámenná zmluva - výmena budov a pozemkov medzi SP a MOSR – crossmodulové neštandardné riešenie pre účtovný postup a použitie rozpočtových položiek v moduloch AA, FI a PSM.

Modul FI-AA

- Hromadné zaradenie drobného majetku (účtovanie),
- Report zoznam nezaradeného majetku,
- Údržba zákazníckych číselníkov v module FI-AA, ktoré sú použité v rozšírených Z* poliach v kartách majetku pre jednotlivé triedy majetku,
- Údržba zákazníckeho číselníka miestností,
- Hromadné zaradenie dlhodobého majetku pre pobočky SP (účtovania),
- Karta majetku + tlačový výstup (vybraný zoznam atribútov z kmeňového záznamu karty majetku),
- Miestny zoznam + tlačový výstup (zoznam majetku),
- Osobná karta zamestnanca + tlačový výstup (evidencia pridelenia, odobratia majetku zamestnancovi),
- Prevody majetku v rámci jednotlivých pobočiek SP (účtovanie),
- Hromadné vyradenie dlhodobého/drobného majetku (účtovanie) + tlačový výstup,
- Storno vyradenia dlhodobého/drobného majetku,
- Zaradenie dlhodobého majetku - tlačový výstup,
- Nadstavba FI-AA – modul FAIN – inventarizácia majetku.

Modul CO

- Kmeňové dáta – nákladové stredisko (založené na najnižšej organizačnej úrovni), nákladový druh, vnútropodnikové zákazky,
- Hromadné založenie nákladových stredísk podľa ziskových stredísk,
- Editácia/priradenie pracovných úsekov podľa oblastí hierarchie,

- Zmena ziskových a nákladových stredísk a priradenie podľa oblastí hierarchie po zmene organizačnej štruktúry s možnosťou prepisu existujúceho nákladového strediska, nastavenia dátumu zmeny,
- Report porovnanie vybraných účtov za CO/PSM,
- Kopírovanie plánovania,
- Účtovníctvo vnútropodnikových zákaziek - Založenie, zmena a zobrazenie vnútropodnikovej zákazky. Rozdelenie zákaziek na investičné, prevádzkové, ostatné,
- Plánovanie - jednotlivé verzie, zadávanie plánovaných hodnôt pobočkou, ústredím, s možnosťou nastavenia profilu plánovača, možnosť zadávania potrebných zmien, možnosť automatizovaného prenosu plánovaných mzdových nákladov a poistného do prostredia PSM z Excelu,
- Prenos plánovaných dát do verzie PSM,
- Kopírovanie plánovaných dát medzi jednotlivé verzie,
- Výkazy spracované na podmienky Sociálnej poisťovne,
- Integrácia s modulom MM,
- Integrácia s modulom FI-AA,
- Integrácia s modulom HR,
- Integrácia s modulom PSM.

Modul PSM

- Výkazníctvo – príjmy a výdavky v sledovaní za schválený rozpočet, rozpočet po zmenách, očakávaná skutočnosť a skutočné čerpanie k danému obdobiu, možnosť automatizovaného vyplnenia výkazu, prenos zo súborov .xlsx,
- Výkazníctvo - Finančný výkaz o príjmoch, výdavkoch a finančných operáciách FIN 1-12,
- Opatrenie MF SR č. MF/017353/2017-352 z 19. decembra 2017, ktorým sa ustanovuje usporiadanie, obsahové vymedzenie, spôsob, termín a miesto predkladania informácií z účtovníctva a údajov potrebných na účely hodnotenia plnenia rozpočtu verejnej správy, v znení neskorších predpisov (transakcia J6GFMP),
- Základný proces rozpočtovania v podmienkach Sociálnej poisťovne (návrh rozpočtu, rozpis rozpočtu, úprava rozpočtu rozpočtové opatrenia),
- Rozpočet – rozdelenie na fondy a to základné fondy a správny fond, následne podrobnejšie rozdelenie fondov,
- Kmeňové dáta – finančné strediská, finančné položky, ktoré sú spojením rozpočtových položiek a účtov hlavnej knihy, ich hierarchia, funkčná oblasť, fondy, programy,
- Štruktúrovaný plán rozpočtu – kontrola pre elimináciu nesprávnych priradení,
- Čerpanie rozpočtu, kontrola disponibility,
- Otváranie období pre rozpočet,
- Programy rozpočtu – kapitálové výdavky, ich sledovanie v aktuálnom roku,
- Komplexné rozpočtové operácie (kopírovanie verzií, prenos z CO),
- Návrh rozpočtu – verzie rozpočtu, profil plánovača, zmena plánovacích dát, úpravy layoutov plánovania, kopírovanie verzií, výmaz dát, prenos z controlingu,

- Zostavovanie a úprava rozpočtu tzv. rozpočtové opatrenia – zadávanie dokladov rozpočtu, zobrazenie dokladov rozpočtu, storno, nastaviť,
- Integrácie s nákupom,
- Integrácia s HR,
- Integrácia s FI,
- Integrácia s FI-AA a CO,
- Uzávierkové operácie (proces mesačnej a koncoročnej uzávierky, prevodu obliga z nákupných objednávok),
- Zdaňovaná činnosť,
- EÚ projekty a riadenie projektov,
- Výkazníctvo – vytvorenie výkazov podľa potreby Sociálnej poisťovne okrem štandardných s možnosťou výberu podľa kritérií (finančná položka, finančné stredisko, blok rozpočtu....),
- Rozpočet a úprava rozpočtu jednotlivých základných fondov (vrátane základného fondu príspevkov na starobné dôchodkové sporenie), rezervného fondu solidarity a osobitného fondu, kmeňové dáta a štruktúrovaný plán rozpočtu, plánovanie a rozpis rozpočtu ZF a ostatných fondov – podľa mesiacov roka za ústredie a jednotlivé pobočky SP, sumárne celkom za SP,
- Kmeňové dáta (finančná položka, finančné stredisko, fond, funkčná oblasť), návrh rozpočtu základných fondov, zadávanie očakávanej skutočnosti (pre potreby výkazu FIN 1-12), zmeny v návrhu rozpočtu, zadanie rozpisu rozpočtu,
- Rozpočtovanie a rozpis na mesiace ZFNP za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy a výdavky),
- Rozpočtovanie a rozpis na mesiace ZFSP za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy),
- Rozpočtovanie a rozpis na mesiace ZFSP za ústredie a sumárne SP (výdavky),
- Rozpočtovanie a rozpis na mesiace ZFIP za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy),
- Rozpočtovanie a rozpis na mesiace ZFIP za ústredie a sumárne SP (výdavky),
- Rozpočtovanie a rozpis na mesiace ZFUP za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy a výdavky),
- Rozpočtovanie a rozpis na mesiace ZFGP za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy a výdavky),
- Rozpočtovanie a rozpis na mesiace ZFPvN za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy a výdavky),
- Rozpočtovanie a rozpis na mesiace RFS za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy),
- Rozpočtovanie a rozpis na mesiace OF za ústredie, jednotlivé pobočky SP a sumárne SP (príjmy a výdavky),
- PSM výkazy ZF – ústredie, pobočky (príjmy a výdavky) k obdobiu,
- Základný proces rozpočtovania v podmienkach Sociálnej poisťovne - návrh rozpočtu, rozpis rozpočtu, úprava rozpočtu - rozpočtové opatrenia – rozdelenie na fondy a to základné fondy a správny fond, následne podrobnejšie rozdelenie fondov,
- Nástroj na vyplnenie poľa "USERDIM"=pole zákazníka využívané na porovnanie stavu čerpania rozpočtu voči stavom na bankovom účte,

- Nástroj na porovnanie stavu čerpania rozpočtu voči stavom na bankovom účte - sumárny pohľad,
- Nástroj na porovnanie stavu čerpania rozpočtu voči stavom na bankovom účte,
- Otváranie povolených období rozpočtovania na úrovni finančného strediska, verzie rozpočtu a fondu,
- Nástroj na identifikovanie pohybov FI, ktoré nie sú korektne priradené v rámci modulu PSM,
- Nástroj na porovnanie stavu čerpania rozpočtu voči stavom na bankovom účte - identifikovanie dokladov.

Modul MM/MME

- Údržba CPV kódov,
- Report zoznam CPV kódov,
- Report zostavy vývoja objednávky,
- Uvoľnenie (schválenie) a odschválenie objednávky – jednotlivé úrovne,
- Hromadné vytvorenie tlačového výstupu objednávky,
- Hromadná zmena objednávky - Konečná dodávka/Zúčtovanie,
- Údržba povolených kombinácií objektov priradenia účtu v objednávke,
- Kontrola statusu spracovania objednávky,
- Report prehľad kmeňových záznamov materiálu s výberom označenia na výmaz,
- Hromadný výmaz tlačových výstupov objednávky,
- Organizačná štruktúra skupín nákupu (priradenie skupín nákupu po zmenách v org. štruktúre),
- Zobrazenie zmien organizačnej štruktúry,
- Údržba schvaľovacích úrovní objednávok podľa hodnoty a org. štruktúry – zabezpečená finančná kontrola v IS,
- Report zostava vývoja objednávky,
- Kontrola status blokovania faktúry,
- Report prehľad položiek objednávky,
- Tlač objednávky,
- Tlač požiadavky na objednávku,
- Report zoznam objednávok pre tlač,
- Zmena štandardnej funkcionality v transakciách MIR7 na MIRO – vytvorené zostavy „simulácia dokladu“. Doplnenie stĺpca FOND a PRACOVNÝ ÚSEK. Zapracovanie tlače simulácie dokladu,
- Fakturačné doklady – MIR 7 – predbežné obstaranie vstupnej faktúry a ZDOLOŽKA – likvidačná doložka k faktúre,
- Report, kontrola finančného čerpania kontraktu.

Modul HR

- Prístupová transakcia pre query zostavy - slúži len pre prístup k infosade,

- Rekapitulácia mzdových prostriedkov pre správny fond s výpisom vybratých mzdových zložiek a období, za ktoré bol zamestnanec aktívny – tak, ako sú nastavené t. j.:
  - rekapitulácia mzdových druhov zvislá (detailne na zamestnanca, podľa jednotlivých pobočiek, ústredia a celej Sociálnej poisťovne),
  - rekapitulácia mzdových druhov vodorovná,
  - evidenčné stavy pracovníkov (fyzický, priemerný prepočítaný, úväzky...),
  - štvrťročný výkaz o práci „Práca 2-04“,
  - Odmena – vytvorenie návrhu odmien,
- Nástroj pre konzultanta na výmaz výsledkov zúčtovania,
- Šablóna pre dohodu o zmene pracovnej zmluvy,
- Exportný súbor pre zostatky dovoleniek na mesačnej báze exportovaný do dochádzkového systému,
- Šablóna pre nahlásenie zmien v kmeňových údajoch zamestnancov,
- Exportný súbor kmeňových dát zamestnanca, na dennej báze exportovaný do dochádzkového systému,
- Nástroj pre konzultanta na update infotypu 0003,
- Upravená verzia štandardnej mincovky,
- Elektronické posielanie výplatných pások,
- Formulár pre výšku čistého príjmu,
- Export kmeňových údajov zamestnanca nastavaný ako opakovaný job pre Act Dir,
- Export kmeňových údajov zamestnanca nastavaný ako opakovaný job pre Act Dir – pre vystúpených zamestnancov,
- Šablóna pre nahlásenie zmien v kmeňových údajoch zamestnancov,
- Aktualizácia infotypu 0003 na požadovaný dátum,
- Tlač štítkov na pracovno-právne dokumenty,
- Hromadné spustenie valorizácie miezd,
- Reporty spoločného riešenia pre tlač mzdových listov so zoznamom vytlačených objektov, ktoré sa používa pri hromadnej tlači mzdových listov,
- Riešenie pre import dát do IT0014, 0015, 2010, používa mzdové odd. pre hromadný import dát za zamestnancov,
- Zákaznícka rekapitulácia mzdových druhov s možnosťou výberu období, mzdových druhov a ich vlastností, kmeňových dát zamestnanca a ich vzájomnej kombinácie,
- Aktualizácia – zasielanie aktualizačných AOP balíkov,
- Elektronická distribúcia dokumentov a aktualizácia vzorových formulárov vydaných Finančnou správou SR,
- Prenos dát z Organizačného manažmentu do Personalistiky – tvorba mapy (zoznamu dát), ktorá slúži na prenos dát (aktuálnych ISCO-08 kódov) z organizačného manažmentu do personalistiky.

Legislatíva a bezpečnostné štandardy

IS FRSP garantuje súlad s platnou legislatívou v rozsahu na dodané moduly a funkcionalitu. IS FRSP podporuje platnú legislatívu a štandardy podľa nasledovných právnych predpisov:

- Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov,
- Zákon 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov,
- Zákon č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Metodické usmernenie Ministerstva financií Slovenskej republiky (MF SR) k č. MF/010175/2004-42 zo dňa 8. decembra 2004 a vysvetlivky k ekonomickej klasifikácii rozpočtovej klasifikácie v znení Dodatkov č. 1 až 17 uverejnených vo FS,
- Funkčná klasifikácia v zmysle vyhlášky Štatistického úradu Slovenskej republiky č. 257/2014 Z. z., ktorou sa vydáva štatistická klasifikácia výdavkov verejnej správy (SK COFOG),
- Zákon č. 291/2002 Z. z. o Štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov + všeobecné podmienky, výnosy a vyhlášky Štátnej pokladnice,
- Zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov,
- Opatrenie Ministerstva financií Slovenskej republiky z 30. marca 2020 č. MF/007222/2020-74, ktorým sa mení a dopĺňa opatrenie Ministerstva financií Slovenskej republiky zo 14. decembra 2005 č. MF/26940/2005-74, ktorým sa ustanovujú podrobnosti o usporiadaní, označovaní a obsahovom vymedzení položiek účtovnej závierky pre Sociálnu poisťovňu v znení neskorších predpisov,
- Opatrenie Ministerstva financií Slovenskej republiky z 26. februára 2020 č. MF/007223/2020-74, ktorým sa mení a dopĺňa opatrenie Ministerstva financií Slovenskej republiky z 30. novembra 2005 č. MF/24035/2005-74, ktorým sa ustanovujú podrobnosti o postupoch účtovania a účtovej osnove pre Sociálnu poisťovňu v znení neskorších predpisov,
- Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov,
- Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov,
- Zákon č. 663/2007 Z. z. o minimálnej mzde v znení neskorších predpisov,
- Každoročné nariadenie vlády o minimálnej mzde v znení neskorších predpisov,
- Zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení zákona č. 90/2002 Z. z. o poisťovníctve a o zmene a doplnení zákonov v znení neskorších predpisov,
- Zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení zákonov v znení neskorších predpisov,
- Zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov,
- Zákon č. 553/2003 Z. z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 160/2015 Z. z. Civilný sporový poriadok v znení neskorších predpisov,
- Zákon č. 161/2015 Z. z. Civilný mimosporový poriadok v znení neskorších predpisov,
- Zákon č. 162/2015 Z. z. Správny súdny poriadok v znení neskorších predpisov,
- Zákon č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok), a o zmene a doplnení ďalších zákonov v znení neskorších predpisov,

- Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Nariadenie vlády SR č. 268/2006 Z. z. o rozsahu zrážok zo mzdy pri výkone rozhodnutia v znení neskorších predpisov,
- Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov,
- Zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 2/1991 Zb. o kolektívnom vyjednávaní v znení neskorších predpisov,
- Zákon č. 176/2004 Z. z. o nakladaní s majetkom verejnoprávnych inštitúcií a o zmene zákona Národnej rady Slovenskej republiky č. 259/1993 Z. z. o Slovenskej lesníckej komore v znení zákona č. 464/2002 Z. z. v znení neskorších predpisov,
- Interné predpisy objednávateľa (napr. Kolektívna zmluva a pod.),
- Novela č. 221/2019 Z. z. ktorou sa mení a dopĺňa zákon č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii). V nadväznosti na to, s účinnosťou od 1.12.2019 sa dopĺňa zákon 595/2003 Z. z. o dani z príjmov v § 37 ods. 3. Potvrdenie o návšteve školy a potvrdenie príslušného úradu o poberaní prídavku na vyživované dieťa sa nepredkladá zamestnávateľovi podľa osobitného predpisu (§ 1 ods. 2 zákona č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov a zákon č. 55/2017 Z. z. v znení neskorších predpisov),
- Novela zákona č. 461/2003 Z. z. o sociálnom poistení, ktorá ukladá zamestnávateľovi povinnosť uvádzať a identifikovať zamestnanca prostredníctvom identifikačného čísla právneho vzťahu,
- Opatrenie MF SR z 19. januára 2022 č. MF/004791/2022-313, ktorým sa mení opatrenie MF SR z 19. decembra 2017 č. MF/017353/2017-352, ktorým sa ustanovuje usporiadanie, obsahové vymedzenie, spôsob, termín a miesto predkladania informácií z účtovníctva a údajov potrebných na účely hodnotenia plnenia rozpočtu verejnej správy v znení opatrenia z 22. februára 2021 č. MF/005583/2021-31,
- Metodické usmernenie Ministerstva financií Slovenskej republiky č. MF/005774/2023-31 k postupu pri aplikácii § 2 až 7 opatrenia Ministerstva financií Slovenskej republiky z 19. decembra 2017 č. MF/017353/2017-352, ktorým sa ustanovuje usporiadanie, obsahové vymedzenie, spôsob, termín a miesto predkladania informácií z účtovníctva a údajov potrebných na účely hodnotenia plnenia rozpočtu verejnej správy v znení opatrenia MF SR č. MF/005583/2021-31 a v znení opatrenia MF SR č. MF/004791/2022-31,
- Príručka Ministerstva financií slovenskej republiky pre subjekt verejnej správy k obsahovej náplni finančných výkazov (FIN),
- Zákon č. 215/2021 Z. z. zo dňa 4. mája 2021 o podpore v čase skrátenej práce a o zmene a doplnení niektorých zákonov,
- Zákon č. 211/2002 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií).

B. Opis predmetu dohody

Predmetom dohody je záväzok poskytovateľa poskytovať služby pre IS FRSP podľa jeho charakteristiky uvedenej v bode A. v nasledovnom rozsahu:

a) poskytovanie služieb technickej podpory IS FRSP,

b) poskytovanie služieb rozvoja IS FRSP,

c) poskytovanie školení v súvislosti s používaním IS FRSP.

Požadovaný rozsah poskytovaných služieb je uvedený v bodoch nižšie.

a) Poskytovanie služieb technickej podpory IS FRSP

Služby podpory prevádzky

- Podpora pri upgrade a nasadzovaní patchov DB ORACLE do technologického prostredia IS FRSP,
- Riešenie problémov technickej infraštruktúry,
- Kontrola a diagnostika jednotlivých prostredí,
- Kontrola a prípadná úprava rozhraní,
- Kontrola a diagnostika databáz,
- Podpora pri obnove po havarijných situáciách,
- Riešenie chybových stavov (vecnej, technickej a užívateľskej povahy),
- Súčinnosť pri riešení problémov podporovaného IS (pomoc pri analýze problémov, predkladanie návrhov a doporučení pre možné riešenia),
- Udržiavanie IS ako aj všetkých komponentov dodávaného riešenia na aktuálnych a podporovaných verziách,
- Udržiavanie postupu pre aktualizácie a aplikáciu záplat v príslušnej dokumentácii,
- Aktualizácia príslušnej dokumentácie (používateľskej, prevádzkovej a podobne),
- Poskytovanie konzultačných služieb pre správcov infraštruktúry, kľúčových používateľov,
- Nastavenie parametrov rozhraní,
- Konzultačná podpora pri Ročnej závierke,
- Úprava číselníkov a aktualizácia nastavení pre prechod do nového roka v zmysle harmonogramu „Prechod do roku RRRR“,
- Generovanie jednorazových alebo opakovaných výstupov aplikácie na základe požiadaviek používateľov,
- Práca so štatistickými zostavami,
- Podpora pri FAIN inventarizácii majetku pre ústredie a pobočky SP, softvérová údržba prístrojov na snímanie („Zebra“).

Úroveň poskytovanej služby

Aktivity realizované v rámci služieb technickej podpory budú podľa závažnosti zadelené do jednej z troch skupín podľa priority:

- **kritická priorita** – kritické zlyhanie systému, ktoré znemožňuje prácu so systémom, znemožňuje používanie systému; alebo celoplošný problém, jeho okamžité riešenie je nevyhnutné pre (dosiahnutie významného míľnika) fungovanie systému,

- **vysoká priorita** – zlyhanie systému, ktoré degraduje dostupnosť kritických funkcionalít, prevádzkyschopnosť systému je výrazne obmedzená; alebo lokálny problém, jeho okamžité riešenie je nevyhnutné pre (dosiahnutie významného míľnika) fungovanie systému. Náhradné riešenie/postup musí byť pre objednávateľa primerane akceptovateľné,
- **normálna priorita** – chyby systému, ktoré postihujú menej dôležité funkcionality a nemajú kritický dopad na prácu používateľov; alebo problém významným spôsobom ovplyvňuje fungovanie systému a spôsob realizácie operácií v ňom, pričom problém neohrozuje (dodržanie významného míľnika) fungovanie systému, funkcionalita existuje, ale zhoršený je jeden parameter.

Maximálne hodnoty časových limitov pre odstraňovanie vád (chýb):

Tabuľka č. 1: Definícia reakčných a servisných dôb

Priorita	Doba potvrdenia prevzatia požiadavky	Reakčná doba	Servisná doba
Kritická*	30 minút	4 hodiny	24 hodín
Vysoká	30 minút	8 hodín	32 hodín
Normálna	30 minút	24 hodín	72 hodín

* Ak je poskytovateľovi v pracovných dňoch v čase od 8.00 h do 16.00 h hlásená vada (chyba) s prioritou „kritická“, na reakčnú a servisnú dobu sa nevzťahuje štandardná servisná pohotovosť, ale režim 24x7. Do reakčnej a servisnej doby režimu 24x7 sa nezapočítavajú dni pracovného voľna, pracovného pokoja a štátom uznávané sviatky.

V osobitných prípadoch bude servisná doba upravená na základe dohody zodpovedných osôb objednávateľa a poskytovateľa.

Štandardná servisná pohotovosť je v pracovných dňoch od 8.00 h do 16.00 h. Do servisnej pohotovosti sa nezapočítavajú dni pracovného voľna, pracovného pokoja a štátom uznávané sviatky.

V prípade potreby zásahu pri vade s kritickou prioritou je poskytovateľ povinný vadu vyriešiť aj prostredníctvom vzdialeného zabezpečeného pripojenia (VPN) z miesta sídla poskytovateľa, pokiaľ mu objednávateľ nebude schopný poskytnúť fyzicky miesta v ústredí objednávateľa.

Riešenie servisných požiadaviek

- Replikácia dát z prevádzkovej do testovacej DB schémy,
- Plnenie servisných požiadaviek na vyžiadanie,
- Mimoaplikačné výbery, opravy dát v databáze na vyžiadanie,
- Reporty dát podľa špecifických požiadaviek objednávateľa,
- Testovanie IS na prechod SW tretích strán (napr. OS, DB, aplikačný server, integračné rozhrania) na vyššiu verziu alebo inú technológiu,
- Realizácia profylaktiky, ktorá zahŕňa jedenkrát ročne prezretie nastavení a konfigurácie prostredia IS, na ktoré sa vzťahuje podpora podľa uzatvorenej dohody. Termín plánovanej kontroly poskytovateľ vždy dohodne telefonicky alebo písomne s objednávateľom. Pravidelná profylaktika pozostáva z revízie systémových log-súborov na serveroch, kontroly naplnenosti úložiska systému, odstránenia problémov zistených počas preventívnej prehliadky,
- Inventarizácia majetku – softvérová údržba prenosného zariadenia na snímanie („Zebra“) - každoročné nastavenie.

Súčinnosť pri riešení problémov súvisiacich s prevádzkou IS FRSP

- Súčinnosť pri riešení problémov podporovaného IS vykonáva poskytovateľ poskytovaním pomoci pri analýze problémov, predkladaním návrhov a doporučení pre možné riešenia,
- Súčinnosť poskytovateľa pri riešení problémov súvisiacich s IS je poskytovaná telefonicky alebo v mieste sídla objednávateľa.

Odstraňovanie vád (chýb)

- Komunikácia s poskytovateľom IT služby je zabezpečená prostredníctvom integrovaných ServiceDeskových nástrojov cez webové služby (web service) počas, aj mimo prevádzkovej doby, alebo formou štruktúrovaného mailu (podľa prílohy č. 6 k rámcovej dohode). Prijatá komunikácia od objednávateľa bude spracovaná v čase prevádzkovej doby poskytovateľa IT služby.
- Poskytovateľ na svoje náklady prispôsobí technickú aj aplikačnú architektúru na svojej strane tak, aby bola zabezpečená bezpečná komunikácia prostredníctvom Service Deskov objednávateľa a poskytovateľa cez webové služby (web service).
- Objednávateľ pri hlásení požiadavky (vady (chyby)) v písomnej špecifikácii uvedie čo najpresnejší užívateľský popis služby pred zobrazením vady (chyby) s uvedením priority podľa bodu vyššie „Úroveň poskytovanej služby“, označenie verzie IS a v prípade systémových a aplikačných výpisov zašle aj znenie týchto výpisov; pri opakujúcom sa výskyte rovnakej vady (chyby) bude objednávateľ odosielať aj výpis z eventlogov na základe požiadavky poskytovateľa.
- Reakčná doba sa riadi zadelením požiadavky (vady (chyby)) do príslušnej kategórie podľa stanovenej priority podľa bodu vyššie „Úroveň poskytovanej služby“, pričom reakčná doba začína plynúť ihneď, ako bolo hlásenie doručené (od 8.00 h do 16.00 h v pracovných dňoch, v ostatných prípadoch od 8.00 h nasledujúceho pracovného dňa od doručenia hlásenia). Do reakčnej doby sa nezapočítavajú dni pracovného voľna, pracovného pokoja a štátom uznané sviatky; reakčná doba je považovaná za ukončenú zo strany objednávateľa vyriešením požiadavky cez WS, alebo v prípade komunikácie prostredníctvom štruktúrovaného mailu odoslaním riešenia na adresu ServiceDeskExt@socpoist.sk v štruktúrovanej forme.
- Služby sú poskytované počas pracovných dní od 8.00 h do 16.00 h.
- V osobitných prípadoch môže byť služba poskytnutá aj mimo času uvedeného v predchádzajúcom odseku na základe dohody zodpovedných osôb objednávateľa a poskytovateľa.
- Do reakčnej doby sa nezapočítavajú dni pracovného voľna, pracovného pokoja a štátom uznané sviatky; reakčná doba je považovaná za ukončenú zo strany objednávateľa vyriešením požiadavky cez WS, alebo v prípade komunikácie prostredníctvom štruktúrovaného mailu odoslaním riešenia na adresu ServiceDeskExt@socpoist.sk v štruktúrovanej forme.
- Servisná doba sa považuje za ukončenú zo strany objednávateľa zaslaním informácie o odstránení vady (chyby) vrátane popisu riešenia zo strany poskytovateľa formou vyriešením požiadavky cez WS, alebo v prípade komunikácie prostredníctvom štruktúrovaného mailu odoslaním riešenia na adresu ServiceDeskExt@socpoist.sk v štruktúrovanej forme.
- Pri vadách (chybách), ktoré sa nedajú odstrániť v tomto termíne, sa objednávateľ a poskytovateľ dohodnú v tomto čase na ďalšom postupe.
- Do servisnej doby sa nezapočítavajú dni pracovného voľna, pracovného pokoja a štátom uznané sviatky.

Inštalácia opravných verzií IS u objednávateľa

Inštalácia opravných verzií je vykonávaná prostredníctvom vzdialeného prístupu typu Remote Desktop Protocol (RDP) alebo v mieste sídla objednávateľa - Sociálna poisťovňa, Ul. 29. augusta 8 a 10 v Bratislave.

Podmienky poskytovania technickej podpory IS, objednávanie a fakturácia služieb

Objednávateľ je oprávnený počas trvania dohody požadovať poskytovanie služieb technickej podpory IS FRSP v súlade so svojimi potrebami na základe písomnej objednávky. Poskytovateľ poskytne služby technickej podpory IS FRSP za v dohode dohodnutú mesačnú paušálnu cenu.

Faktúru za poskytovanie služieb technickej podpory bude poskytovateľ vystavovať mesačne za uplynulý kalendárny mesiac. Podkladom k schvaľovaniu faktúry poskytovateľa objednávateľom bude protokol o paušálnej podpore (podľa prílohy č. 7 k rámcovej dohode), ktorý bude obsahovať evidenčný zoznam prijatých hlásení prevádzkových problémov a ich stav riešenia.

Tabuľka č. 2: Zoznam kontaktných osôb

Kontakt (Meno Priezvisko)	Oblasť	Tel. číslo	E-mail
Centrálny dispečing objednávateľa	Oznamovanie plánovaných a neplánovaných odstávok IS SP	+421 906171204	dispecing@socpoist.sk
	Hlásenie požiadaviek	+421 906171204	ServiceDeskExt@socpoist.sk
XXXXX	Zodpovedná osoba objednávateľa - projektový manažér	+421 XXXXX	XXX@socpoist.sk
XXXXX	Zodpovedná osoba poskytovateľa - projektový manažér	+421 XXXXX	XXX@dxc.com

b) Poskytovanie služieb rozvoja IS FRSP

Zapracovávanie legislatívnych zmien

Z pohľadu koncepcie ďalšieho rozvoja IS FRSP je nevyhnutné zabezpečiť predovšetkým realizáciu funkcionality v zmysle legislatívnych požiadaviek uvedených najmä v zákone č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, v zákone č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, v zákone č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, v zákone č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, v zákone č. 311/2001 Z. z. Zákonník práce a v ďalších súvisiacich zákonoch.

V rámci rozvojových aktivít bude zabezpečené, aby funkcionalita IS FRSP bola v súlade s legislatívou pre oblasť informačnej, kybernetickej bezpečnosti, štandardov pre informačné systémy verejnej správy a tiež bola v súlade s legislatívou pre oblasť projektového riadenia, a to konkrétne najmä so:

- Zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, uznesením vlády SR č. 328/2015 k návrhu Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020,
- Výnosom Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov,
- Zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení zákona č. 373/2018 Z. z.,
- Zákonom č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákonom č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Zákonom č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov,
- Zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- Zákonom č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-governmente) v znení neskorších predpisov,
- Vyhláškou č. 401/2023 Z. z. Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v znení neskorších predpisov,
- Vyhláškou č. 78/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov,
- Vyhláškou č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa upravuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- Vyhláškou NBÚ 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,
- Vyhláškou NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v aktuálne platnom znení,
- Metodikou pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti 2.1 (dostupná na https://www.csirt.gov.sk/wp-content/uploads/2021/08/MetodikaZabezpeceniaIKT_v2.1.pdf, ďalej len „Metodika zabezpečenia“),
- Nariadením 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 (GDPR),
- Zákonom č. 215/2021 Z. z. zo dňa 4. mája 2021 o podpore v čase skrátenej práce a o zmene a doplnení niektorých zákonov,
- a s ďalšími, neskôr v požiadavkách špecifikovanými, tu neuvedenými legislatívnymi zmenami.

Implementácia zmien a úprav v IS FRSP na základe požiadaviek objednávateľa

Objednávateľ môže požadovať implementáciu zmien a úprav, ktoré vyplynú z potrieb vecne príslušných útvarov za účelom najmä:

- zvyšovania automatizácie a elektronizácie,
- zmien, úprav a doplnenia procesov,
- úprav a rozširovania funkcionality,
- integrácie a konsolidácie údajovej základne,
- úprav komunikačných rozhraní a integrácie na zdroje dát (poskytovanie údajov).

Objednávateľ môže tiež požadovať implementáciu najmä nasledovných zmien a úprav:

- nadstavby modulu SAP FI-AA – modul FAIN – inventarizácia majetku,
- periodické práce s majetkom – zaradenie, vyradenie majetku, prevody,
- reporting hromadných exportov osobných kariet zamestnancov (aktívnych, neaktívnych),
- vykonanie technického redizajnu riešenia tak, aby bolo zabezpečené, že časové údaje v ZOSK a SAP FI-AA budú identické,
- nastavenie, doplnenie nových parametrov v súvislosti s evidenciou nehnuteľností v majetku SP,
- možnosť vyhotovenia reportu, resp. porovnania údajov z osobných kariet so zoznamom „aktívnych zamestnancov“,
- reporting a sledovanie nákladov na konkrétnych účtoch pre vybrané komodity (energie, nájmy, prenájmy, služby spojené s nájmami, opravy a údržba budov a pod.) z pohľadu sledovania čerpania finančných prostriedkov na jednotlivé objekty SP: budovy, lokality,
- prístup k transakciám pre správu budov z pohľadu plánovania, rozpočtovania a sledovania vynakladaných prostriedkov,
- automatizovaný prenos účtovných zápisov z Excel do SAP FI - univerzálny nástroj,
- zverejňovanie faktúr - rozšírenie prenosu zo SAP o identifikáciu (príslušnosť) k organizačnej zložke – pracovnému úseku na web Sociálnej poisťovne v zmysle dodržania zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám,
- aktualizácia word šablón vybraných účtovných dokladov, ktoré sa napĺňajú v SAP,
- riešenie Základnej finančnej kontroly v SAP – proces schvaľovania,
- programová úprava pre realizovanie výstupov účtovných scenárov a podstromov v štruktúre xls,
- crossmodul - aktivity súvisiace s ročnou účtovnou závierkou v zmysle bodov harmonogramu „Prechod do roku RRRR“,
- zapracovanie elektronických daňových formulárov – nové šablóny v SAP HR pre aktuálny rok,
- grafické zobrazenie organizačnej štruktúry, zobrazenie personálnej obsadenosti a sledovanie voľných neobsadených miest v Organizačnom manažmente v module HR.

Objednávateľ môže ďalej požadovať implementáciu zmien a úprav, ktorých potreba objektívne vyplynie z prevádzkových potrieb IS FRSP v čase plnenia dohody (napr. technologický upgrade súčasnej infraštruktúry prevádzkovaného IS) za účelom:

- opätovnej inštalácie IS a systémových komponentov po vadách infraštruktúry objednávateľa alebo neočakávaných udalostiach spôsobených prírodným alebo ľudským faktorom,
- rekonfigurácie a reinštalácie IS a systémových komponentov v prípade technologických zmien v prostredí objednávateľa,
- inštalácie nových verzií systémových komponentov v prípade ich upgradu.

Poskytovateľ je povinný dodržiavať okrem iného aj platnú legislatívu pre oblasť kybernetickej bezpečnosti a zabezpečenia ITVS, ako aj pre oblasť projektového riadenia a zabezpečiť ochranu kybernetickej bezpečnosti objednávateľa v súvislosti s predmetom dohody, a teda aj bezpečnosť, integritu, dôvernosť a dostupnosť údajov predmetu dohody. V prípade, ak poskytovateľ nebude konať sám v zmysle nižšie uvedených bezpečnostných požiadaviek a platnej legislatívy pre oblasť kybernetickej bezpečnosti a zabezpečenia ITVS, ako aj pre oblasť projektového riadenia, požiada objednávateľ o implementáciu úprav a zmien pre predmet dohody.

- Takéto úpravy a zmeny vyplývajúce z aktuálnej platnej legislatívy pre oblasť kybernetickej bezpečnosti a zabezpečenia ITVS, ako aj pre oblasť projektového riadenia, nemožno považovať za nadprácu, či úpravy a zmeny mimo dohodnutých či objednaných.

Úroveň poskytovaných výkonov a služieb, spôsob a forma realizácie rozvoja IS FRSP

Objednávateľ bude požadovať poskytovanie služieb rozvoja v súlade so svojimi potrebami na základe písomnej objednávky. Objednávke bude predchádzať vypracovanie ponuky - stanoviska s návrhom riešenia poskytovateľom v rozsahu požiadaviek definovaných objednávateľom.

▪ Požiadavky objednávateľa

Návrhy požiadaviek na zmeny/úpravy IS FRSP (podľa prílohy č. 8 k rámcovej dohode) bude poskytovateľovi predkladať projektový manažér objednávateľa za účelom vypracovania stanoviska s návrhom riešenia.

▪ Stanovisko poskytovateľa

Ku každej požiadavke na zmeny/úpravy IS FRSP vypracuje poskytovateľ najneskôr do desiatich (10) pracovných dní od jej predloženia ponuku - písomné stanovisko s návrhom riešenia, v ktorom uvedie:

- vyjadrenie k realizovateľnosti navrhovaných zmien/úprav,
- návrh riešenia,
- rozsah výkonov a služieb s uvedením človekohodín/človekodní,
- vplyv na náklady - s uvedením ceny v mene €,
- vplyv na termíny - s uvedením termínu/realizácie od momentu prijatia objednávky,
- prípadné podmienky realizácie.

Ponuka poskytovateľa bude vypracovaná na tlačive príslušnej požiadavky objednávateľa na zmeny/úpravy IS FRSP (podľa prílohy č. 8 k rámcovej dohode).

Zodpovedná osoba objednávateľa zabezpečí do 10 pracovných dní schválenie/neschválenie stanoviska poskytovateľa k návrhu na zmenu/úpravu IS.

- **Objednávanie služieb a potvrdzovanie objednávky**

Objednávateľ potvrdí prijatie návrhu poskytovateľa na základe požiadavky schválenej oboma stranami zaslaním písomnej objednávky.

Poskytovateľ služieb potvrdí prijatie každej objednávky objednávateľa bez zbytočného odkladu, najneskôr však do dvoch (2) pracovných dní odo dňa jej doručenia.

- **Odovzdávanie a akceptácia vykonaných výkonov a/alebo služieb, aktualizácia dokumentácie**

O činnosti poskytovateľa pri realizácii zmien/úprav IS FRSP bude zodpovedná osoba poskytovateľa vyhotovovať akceptačný protokol o vykonaných výkonoch a/alebo službách (podľa prílohy č. 9 k rámcovej dohode) (ďalej aj ako „protokol“). Protokol o vykonaných výkonoch a/alebo službách bude zodpovedná osoba poskytovateľa predkladať na potvrdenie zodpovednej osobe objednávateľa po realizácii výkonov a/alebo služieb. Protokol zároveň deklaruje platnosť nastavených zmien, ich funkčnosť a prenos do produkcie.

V prípade, ak objednávateľ z objektívnych dôvodov upraví rozpracovanú už objednanú požiadavku na rozvoj IS počas jej realizácie, poskytovateľ preruší výkon a spracuje stanovisko k predloženému upravenému návrhu na úpravu a zmenu IS, v ktorom zapracuje aj realizované výkony a/alebo služby do lehoty prerušenia výkonov a/alebo služieb. Ku dňu prerušenia výkonov a/alebo služieb zodpovedná osoba poskytovateľa vyhotoví protokol o vykonaných prácach a predloží ho na potvrdenie zodpovednej osobe objednávateľa. Poskytovateľ bude pokračovať v spracovaní požiadavky na úpravu a zmenu IS až po schválení jeho nového stanoviska zodpovednou osobou objednávateľa.

V prípade, ak objednávateľ z objektívnych dôvodov zruší rozpracovanú už objednanú požiadavku na rozvoj IS počas jej realizácie, zo strany poskytovateľa dôjde k bezodkladnému ukončeniu výkonov a služieb s tým, že náklady spojené s výkonom a službou poskytovateľa do momentu zrušenia úpravy budú uhradené zo strany objednávateľa v rozsahu skutočne realizovaných výkonov a/alebo služieb stanovených v počte človekohodín/človekodní na základe potvrdeného protokolu o vykonaných výkonoch a/alebo službách. Za vykonané služby sa považuje aj analýza, potrebná k požadovanej úprave a vykonaná poskytovateľom po vystavení záväznej objednávky objednávateľom.

Realizované úpravy a zmeny IS bude poskytovateľ odovzdávať objednávateľovi vykonaním akceptačných testov vrátane bezpečnostných testov.

Akceptačné testy budú vykonávané podľa špecifikácie schválenej zodpovednými osobami oboch účastníkov dohody.

Ak sa pri akceptačnom teste vyskytnú vady (chyby), ktoré budú znemožňovať používanie realizovaných úprav a zmien IS, po odstránení týchto vád (chýb) sa vykoná opakovaný akceptačný test.

Ak sa pri akceptačnom teste nevyskytnú vady (chyby), realizácia zmien/úprav IS sa bude považovať za vykonanú a za odovzdanú objednávateľovi. Zodpovedné osoby oboch účastníkov dohody podpíšu akceptačný protokol, ktorý bude obsahovať výsledok testovania.

Ak úprava IS významným spôsobom mení spôsob prevádzkovania príslušnej časti aplikácie, pri prevzatí úpravy/zmeny funkcionality IS do produkčnej prevádzky bude objednávateľovi odovzdaná aktualizácia používateľskej, administrátorskej a prevádzkovej dokumentácie s aktualizovanými zdrojovými kódmi minimálne v súlade a v rozsahu Vyhlášky č. 401/2023 Z. z., ktorá bude obsahovať zapracované zmeny a zároveň poskytovateľ dodá zoznam zmien na jednotlivých úrovniach, a to s uvedením rozdielu voči pôvodnej verzii tak, aby bolo preukázané, či došlo k zmene, pridaniu

alebo odstráneniu „časti“. Poskytovateľ taktiež dodá vyplnený rozpis dodávky/zmeny (podľa prílohy č. 12 k rámcovej dohode).

Inštalácia nových verzií bude vykonávaná v mieste sídla objednávateľa Sociálna poisťovňa, ústredie, Bratislava (Ul. 29. augusta 8 a 10) alebo prostredníctvom vzdialeného zabezpečeného pripojenia (VPN) z miesta sídla poskytovateľa.

- **Dodávka dokumentácie a sprístupnenie zdrojového kódu prostredníctvom GitLab**

1. Poskytovateľ je povinný dodať objednávateľovi súčasne s dodaním každej úpravy a zmeny APV aktualizáciu používateľskej a administrátorskej dokumentácie v slovenskom jazyku v elektronickej forme na prenosnom dátovom úložisku (USB resp. flash disk). Poskytovateľ je povinný dodať objednávateľovi do tridsať (30) dní odo dňa nadobudnutia účinnosti dohody komentované zdrojové kódy k celému informačnému systému v jeho aktuálnom stave ku dňu nadobudnutia účinnosti dohody v elektronickej forme na prenosnom dátovom úložisku (USB resp. flash disk) v počte dvoch (2) ks. Poskytovateľ je povinný dodať objednávateľovi komentované aktualizované zdrojové kódy k IS v elektronickej forme na prenosnom dátovom úložisku (USB resp. flash disk) v počte dvoch (2) ks do desať (10) pracovných dní odo dňa skončenia kalendárneho roka. Poskytovateľ je povinný dodať objednávateľovi komentované aktualizované zdrojové kódy k IS ku dňu skončenia dohody v elektronickej forme na prenosnom dátovom úložisku (USB resp. flash disk) v počte dvoch (2) ks v deň skončenia dohody.
2. Ak objednávateľ vytvorí vo svojom prostredí možnosť použitia produktu GitLab na účely dodania zdrojového kódu, poskytovateľ sa zaväzuje nainštalovať na objednávateľom vyhradenú infraštruktúru nevyhnutné komponenty GitLab pre ukladanie a kompilovanie zdrojového kódu IS FRSP. Ak poskytovateľ začne dodávať zdrojové kódy objednávateľovi prostredníctvom gitlab.socpoist.sk, dodávanie zdrojových kódov formou na prenosnom USB nosiči podľa bodu 1 bude používané len ako náhradná metóda dodania zdrojového kódu v prípade nefunkčnosti GitLab.
3. Bod 1 a 2 sa neaplikuje na diela tretích strán, ak sa účastníci dohody písomne nedohodli inak.
4. Povinnosti poskytovateľa vzťahujúce sa na dodanie zdrojových kódov k celému informačnému systému, ako aj aktualizovaných verzií zdrojových kódov sa neaplikuje pre dodanie v elektronickej forme na prenosovom dátovom úložisku v prípade, že objednávateľ disponuje so zdrojovými kódmi na všetky moduly tvoriace IS FRSP v zmysle vyššie uvedeného a môže s nimi nakladať v súlade s ustanoveniami zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov. Povinnosť okomentovaných zdrojových kódov, ako aj uvedenie zapracovaných zmien na jednotlivých úrovniach, a to s uvedením rozdielu voči pôvodnej verzii tak, aby bolo preukázané, či došlo k zmene, pridaniu alebo odstráneniu „časti“ do príslušnej dokumentácie, ale trvá.

- **Fakturácia**

Faktúra za plnenia bude vystavená poskytovateľom po odovzdaní zmien/úprav IS. Podkladom k schváleniu úhrady faktúry bude akceptačný protokol o prevzatí zmien/úprav IS do prevádzky podpísaný zodpovednými osobami objednávateľa, ktorý bude tvoriť prílohu faktúry predloženej na úhradu.

- **Bezpečnostné požiadavky**

Poskytovateľ sa v súvislosti s plnením predmetu dohody zaväzuje okrem iných zákonných požiadaviek dodržiavať bezpečnostnú politiku objednávateľa, ďalšie objednávateľom vydané bezpečnostné smernice a štandardy, požiadavky na bezpečnosť definované Zákonom o kybernetickej bezpečnosti, Zákonom o ITVS, Vyhláškou o štandardoch pre ITVS a Vyhláškou, ktorou sa upravuje spôsob kategorizácie a obsah bezpečnostných opatrení ITVS a

iné bezpečnostné požiadavky za predpokladu, ak ich objednávateľ uplatňuje a informuje o nich poskytovateľa.

Oprávnené osoby a pracovníci poskytovateľa, ktorí budú vykonávať pre objednávateľa činnosti súvisiace s plnením predmetu tejto dohody, musia byť poučení o povinnostiach podľa predchádzajúceho odseku a o tomto poučení musí poskytovateľ vytvoriť záznam, ktorý bude podpísaný poučenou osobou a osobou, ktorá poučenie vykonala. Za riadne poučenie zodpovedá poskytovateľ.

Poskytovateľ sa zaväzuje zaistiť bezpečnosť a odolnosť IS a jeho modulov voči aktuálne známym typom útokov a pred jeho odovzdaním vykonať testovanie na prítomnosť známych zraniteľností. V prípade zistenia zraniteľností sa poskytovateľ zaväzuje tieto zraniteľnosti odstrániť, vykonať opätovné testovanie a zdokumentovaný výsledok testovania odovzdať objednávateľovi spolu s dodávaným riešením.

Zdokumentovaný výsledok bezpečnostného testovania v zmysle vyššie uvedeného bodu musí obsahovať nasledovné údaje:

- čo konkrétne bolo testované,
- aká metodika bola použitá,
- kto testy vykonal spolu s informáciou o jeho kvalifikácii,
- časové údaje o testovaní,
- výsledok testovania,
- vykonané opatrenia voči zisteniam,
- ďalší priebeh – opakované testovania až do odstránenia zistení.

Poskytovateľ sa zaväzuje dodržiavať nasledovné bezpečnostné opatrenia a zásady:

- všetky vstupy aplikácií tvoriacich systém sú kontrolované na validnosť a sú sanitované,
- je zapnutá len nutne potrebná funkcionalita, porty a IP adresy a všetky ostatné sú vypnuté,
- v prípade, že je nevyhnutné vykonávať správu informačného systému na diaľku, je to možné vykonávať výhradne prostredníctvom šifrovaných protokolov,
- všetky pôvodné a administrátorské účty sú zdokumentované a majú unikátne prvotné heslo zložené z náhodnej postupnosti aspoň 14 znakov,
- systém disponuje funkcionalitou pre zmenu používateľských a administrátorských mien a hesiel a funkcionalitou vypnutia používateľského účtu,
- všetky komponenty sú aktuálne a podporované výrobcom a postup pre aktualizácie a aplikáciu záplat je zdokumentovaný a dodržiavaný,
- poskytovateľ umožní objednávateľovi vykonať skeny zraniteľností alebo penetračné testy dodávaného riešenia pred jeho finálnym odovzdaním a poskytovateľ sa zaväzuje nedostatky zistené týmto testovaním pred odovzdaním riešenia odstrániť.

Informačný systém a jeho moduly musia byť rozvíjané v bezpečnom vývojovom prostredí s použitím nástrojov, ktoré:

- musia byť získané legálnym spôsobom z dôveryhodných zdrojov,
- musia byť stále podporované výrobcom (t. j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané,
- musia byť aktualizované minimálne raz za 6 mesiacov a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.

Musia byť implementované príslušné opatrenia na zabezpečenie integrity IS a jeho modulov na základe najvyššej požadovanej úrovne ochrany dôvernosti, integrity a dostupnosti informácií, ktoré budú spracovávané vo vyvíjanom riešení.

Ak samotný vyvíjaný IS a jeho moduly obsahujú informácie, ktoré je potrebné chrániť z hľadiska dôvernosti (napr. prihlasovacie údaje k databázam), musia byť vo vývojovom prostredí

implementované opatrenia na zaistenie dôvernosti na základe požadovanej úrovne ochrany dôvernosti týchto údajov.

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 (napr. knižnice a komponenty dodané tretími stranami; systémy, na ktorých bude IS a jeho moduly postavené alebo ktoré bude využívať pri svojej prevádzke).

V prípade, že implementovaný IS a jeho moduly potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.

Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje:

- autentifikačné údaje musia byť uložené iba v podobe osolených hashov (salted hash), pričom použitá hashovacia funkcia by mala byť minimálne sha256,
- dôverné údaje (adresy, čísla platobných kariet, čísla občianskych preukazov, informácie o zdravotnom stave, údaje klasifikované klasifikačným stupňom chránené alebo vysoko chránené alebo ekvivalenty) musia byť uložené v šifrovanej podobe,
- ostatné osobné údaje nesmú byť ukladané v čistej podobe, ale musia byť chránené šifrovaním, pričom je možné použiť aj niektoré „Format-Preserving Encryption“ algoritmy.

Musí byť implementované logovanie a logy by mali zaznamenávať minimálne:

- prihlásenie a odhlásenie (úspešné aj neúspešné),
- vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny (úspešné aj neúspešné),
- pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie) (úspešné aj neúspešné),
- pokusy o kritické operácie (úspešné aj neúspešné).

Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov.

Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server.

Po ukončení vývoja musí prejsť IS a jeho moduly testovaním a verifikáciou:

- poskytovateľ musí overiť aspoň pomocou automatizovaných nástrojov štandardné zraniteľnosti. Malo by prebehnúť minimálne testovanie vstupov (fuzzing) a kontrola práce s pamäťou (memory leaky, memory corruption),
- poskytovateľ musí zabezpečiť realizáciu opatrení vyplývajúcich z analýzy rizík vypracovanej v rámci Cieľového konceptu,
- poskytovateľ musí zabezpečiť penetračné testovanie externou organizáciou,
- zraniteľnosti a problémy zistené na základe testovania musia byť poskytovateľom odstránené a ich oprava musí byť potvrdená opakovaným testovaním, a to pred odovzdaním a prevzatím predmetu dohody.

Hotový predmet dohody s odstránenými nájdenými zraniteľnosťami musí byť nasadený v prostredí zabezpečenom na základe odporúčaní v kapitolách o zabezpečení služieb a infraštruktúry v Metodike zabezpečenia.

Musí byť zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami.

Pri prevzatí úpravy a zmeny funkcionality IS do prevádzky bude objednávateľovi odovzdaná aktualizácia používateľskej, administrátorskej a prevádzkovej dokumentácie a vyhlásenie

poskytovateľa, že realizované úpravy a zmeny boli poskytovateľom analyzované a testované na známe bezpečnostné riziká.

Pre zamedzenie pochybností, povinnosti poskytovateľa týkajúce sa zdrojových kódov platia i na akékoľvek opravy, zmeny, doplnenia, upgrade alebo update zdrojového kódu a/alebo vyššie uvedenej dokumentácie, ku ktorým dôjde pri plnení tejto dohody alebo v rámci záručných opráv. Zdrojové kódy budú vytvorené vyexportovaním z vývojového prostredia a budú odovzdané objednávateľovi na elektronickom médiu v zapečatenom obale. Poskytovateľ je povinný umožniť objednávateľovi pri odovzdávaní zdrojových kódov, pred zapečatením obalu, skontrolovať v priestoroch objednávateľa prítomnosť zdrojových kódov na odovzdávanom elektronickom médiu.

Kontrola vykonaných opatrení sa vykonáva dvoma spôsobmi:

- pri odovzdávaní predmetu dohody na mieste dohodnutom medzi objednávateľom a poskytovateľom,
- počas implementácie predmetu dohody na mieste, kde prebieha vývoj riešenia.

Kontrola pri odovzdávaní predmetu dohody pozostáva z:

- kontroly projektovej dokumentácie obsahujúcej minimálne návrh predmetu dohody s popisom jednotlivých súčastí - modulov (Cieľový koncept), vývojársku dokumentáciu a dokumentáciu pre používateľov a správcov,
- kontroly analýzy rizík a implementácie navrhnutých opatrení,
- kontroly verzionovanej histórie vývoja predmetu dohody pozostávajúcej minimálne z kontroly podpísaných commitov a z kontroly, či zmeny vykonané v danom commite súvisia s jeho popisom,
- kontroly zdrojových kódov na použité zastarané/nebezpečné funkcie,
- kontroly formátu citlivých údajov v databáze,
- kontroly výsledkov testovania implementovaného riešenia.

Kontrola počas implementácie predmetu dohody na mieste, kde prebieha vývoj predmetu dohody, pozostáva z:

- kontroly použitých vývojárskych nástrojov, ich pôvodu, legálnosti a aktuálnosti,
- kontroly implementovaných opatrení na zabezpečenie integrity vyvíjaného predmetu dohody, prípadne aj jeho dôvernosti,
- kontroly anonymizácie použitých testovacích údajov počas implementácie predmetu dohody,
- kontroly zapnutých bezpečnostných vlastností použitých nástrojov (varovania, ochrany).

Poskytovateľ je povinný bezodplatne uzavrieť ako tretia osoba s objednávateľom ako prevádzkovateľom základnej služby samostatnú 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 a to súčasne s uzatvorením tejto dohody (podľa prílohy č. 14 k rámcovej dohode).

c) Poskytovanie školení v súvislosti s používaním IS FRSP

Objednávateľ môže od poskytovateľa požadovať poskytovanie školení zamestnancom Sociálnej poisťovne v súvislosti s používaním IS FRSP.
Cieľom školení bude zlepšenie a rozšírenie používateľských zručností zamestnancov alebo preškolenie zamestnancov v súvislostí s rozvojom IS FRSP, s úpravami a rozšírením funkcionality, so zmenami, úpravami a doplneniami procesov, a to najmä v oblastiach:

- finančné účtovníctvo,
- controlling,
- rozpočtovníctvo,

- majetok, vrátane inventarizácie majetku (modul FAIN),
- materiálové hospodárstvo a obstarávanie,
- odberateľská fakturácia,
- personalistika a mzdy,
- administratíva a správa systému,
- integračné rozhrania s ostatnými systémami Sociálnej poisťovne.

Spôsob realizácie školení

Objednávateľ stanoví štruktúru a rozsah školení na základe svojich aktuálnych potrieb.

Objednávateľ bude požadovať poskytovanie školení v súlade so svojimi potrebami na základe písomnej objednávky. Objednávke bude predchádzať vypracovanie ponuky - stanoviska s návrhom riešenia poskytovateľom v rozsahu požiadaviek definovaných objednávateľom.

Cena za školenia bude stanovená na základe počtu realizovaných človekohodín/človekodní školenia nezávisle od počtu školených zamestnancov Sociálnej poisťovne a od miesta školenia.

Miestom školenia môže byť sídlo objednávateľa Sociálna poisťovňa, ústredie, Bratislava (Ul. 29. augusta 8 a 10) alebo vybrané pobočky Sociálnej poisťovne na úrovni kraja v rámci Slovenskej republiky, prípadne len po vzájomnej dohode môže byť školenie vykonávané online cez aplikáciu Microsoft Teams.

- **Požiadavka objednávateľa**

Návrh požiadavky na školenie (podľa prílohy č. 10 k rámcovej dohode) bude poskytovateľovi predkladať projektový manažér objednávateľa za účelom vypracovania stanoviska s návrhom riešenia.

- **Stanovisko poskytovateľa**

Ku každej požiadavke na školenie vypracuje poskytovateľ najneskôr do desiatich (10) pracovných dní od jej predloženia ponuku - písomné stanovisko s návrhom riešenia, v ktorom uvedie:

- vyjadrenie k realizovateľnosti navrhovaného školenia,
- návrh a rozsah školenia s uvedením človekohodín/človekodní,
- vplyv na náklady - s uvedením ceny v mene €,
- vplyv na termíny - s uvedením termínu/realizácie od momentu prijatia objednávky,
- prípadné podmienky realizácie.

Ponuka poskytovateľa bude vypracovaná na tlačive súvisiacej požiadavky objednávateľa na školenie (podľa prílohy č. 10 k rámcovej dohode).

Zodpovedná osoba objednávateľa do 10 pracovných dní zabezpečí schválenie/neschválenie stanoviska poskytovateľa k návrhu na školenie.

- **Objednávanie služieb a potvrdzovanie objednávky**

Objednávateľ potvrdí prijatie návrhu poskytovateľa na základe požiadavky schválenej oboma stranami zaslaním písomnej objednávky.

Poskytovateľ služieb potvrdí prijatie každej objednávky objednávateľa bez zbytočného odkladu, najneskôr však do dvoch (2) pracovných dní odo dňa jej doručenia.

- **Protokol o vykonanom školení**

O realizácii školenia bude zodpovedná osoba poskytovateľa vyhotovovať protokol o vykonanom školení (podľa prílohy č. 11 k rámcovej dohode) (ďalej aj ako „protokol“), ktorého prílohu bude tvoriť prezenčná listina účastníkov školenia. Protokol bude zodpovedná osoba poskytovateľa predkladať na potvrdenie zodpovednej osobe objednávateľa po realizácii školenia.

- **Fakturácia**

Faktúra za školenie bude vystavená poskytovateľom po realizácii školenia. Podkladom k schváleniu úhrady faktúry bude protokol o vykonanom školení podpísaný zodpovednou osobou objednávateľa, ktorý bude tvoriť prílohu faktúry predloženej na úhradu.

C. Zoznam vybraných skratiek

Tabuľka č. 3: Zoznam vybraných skratiek

Skratka	Vysvetlenie
APV	Aplikačné programové vybavenie
IS	Informačný systém
IS DAÚP	Informačný systém Dávková agenda úrazového poistenia
IS FRSP	Informačný systém Finančného riadenia Sociálnej poisťovne
IS JVP	Informačný systém Jednotný výber poistného
IS NPaLPČ	Informačný systém Nemocenské poistenie a lekárska posudková činnosť
IS PvNGP	Informačný systém Poistenie v nezamestnanosti a garančné poistenie
IT	Informačné technológie
ITVS	Informačné technológie verejnej správy
MPSVaR	Ministerstvo práce, sociálnych vecí a rodiny
SAP	Softvérová aplikácia na správu firemných dát a procesov
SE9	Archívny systém po eurokonverzii, so stavom produkčného systému pred implementáciou aplikačných modulov (SAP PSM, SAP FI-AA, SAP-MM/MME, SAP CO) v roku 2009 (Účtovanie do roku 2009)
SED	Vývojovo-customizačné prostredie v IS FRSP
SEE	Archívny systém so stavom produkčného systému pred eurokonverziou
SEP	Produkčné prostredie v IS FRSP
SEQ	Testovacie prostredie v IS FRSP
SAP Legacy	Informačný systém, ktorý združuje staršie IS výberu poistného
SP	Sociálna poisťovňa
SW	Softvér
ÚPSVaR	Ústredie práce, sociálnych vecí a rodiny
VRP	Vrátené platby

Príloha č. 2 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

PREDPOKLADANÉ MNOŽSTVO A CENA

Predmet dohody	**Merná jednotka (MJ)**	**Predpokladaný počet MJ**	**Cena za MJ v EUR bez DPH**	**Cena za MJ v EUR s DPH**
a	b	c	d	e
Služby technickej podpory IS FRSP podľa čl. III bodu 3.1.1 dohody	mesiac	12	3 905,00 €	4 686,00 €
Služby rozvoja IS FRSP podľa čl. III bodu 3.1.2 dohody	človekodeň*	269**	585,00 €	702,00 €
Poskytovanie školení podľa čl. III bodu 3.1.3 dohody	človekodeň*	15**	550,00 €	660,00 €

* Pozn.: 1 človekodeň = 8 hodín

** Počet človekodní uvedený v tejto kalkulácii je stanovený len ako predpokladaný, pričom objednávateľ nie je povinný počas platnosti a účinnosti tejto dohody vyčerpať, resp. objednať celý predpokladaný počet človekodní, ale len počet, ktorý bude zodpovedať aktuálnej potrebe objednávateľa.

V Bratislave dňa .....

.....
Ing. Martin Peluha, konateľ
DXC Technology Slovakia s.r.o.

Príloha č. 3 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

ZOZNAM SUBDODÁVATEĽOV

Obchodné meno uchádzača: DXC Technology Slovakia s.r.o.
Adresa/sídlo uchádzača: Galvaniho 7, 820 02 Bratislava
IČO uchádzača: 35 785 306

Na uskutočnení plnenia rámcovej dohody o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA**

a) ~~sa nebudú podieľať subdodávatelia a celý predmet rámcovej dohody 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 rámcovej dohody v %	Predmet subdodávok
1.	GLOBESY, s.r.o. Framborská 58 010 01 Žilina	36407275	Ing. Martin Valúch Hore jarky 83/5 Hôrky 010 04 27.06.1972	36407275	40%	Programátorské služby
2.						
3.						

V Bratislave, dňa .....

.....
Ing. Martin Peluha, konateľ
DXC Technology Slovakia s.r.o.

*Nehodiace sa prečiarknite

Príloha č. 4 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

ZÁPIS
O ZMENE PRÍLOHY Č. X „ZOZNAM XXX“

k rámcovej dohode o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA** uzatvorenej podľa § 269 ods. 2 Obchodného zákonníka a podľa § 83 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „dohoda“) medzi:

poskytovateľom **DXC Technology Slovakia s.r.o., Galvaniho 7, Bratislava 820 02**, *IČO: 35 785 306*
(ďalej len „poskytovateľ“) 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.X dohody, v ktorom sa účastníci dohody dohodli o spôsobe zmeny prílohy č. X k dohode „Zoznam XXX“, účastníci dohody v zastúpení ich oprávnenými zástupcami podpisujú tento zápis, ktorým sa mení príloha č. X k dohode „Zoznam XXX“, ktorá tvorí prílohu k tomuto zápisu.

Dôvod potreby uskutočnenia zmeny prílohy č. X k dohode „Zoznam XXX“:

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

Tento zápis je neoddeliteľnou súčasťou dohody.

Tento zápis nadobúda platnosť dňom jeho podpísania oprávnenými zástupcami oboch účastníkov dohody 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 dohode „Zoznam XXX“.

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

Príloha:

Príloha č. X k dohode „Zoznam XXX“

Príloha č. 5 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

ZOZNAM EXPERTOV

Poradové číslo experta	Meno a priezvisko experta
Expert č. 1 Architekt pre SAP riešenia	XXXXX
Expert č. 2 ABAP programátor	XXXXX

Príloha č. 6 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

POŽIADAVKA PRE HLÁSENIE CHÝB

Požiadavka používateľa:

Stanovisko interného riešiteľa:

Výrobné číslo zariadenia:
Priorita:

Kontakt na používateľa:
E-mail:
Telefón:
Lokalita:
ŠPZ:

Kontakt na interného riešiteľa:
E-mail:
Telefón:
Lokalita:
ŠPZ:

Podrobnosti požiadavky:
Záznam riešiteľa:
Detailný záznam riešiteľa:

Cieľové časy SLA:
Cieľový reakčný čas:
Cieľový čas vyriešenia:

Riešenie, prosíme zaznamenať medzi nasledovné XML zátvorky FR2CODE_LONGDESCRIPTION a zmeniť hodnotu v YSTATUS na RESOLVED

<MAXIMOEMAILCONTENT>
<LSNRACTION>UPDATE</LSNRACTION>
<LSNRAPPLIESTO>SR</LSNRAPPLIESTO>
<TICKETID>xxxx</TICKETID>
<CLASS>SR</CLASS>
<EXTERNALSYSTEM_TICKETID></EXTERNALSYSTEM_TICKETID>
<YSTATUS>ASSIGNED</YSTATUS>
<FR2CODE_LONGDESCRIPTION>

</FR2CODE_LONGDESCRIPTION>
</MAXIMOEMAILCONTENT>

Zoznam hodnôt pre stav z pohľadu externého dodávateľa:
ASSIGNED - Priradený na riešiteľskú skupinu
INPROG - Prevzatý externým riešiteľom
WAIT4INFO - Zo strany externého dodávateľa čaká na reakciu SP
RESOLVED - Zo strany externého dodávateľa vyriešený

Pozn.: Ide o vzor xml štruktúry e-mailu v rámci aplikácie Service Desk.

Príloha č. 7 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

PROTOKOL O PAUŠÁLNEJ PODPORE

Sociálna poisťovňa
Rámcová dohoda o poskytovaní služieb
pre informačný systém Finančného riadenia Sociálnej poisťovne

Poskytovateľ:

Objednávateľ:
Sociálna poisťovňa
Ul. 29. augusta 8 a 10
813 63 Bratislava

Na základe Rámcovej dohody o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA** zo dňa XX.XX.2024 poskytovateľ vykonal služby technickej podpory pre informačný systém Finančného riadenia Sociálnej poisťovne za obdobie ... (mesiac). V rámci tejto podpory boli predmetom riešenia nasledujúce vady:

Referencia	Dátum evidencie	Popis	Stav riešenia
			Otvorený
			Uzatvorený

Na znak súhlasu s obsahom tohto protokolu o paušálnej podpore ho obaja účastníci dohody podpísali. Protokol o paušálnej podpore je vyhotovený v dvoch vyhotoveniach, pričom každý účastník dohody dostane jeden.

V Bratislave dňa XX. XX. 202X

Za poskytovateľa

Za objednávateľa

.....

zodpovedná osoba

.....

zodpovedná osoba

Príloha č. 8 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

POŽIADAVKA NA ZMENY / ÚPRAVY IS FRSP

Požiadavka na zmeny / úpravy			**Číslo požiadavky:**	
Predmet zmeny/úpravy:				
Meno žiadateľa zmeny/úpravy	**Pracovisko**	**Dátum**	**Telefón**	**Email**
Popis požadovanej zmeny/úpravy: **Prílohy k požiadavke:**				

Stanovisko poskytovateľa:
Vyjadrenie k realizovateľnosti: **Návrh riešenia:** **Rozsah výkonov a služieb:** **Vplyv na náklady**: **Vplyv na termíny**: **Podmienky realizácie:**

Návrh vypracoval	**Pracovisko**	**Dátum**	**Podpis**

Akceptoval:					
Za objednávateľa			**Za poskytovateľa**		
Meno a priezvisko	**Dátum**	**Podpis**	**Meno a priezvisko**	**Dátum**	**Podpis**

Príloha č. 9 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

AKCEPTAČNÝ PROTOKOL

Objednávateľ:	
Poskytovateľ:	
Projekt/dohoda:	
Číslo požiadavky:	
Predmet požiadavky:	
Predmet akceptácie:	
Miesto prevzatia:	

Potvrdenie o akceptovaní:
Predmet požiadavky bol dodaný v požadovanom termíne, plnom rozsahu a kvalite. Súčasťou tohto Akceptačného protokolu je: 1. Celkový výsledok testovania, ktoré prebehlo za účasti poskytovateľa.

Akceptoval:					
Za objednávateľa			**Za poskytovateľa**		
Meno a priezvisko	**Dátum**	**Podpis**	**Meno a priezvisko**	**Dátum**	**Podpis**

Príloha č. 10 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

POŽIADAVKA NA ŠKOLENIE

Požiadavka na školenie			**Číslo požiadavky:**	
Predmet školenia:				
Meno žiadateľa zmeny/úpravy	**Pracovisko**	**Dátum**	**Telefón**	**Email**
Popis, miesto a spôsob požadovaného školenia: **Prílohy:**				

Stanovisko poskytovateľa:
Vyjadrenie k realizovateľnosti: **Návrh a rozsah školenia:** **Vplyv na náklady**: **Vplyv na termíny**: **Podmienky realizácie:**

Návrh vypracoval:	**Pracovisko**	**Dátum**	**Podpis**

Akceptoval:					
Za objednávateľa			**Za poskytovateľa**		
Meno a priezvisko	**Dátum**	**Podpis**	**Meno a priezvisko**	**Dátum**	**Podpis**

Príloha č. 11 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

PROTOKOL O VYKONANOM ŠKOLENÍ

Objednávateľ:	
Poskytovateľ:	
Projekt/dohoda:	
Číslo požiadavky:	
Predmet školenia:	
Dátum školenia:	
Miesto školenia:	

Potvrdenie o akceptovaní:
Školenie bolo dodané v požadovanom termíne, plnom rozsahu a kvalite. Súčasťou tohto protokolu je: 1. Prezenčná listina účastníkov školenia.

Akceptoval:					
Za objednávateľa			**Za poskytovateľa**		
Meno a priezvisko	**Dátum**	**Podpis**	**Meno a priezvisko**	**Dátum**	**Podpis**

Príloha č. 12 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

ROZPIS DODÁVKY/ZMENY

Súčasti dodávky riešenia:

PREDMET ZMENY:	*Popis predmetu zmeny/novej funkčnosti*
Etapa:	*Názov etapy projektu*
Fáza:	*Názov fázy projektu*
Rola:	*Zodpovedný za danú fázu*

Činnosť presný popis	**Riešiteľ Meno a kontakt**	**Čas riešenia Človekodni/ človekohodiny**	**Poznámka**	**Vyjadrenie SP**
Uviesť čo najpresnejší popis činnosti	*Uviesť meno a kontakt na riešiteľa/kontaktnú osobu*	*Uviesť strávený čas na riešení činnosti*	*V prípade nutnosti spresniť poznámkou*	*Vyjadrenie SP či je riešenie v súlade so zadaním*

Rozpis dodávky/zmeny je potrebné vyplniť a jasne uviesť využitie pre nasledovné role/pozície:

Administrátor, Analytik, architekt, Podpora, Programátor, Rutinné práce, Technik, Tester, Vedúci projektu/PM, Školiteľ, Špecialista, Iné.

Príloha č. 13 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

Sprostredkovateľská zmluva č. 148-9/2024-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

Sociálna poisťovňa

Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
V zastúpení:	Ing. Michal Ilko, generálny riaditeľ
IČO:	308 07 484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA

(ďalej len „prevádzkovateľ)

a

DXC Technology Slovakia s.r.o.

Sídlo organizácie:	Galvaniho 7, 820 02 Bratislava
V zastúpení:	Ing. Martin Peluha, konateľ
IČO:	35 785 306
DIČ:	2020213393
IČ DPH:	SK2020213393
Bankové spojenie:	Všeobecná úverová banka, a.s.
Číslo účtu:	XXXXX
IBAN:	XXXXX
SWIFT:	SUBASKBX

Zapísaný v Obchodnom, resp. živnostenskom registri Mestského súdu Bratislava III, oddiel: sro, vložka č.: 21438/B
(ďalej len „sprostredkovateľ)
(spolu ďalej ako „zmluvné strany“)

Preambula

Zmluvné strany spolu uzatvárajú Rámcovú dohodu o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA** (ďalej len „rámcová dohoda“), predmetom ktorej je najmä poskytovanie služieb technickej podpory a rozvoja IS FRSP, podľa požiadaviek prevádzkovateľa. Sprostredkovateľ vystupuje v tejto rámcovej dohode ako poskytovateľ služieb, pričom nie je vylúčené, že v rámci plnenia predmetu rámcovej dohody sa dostane priamo aj k spracovaniu osobných údajov dotknutých osôb. Vzhľadom na vyššie uvedenú možnosť spracovania osobných údajov dotknutých osôb 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.
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje po splnení povinností uvedených v tejto zmluve a výlučne na účel poskytovania služieb pre informačný systém Finančného riadenia Sociálnej poisťovne.
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 a v medzinárodných zmluvách, ktorými je Slovenská republika viazaná, podľa ktorých je prevádzkovateľ oprávnený spracúvať osobné údaje dotknutých osôb za účelom výkonu sociálneho poistenia.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou rámcovej dohody a to pri poskytovaní poradenských služieb na základe samostatných písomných objednávok prevádzkovateľa, v rozsahu, v špecifikácii a za podmienok dohodnutých v rámcovej dohode.
5. 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 rámcovej dohode a v objednávkach, prípadne iné písomne zdokumentované pokyny

alebo požiadavky prevádzkovateľa na poskytnutie služby v zmysle rámcovej dohody.

6. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu zmluvy o vykonaní služieb je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom konkrétu zákonnú povinnosť ustanovuje zmluva o vykonaní 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 prevádzkovateľa:
   Rámcová dohoda o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA**.

2. Zoznam osobných údajov, ktoré môžu byť v prípade potreby realizácie predmetu rámcovej dohody predmetom spracúvania:
   Meno, priezvisko, titul, dátum narodenia, rodné číslo, pohlavie, stav, adresa trvalého pobytu, adresa korešpondenčného pobytu, dátum úmrtia, miesto narodenia, štátna príslušnosť, email, telefón, bankové spojenie, číslo bankového účtu, posledné priezvisko, osobné číslo zamestnanca, občianstvo, národnosť, číslo občianskeho preukazu / pasu, rodinný stav, profesia, zložky mzdy, príjmy, zrážky zo mzdy, rodina / člen rodiny, vzdelanie, poistné, daňové údaje, údaje o dôchodku, identifikačné údaje o dodávateľoch a odberateľoch.

3. Spracúvané osobné údaje sú povahy:
   Iné osobné údaje v rozsahu bodu 2 tohto článku.
   Spracúvané osobné údaje sú typu:
   adresné, zamestnanecké, ekonomické, sociálne,
   elektronické.

4. Sprostredkovateľ spracúva osobné údaje o dotknutých osobách .

Čl. IV
Spôsob výkonu a oprávnenia sprostredkovateľa

1. Sprostredkovateľ vykonáva spracúvanie osobných údajov prostredníctvom IS FR v súvislosti s plnením Rámcovej dohody o poskytovaní služieb pre IS FR.

2. Osobné údaje o dotknutých osobách sa získavajú 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, s medzinárodnými zmluvami o sociálnom zabezpečení, ktorými je Slovenská republika viazaná, za účelom výkonu sociálneho poistenia a vedenia ekonomickej, prevádzkovej, personálnej a mzdovej agendy Sociálnej poisťovne.

3. Na spracúvanie osobných údajov sprostredkovateľom sa v zmysle § 34 ods. 1 ZOOU nevyžaduje súhlas dotknutej osoby.

4. 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.

5. Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb po dobu trvania účelu spracúvania, resp. po dobu platnosti a účinnosti rámcovej dohody 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 dotknutých 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, rámcovej dohody 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 rámcovej dohody 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 a

rámcovej dohody, 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 rámcovej dohody nezverejňovať, neposkytovať a nesprístupňovať tretím stranám,
f) zachovávať mlčanlivosť a zabezpečiť diskrétnosť pri akomkoľvek spracúvaní osobných údajov,
g) ak rámcová dohoda 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, 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) 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, nepoužiť spracúvané osobné údaje v mene prevádzkovateľa pre vlastnú potrebu, pokiaľ všeobecne záväzné platné právne predpisy neustanovujú inak,
o) 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 sprostredkovateľ 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 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, a zároveň prostredníctvom iných osôb (ďalej len „subdodávateľ"), ktorými sú spoločnosti GLOBESY, s.r.o.. 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 obdržaní 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 rámcovej dohody 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:
   XXXXX, tel.: XXXXXXXX
   Email: XXXXX
7.

Čl. X
Trvanie a ukončenie Zmluvy

1. Táto Zmluva sa uzatvára po dobu trvania spolupráce Prevádzkovateľa a Sprostredkovateľa v zmysle Rámcovej dohody o poskytovaní služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA.**

Čl. XI
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 oboch zmluvných strán a účinnosť dňom nasledujúcim deň po dni zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Zmluvné strany sa dohodli, že táto Zmluva je uzatváraná v písomnej forme a písomné budú aj zmeny Zmluvy alebo pokyny Prevádzkovateľa Sprostredkovateľovi. Na potreby pokynov na plnenie sa za písomnú formu považuje aj e-mail, ak bude pri tom zachovaná dôvernosť odovzdávaných informácií.
4. Počas platnosti rámcovej dohody 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 Tariška
generálny riaditeľ
Sociálnej poisťovne

V ..... dňa .....

Za sprostredkovateľa:

Ing. Martin Peluha
konateľ
DXC Technology Slovakia s.r.o.

Príloha č. 14 k rámcovej dohode o poskytovaní služieb č. 148-8/2024-BA

Zmluva
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
č. 148-10/2024-BA

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 Tariška, 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:	**DXC Technology Slovakia s.r.o.**
Sídlo:	Galvaniho 7, 820 02 Bratislava
Štatutárny orgán:	Ing. Martin Peluha, konateľ
Zápis v registri:	Obchodný register Mestského súdu Bratislava III, oddiel Sro, vložka č. 21438/B.
IČO:	357 853 06
DIČ:	2020213393
IČ pre DPH:	SK2020213393
Bankové spojenie:	Všeobecná úverová banka, a.s.,
IBAN:	XXXXX

(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 Rámcovú dohodu na poskytovanie služieb pre informačný systém Finančného riadenia Sociálnej poisťovne č. **148-8/2024-BA.**
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: Matúš Ficko
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: bis@socpoist.sk.
5. Kontakt na zástupcu dodávateľa na úseku kybernetickej bezpečnosti je: matus.ficko.@dxc.com.
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 - Rámcová dohoda č. **148-8/2024-BA** o poskytovaní

služieb pre informačný systém Finančného riadenia Sociálnej poisťovne podľa § 269 odsek 2 zákona č. 513/19 91 Zb. Obchodného zákonníka a podľa § 83 zákona č. 343/2015 Z. z. o verejnom obstarávaní v znení neskorších predpisov, predmetom ktorej je poskytovanie služieb technickej podpory a rozvoja IS FRSP.

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 Príloha č. 1 – Bezpečnostné politiky.

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 Tariška, generálny riaditeľ Sociálnej poisťovne	Ing. Martin Peluha konateľ DXC Technology Slovakia s.r.o.

Príloha č. 1 k Prílohe č. 14

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 BIS@socpoist.sk a,

b) e-mailom oddeleniu centrálneho dispečingu a monitorovania služieb IS SP na adresu dispecing@socpoist.sk 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 dispecing@socpoist.sk.

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 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. 14 - zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Kyberbezpečnostný štandard
pre projekty a IT v Sociálnej poisťovni

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 v znení neskorších predpisov,
- 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 Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **401/2023** Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v znení neskorších predpisov,
- Vyhláška Národného bezpečnostného úradu č. 48/2019 Z. z., ktorou sa ustanovujú podrobnosti 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 v Únii,
- 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.