Z m l u v a
o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou

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

Zmluvné strany

1.	**Objednávateľ:**	**Sociálna poisťovňa**
	Sídlo:	Ul. 29. augusta č. 8 a 10, 813 63 Bratislava
	Štatutárny orgán:	Ing. Michal Tariška generálny riaditeľ Sociálnej poisťovne
	IČO:	30807484
	DIČ:	2020592332
	IČ DPH:	SK2020592332
	Bankové spojenie:	Štátna pokladnica
	IBAN:	SK40 8180 0000 0070 0016 4314
	SWIFT:	SPSRSKBA

(ďalej ako „*Objednávateľ*“)

a

2.	**Poskytovateľ:**	**CRIF – Slovak Credit Bureau, s.r.o**
	Sídlo:	Mlynské nivy 14, 821 09 Bratislava
	Štatutárny orgán:	Ing. Ján Budinský, konateľ Mgr. Petr Kučera, konateľ Natalia Shchelovanova, konateľ
	IČO:	35886013
	DIČ:	2021842042
	IČ pre DPH:	SK2021842042
	Bankové spojenie:	[illegible]
	IBAN:	
	SWIFT:	

Zapísaný v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sro, vložka č. 31737/B.

(ďalej ako „*Poskytovateľ*“)

(Objednávateľ a Poskytovateľ jednotlivo ďalej ako „**Zmluvná strana**“ a spoločne ďalej ako „**Zmluvné strany**“)

Zmluvné strany sa dohodli na uzavretí tejto Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou, podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník, v znení neskorších predpisov (ďalej ako „**Zmluva**“).

Článok I
Preambula

1. [*Verejné obstarávanie*] Východiskovým podkladom na uzavretie tejto Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov je Výzva na priame rokovacie konanie a ponuka poskytovateľa zo dňa 22.11. 2024 predložená v rámci zadávania podlimitnej zákazky podľa § 110 ods. 6 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").

2. [*Vyhlásenia Zmluvných strán*] Zmluvné strany ku dňu uzavretia Zmluvy zhodne vyhlasujú, že sú spôsobilé Zmluvu uzatvoriť a plniť záväzky z nej vyplývajúce a že im nie je známa žiadna taká okolnosť, ktorá by mohla ohroziť plnenie povinností vyplývajúcich im zo Zmluvy. Osobitne Poskytovateľ vyhlasuje, že ku dňu uzavretia tejto Zmluvy:

   2.1 je ako partner verejného sektora zapísaný v registri partnerov verejného sektora v zmysle zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v platnom znení (ďalej ako „**zákon o RPVS**") za predpokladu, že mu povinnosť byť zapísaný v registri partnerov verejného sektora zo zákona o RPVS vyplýva a ktorého konečným užívateľom výhod zapísaným v registri partnerov verejného sektora nie je osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní,

   2.2 disponuje dostatočnými oprávneniami, technickými, personálnymi a expertnými kapacitami na riadne a včasné plnenie povinností vyplývajúcich mu zo Zmluvy,

   2.3 nemá uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní,

   2.4 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.

   Vyhlásenia a povinnosti podľa bodov 2.1 až 2.4 tohto článku sa v rovnakom rozsahu vzťahujú na všetkých subdodávateľov poskytovateľa, teda na Subdodávateľov spĺňajúcich kritériá povinného zápisu v registri partnerov verejného sektora podľa zákona o RPVS.

   Vzhľadom na tieto skutočnosti a vyhlásenia Poskytovateľa sa Zmluvné strany v slobodnej vôli a v súlade s platnými právnymi predpismi rozhodli uzatvoriť túto Zmluvu.

3. [*Vzťah Zmluvy a príloh*] Ustanovenia tejto Zmluvy majú prednosť pred ustanoveniami Príloh a v prípade akýchkoľvek rozporov medzi obsahom tejto Zmluvy a Príloh, platia prednostne ustanovenia tejto Zmluvy. Ak sa však úprava v tejto Zmluve nenachádza, platí úprava uvedená v Prílohách.

4. [*Pojmy*] Pojmy definované v Prílohách majú rovnaký význam aj v tejto Zmluve s tým, že pojmu „Poskytovateľ" zodpovedá v Prílohe č. 10 pojem „Dodávateľ" a v Prílohe č. 9 pojem „sprostredkovateľ" a pojmu „Objednávateľ" zodpovedá v Prílohe č. 9 a v Prílohe č. 10 pojem „prevádzkovateľ".

Článok II
Účel Zmluvy

1. Účelom tejto Zmluvy je technické zabezpečenie elektronickej komunikácie medzi bankami a Sociálnou poisťovňou potrebné pre procesy súvisiace so správnym výkonom.

Článok III
Predmet Zmluvy

1. [*Vymedzenie služieb*] Predmetom tejto Zmluvy je záväzok Poskytovateľa technicky zabezpečiť elektronickú komunikáciu medzi bankami a Sociálnou poisťovňou prostredníctvom IT riešenia (ďalej aj ako „predmet Zmluvy" alebo „služby"), a to v rozsahu, termínoch a spôsobom podľa Prílohy č. 2.
2. [*Špecifikácia*] Podrobná špecifikácia predmetu Zmluvy je uvedená v Prílohe č. 2 k tejto Zmluve.
3. [*Záväzok objednávateľa*] Záväzkom Poskytovateľa podľa bodu 1 tohto článku zodpovedá záväzok Objednávateľa zaplatiť Poskytovateľovi dohodnutú cenu.

Článok IV
Cena za predmet Zmluvy a platobné podmienky

1. [*Cena dohodou*] Cena za predmet Zmluvy je stanovená dohodou Zmluvných strán podľa zákona 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 Národnej rady Slovenskej republiky č. 18/1996 Z. z. o cenách v znení neskorších predpisov nasledovne:

   Cena za poskytované služby pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou podľa článku III bodu 1 tejto Zmluvy je dohodnutá ako **celková maximálna cena** za obdobie účinnosti tejto Zmluvy nasledovne:

cena bez DPH	105 000,-- EUR
20 % DPH	21 000,-- EUR
Cena s DPH	**126 000,-- EUR**

   (slovom: jednostodvadsaťšesťtisíc EUR s DPH)

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

2. [*Cenová kalkulácia*] Cenová kalkulácia tvorí Prílohu č. 3. V cene za predmet Zmluvy sú započítané všetky náklady Poskytovateľa spojené s plnením predmetu Zmluvy podľa požiadaviek Objednávateľa. Cenová kalkulácia je uvedená vrátane všetkých nákladov Poskytovateľa, t. j. vrátane všetkých zliav, daní, ciel, poplatkov, licenčných poplatkov, platieb vyberaných v rámci uplatňovania nesadzobných opatrení ustanovených osobitnými predpismi, ako aj iných nákladov súvisiacich s plnením predmetu Zmluvy. Poskytovateľ nie je oprávnený požadovať akúkoľvek inú úhradu za prípadné dodatočné náklady, ktoré si nezapočítal do ceny za predmet Zmluvy.
3. [*Platobné podmienky - služby*] Objednávateľ uhradí cenu dohodnutú v bode 1 tohto článku, za poskytované služby pri technickom zabezpečení elektronickej komunikácie medzi bankami a

Sociálnou poisťovňou podľa článku III bodu 1 tejto Zmluvy, na základe faktúry vystavenej Poskytovateľom v prvý mesiac účinnosti tejto Zmluvy. Podkladom k vystaveniu faktúry musí byť protokol o začatí poskytovania služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou podpísaný zodpovednými zástupcami oboch Zmluvných strán. Splatnosť faktúry je najneskôr do tridsať (30) dní odo dňa jej doručenia do podateľne Objednávateľa. Poskytovateľ sa zaväzuje predkladať objednávateľovi do desať dní od ukončenia predchádzajúceho štvrťroka protokol o paušálnej podpore, ktorý bude obsahovať evidenčný zoznam poskytnutých služieb technickej podpory a údržby podľa Prílohy č. 7 za predchádzajúci kalendárny štvrťrok.

4. [*Platobné podmienky - spoločné ustanovenia]* Zmluvné strany sa dohodli na bezhotovostnom platobnom styku bez zálohovej platby. 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. Poskytovateľ sa zaväzuje vystavenú faktúru zaslať listinne poštou a súčasne aj v textovo čitateľnom súbore vo formáte PDF elektronicky na e-mailovú adresu objednávateľa faktury@socpoist.sk, a to bezodkladne po jej vystavení. Takto predložená faktúra nesmie byť vo forme obrázku, ale musí byť strojovo čitateľná. 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.

5. [*Nedostatky faktúry*] V prípade, že faktúra vystavená Poskytovateľom nebude obsahovať všetky zákonom stanovené alebo zmluvne dohodnuté náležitosti alebo bude obsahovať nesprávne alebo neúplné údaje, Objednávateľ má právo takúto faktúru vrátiť v lehote splatnosti poskytovateľovi na jej doplnenie, resp. opravu a Poskytovateľ je povinný podľa charakteru nedostatku vystaviť novú, opravenú, resp. doplnenú faktúru s novou lehotou splatnosti. Poskytovateľ je povinný bezodkladne poslať opravenú alebo novú faktúru znovu aj v elektronickej podobe na uvedenú e-mailovú adresu Objednávateľa podľa bodu 4 tohto článku.

6. [*Platnosť ceny*] Cena za poskytované služby podľa článku III bodu 1. tejto Zmluvy je fixná počas celej doby platnosti tejto Zmluvy.

Článok V
Doba a miesto plnenia, trvanie Zmluvy

1. [*Začiatok plnenia*] Poskytovateľ sa zaväzuje plniť predmet Zmluvy od účinnosti Zmluvy.

2. [*Trvanie Zmluvy*] Zmluva sa uzatvára na dobu určitú, a to na dvanásť (12) mesiacov od účinnosti Zmluvy.

3 [*Miesto plnenia*] Poskytovateľ sa zaväzuje plniť Predmet Zmluvy **v sídle Objednávateľa**, ak táto Zmluva neustanovuje inak alebo ak nie je medzi Zmluvnými stranami písomne dohodnuté inak.

Článok VI
Zodpovednosť za kvalitu a záruka

1. [*Garancia kvality*] Poskytovateľ sa zaväzuje, že poskytované služby Poskytovateľom pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou budú Objednávateľovi poskytované v súlade a v rozsahu, v kvalite a za podmienok dohodnutých v tejto Zmluve a v jej prílohách.

Článok VII
Ukončenie zmluvného vzťahu

1. [*Spôsoby ukončenia Zmluvy*] Zmluva môže byť ukončená len vzájomnou dohodou Zmluvných strán, odstúpením od Zmluvy v prípadoch stanovených touto Zmluvou alebo z dôvodov ustanovených zákonom alebo výpoveďou.

2. [*Účinky odstúpenia od Zmluvy*] Odstúpenie od Zmluvy nadobúda účinnosť dňom doručenia písomného oznámenia o odstúpení druhej Zmluvnej strane. Odstúpenie od Zmluvy, ako aj jeho právne účinky sa spravujú ustanoveniami podľa § 344 a nasl. Obchodného zákonníka.

3. [*Dôvody odstúpenia s možnou zmluvnou pokutou*] Objednávateľ je oprávnený odstúpiť od Zmluvy v prípade podstatného porušenia Zmluvy zo strany Poskytovateľa, ktorým sa rozumie, ak:

   a) Poskytovateľ opakovane nedodrží dohodnuté reakčné a servisné doby, a to ani napriek predchádzajúcej písomnej výzve Objednávateľa, v ktorej Poskytovateľovi poskytol lehotu na nápravu,

   b) Poskytovateľ poruší niektoré záväzky podľa bodu 6.8 VPZ a Prílohy č. 9 a Prílohy č. 10 k tejto Zmluve,

   c) niektoré z vyhlásení Poskytovateľa uvedené v bodoch 2.1 až 2.4 článku I Zmluvy sa ukáže ako nepravdivé,

   d) Poskytovateľ poruší povinnosť mlčanlivosti podľa bodov 7.8 až 7.13 VPZ.

4. [*Odstúpenie od Zmluvy bez možnosti zmluvnej pokuty*] Objednávateľ má právo odstúpiť od Zmluvy aj v prípade, ak:

   a) na majetok Poskytovateľa je vyhlásený konkurz, exekúcia, je Poskytovateľovi povolená reštrukturalizácia, Poskytovateľ vstúpil do likvidácie, preruší alebo iným ako vyššie uvedeným spôsobom skončí svoju podnikateľskú činnosť,

   b) Poskytovateľ alebo jeho štatutárny zástupca je právoplatne odsúdený za trestný čin spáchaný v súvislosti s výkonom jeho činnosti alebo podnikaním,

   c) Poskytovateľ v procese verejného obstarávania je vyhlásený za subjekt, ktorý vážne porušil Zmluvu tým, že si neplní svoje zmluvné povinnosti,

   d) Poskytovateľ stratí právne predpoklady na riadne plnenie Zmluvy,

   e) Poskytovateľ poruší povinnosť podľa bodu 2.3 alebo 2.4 VPZ.

5. [*Odstúpenie od Zmluvy zo strany Poskytovateľa*] Poskytovateľ môže odstúpiť od Zmluvy, ak:

   a) Objednávateľ nesplní svoj finančný záväzok, napriek písomnej výzve Poskytovateľa, ani do šesťdesiat (60) dní odo dňa splatnosti, alebo

   b) Objednávateľ opakovane aj napriek písomnému upozorneniu hrubo porušuje svoje povinnosti zo Zmluvy.

6. Objednávateľ po odstúpení od Zmluvy ktoroukoľvek Zmluvnou stranou, ku dňu odstúpenia od Zmluvy potvrdí cenu všetkých dovtedy poskytnutých plnení.

7. [*Výpoveď Zmluvy*] Zmluvné strany majú právo vypovedať túto Zmluvu:

a) ak sa preruší, zruší alebo zanikne technické riešenie komunikácie medzi bankami a Objednávateľom, na ktoré sa viaže predmet tejto Zmluvy, a to ku dňu doručenia výpovede druhej Zmluvnej strane,

b) bez uvedenia dôvodu v trojmesačnej výpovednej lehote, ktorá začne plynúť prvým dňom mesiaca nasledujúcom po doručení výpovede druhej Zmluvnej strane,

c) za podmienok dohodnutých v tejto Zmluve a jej prílohách.

Článok VIII
Sankcie

1. [*Sankcie za nesplnenie Poskytovateľa*] V prípade, ak Poskytovateľ nedodrží dohodnuté reakčné a servisné doby dohodnuté v prílohe č. 2 k tejto Zmluve, Objednávateľ je oprávnený uplatniť si nárok na zmluvnú pokutu vo výške 100,00 EUR za každé jedno porušenie, ak sa Zmluvné strany nedohodnú inak.

2. [*Sankcie za omeškanie Objednávateľa*] V prípade omeškania Objednávateľa s úhradou faktúry Poskytovateľa je Poskytovateľ oprávnený požadovať od Objednávateľa úrok z omeškania maximálne vo výške určenej nariadením vlády č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení nariadenia vlády č. 303/2014 Z. z., a to od prvého dňa omeškania.

3. [Sankcie s možnosťou odstúpenia od Zmluvy] V prípade porušenia niektorej zo zmluvných povinností Poskytovateľa zakladajúcej právo Objednávateľa odstúpiť od Zmluvy podľa bodu 3 článku VII tejto Zmluvy má Objednávateľ právo účtovať Poskytovateľovi zmluvnú pokutu vo výške 2 000,00 EUR, slovom dvetisíc eur, a to za každé porušenie. Toto právo má Objednávateľ bez ohľadu na to, či od Zmluvy 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.

4. [*Splatnosť*] Sankcie podľa bodov 1 až 3 tohto článku sú splatné do pätnásť (15) dní odo dňa doručenia písomnej výzvy druhej Zmluvnej strane.

5. [*Započítanie*] Objednávateľ je oprávnený jednostranne znížiť (započítať) sumu na zaplatenie fakturovanú Poskytovateľom o súčet zmluvných pokút Poskytovateľa, ktoré sú splatné ku dňu zaplatenia faktúry. O dôvode a rozsahu zníženia fakturovanej sumy podľa predchádzajúcej vety Objednávateľ informuje Poskytovateľa v lehote splatnosti danej faktúry, ak je to možné.

Článok IX
Záverečné ustanovenia

1. Táto Zmluva sa uzatvára na dobu určitú, a to na 12 mesiacov odo dňa nadobudnutia účinnosti. Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch Zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky (ďalej len „CRZ“) dňom 08.12.2024. V prípade, ak táto Zmluva nebude zverejnená v CRZ najneskôr v deň predchádzajúci dňu 08.12.2024, Zmluvné strany berú na vedomie, že táto Zmluva nadobudne účinnosť dňom nasledujúcim po dni jej zverejnenia v CRZ.

2. Ak to z povahy záväzkov vyplýva, tieto medzi Zmluvnými stranami pretrvajú aj po uplynutí uvedenej doby, na ktorú je Zmluva uzatvorená.

3. Táto Zmluva je povinne zverejňovanou zmluvou v zmysle § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v platnom znení. Zmluvné strany berú na vedomie a súhlasia, že táto Zmluva, vrátane všetkých jej súčastí a príloh, bude zverejnená v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky. Zverejnenie Zmluvy sa nepovažuje za porušenie ani ohrozenie obchodného tajomstva a informácie označené v tejto Zmluve ako dôverné v zmysle § 271 ods. 1 Obchodného zákonníka sa nepovažujú za dôverné.

4. Túto Zmluvu je možné meniť počas jej trvania bez nového verejného obstarávania v súlade s ustanovením § 18 zákona o verejnom obstarávaní, len očíslovanými písomnými dodatkami podpísanými obidvoma Zmluvnými stranami; Zápis o zmene príloh č. 4, 5, 6 a 7 podľa Prílohy č. 8 sa považuje za dodatok.

5. Táto Zmluva je vyhotovená v štyroch (4) rovnopisoch, z ktorých dostane každá Zmluvná strana po dva (2) rovnopisy.

6. Každé ustanovenie tejto Zmluvy sa, pokiaľ je to možné, interpretuje tak, aby bolo účinné a platné podľa platných právnych predpisov. Pokiaľ by však niektoré ustanovenie tejto Zmluvy bolo podľa platných právnych predpisov nevymožiteľné alebo neplatné, nebude tým dotknutá platnosť alebo vymožiteľnosť ostatných ustanovení tejto Zmluvy, ktoré budú i naďalej záväzné a v plnom rozsahu platné a účinné. V prípade takejto nevymožiteľnosti alebo neplatnosti budú Zmluvné strany v dobrej viere rokovať, aby sa dohodli na zmenách resp. dodatkoch k tejto Zmluve, ktoré sú potrebné na naplnenie účelu Zmluvy, potrebných v súvislosti s predmetnou nevymožiteľnosťou alebo neplatnosťou.

7. Táto Zmluva vrátane všetkých jej príloh predstavuje úplnú dohodu Zmluvných strán o predmete tejto Zmluvy ku dňu jej uzavretia.

8. Neoddeliteľnou súčasťou tejto Zmluvy sú nasledovné prílohy:

   Príloha č. 1 - Všeobecné podmienky Zmluvy
   Príloha č. 2 - Opis predmetu Zmluvy
   Príloha č. 3 - Cenová kalkulácia
   Príloha č. 4 - Oprávnené osoby
   Príloha č. 5 - Vzor požiadavky pre hlásenie chýb
   Príloha č. 6 - Zoznam subdodávateľov
   Príloha č. 7 - Vzor protokolu o paušálnej podpore
   Príloha č. 8 - Zápis o zmene prílohy
   Príloha č. 9 - Sprostredkovateľská zmluva
   Príloha č. 10 - Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

9. Práva a povinnosti, ktoré vznikli na základe tejto Zmluvy, alebo v súvislosti s touto Zmluvou sa riadia zákonom č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky.

10. Zmluvné strany vyhlasujú, že sú si vedomé, že na riadne fungovanie elektronickej komunikácie medzi bankami a SP je nevyhnutné na zasielanie Žiadostí, Informácií a Príkazov postupovať v súlade so Zmluvou o elektronickej komunikácii a technickej podpore uzatvorenej medzi Zmluvnými stranami a Slovenskou bankovou asociáciou, Mýtna 48, 811 07 Bratislava, v mene bánk a pobočiek zahraničných bánk, ktorá nadobudla účinnosť dňa 24.06.2017, respektíve v súlade so zmluvou, ktorá ju v budúcnosti nahradí.

11. Zmluvné strany tejto Zmluvy po jej prečítaní vyhlasujú, že súhlasia s jej obsahom a prílohami, ktoré tvoria súčasť tejto Zmluvy. Táto Zmluva bola uzavretá podľa skutočnej a slobodnej vôle Zmluvných strán.

V Bratislave dňa 10 -12- 2024

Za Objednávateľa:

.....

Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

V Bratislave dňa 10 -12- 2024

Za Poskytovateľa:

.....

Ing. Ján Budinský
konateľ
CRIF – Slovak Credit Bureau, s.r.o

.....

Mgr. Petr Kučera
konateľ
CRIF – Slovak Credit Bureau, s.r.o

.....

Natalia Shchelovanova
konateľ
CRIF – Slovak Credit Bureau, s.r.o

Príloha č. 1 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

VŠEOBECNÉ PODMIENKY ZMLUVY
(ďalej ako „VPZ")

Článok 0 Vymedzenie pojmov a skratky

Skratka / Pojem	Vysvetlenie
DU	Dátový uzol Bánk
DUA	Aplikačný server DU, umožňuje komunikáciu Bánk cez webovú službu
DUD	Databáza DU v ktorej sú uložené prenášané správy (t. j. Žiadosti, Príkazy, Informácie), certifikáty s verejnými kľúčmi a prístupové oprávnenia klientov
Reakčná doba	doba od momentu odoslania hlásenia objednávateľom, počas ktorej poskytovateľ vykoná prvotnú analýzu požiadavky. Detailné definovanie je v prílohe č. 2 k tejto Zmluve.
SP	Dátový uzol Sociálnej poisťovne
SPA	Aplikačný server Sociálnej poisťovne, umožňuje komunikáciu cez webovú službu
Subdodávateľ	Zmluvný partner Poskytovateľa, prostredníctvom ktorého Poskytovateľ zabezpečuje plnenie časti predmetu Zmluvy
SPD ÚP	Databáza Sociálnej poisťovne, slúži na výmenu dát medzi zónami Sociálnej poisťovne a dátovým uzlom Bánk
ÚPVS	Ústredný portál verejnej správy
Zmluva/zmluva	Zmluva o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou

Článok 1 Oznámenia, správy a písomná komunikácia

1.1. Zmluvné strany sa dohodli, že akékoľvek oznámenia druhej Zmluvnej strane budú doručené na adresy uvedené v záhlaví Zmluvy.

1.2. Objednávateľ a Poskytovateľ sa zaväzujú bezodkladne oznámiť druhej Zmluvnej strane akúkoľvek zmenu svojich kontaktných alebo korporátnych údajov.

1.3. Každá správa, súhlas, schválenie alebo rozhodnutie, ktoré sa požadujú na základe Zmluvy, sa vyhotovia, pokiaľ nie je stanovené inak, v písomnej podobe. Odosielateľ akejkoľvek písomnej správy môže požadovať písomné potvrdenie príjemcu.

1.4. Písomnosti odoslané druhej Zmluvnej strane na adresu jej sídla uvedenú v Zmluve alebo neskôr písomne oznámenú, sa považujú za prevzaté druhou Zmluvnou stranou aj v deň odmietnutia prevzatia zásielky druhou Zmluvnou stranou vyznačeným poštou alebo v posledný deň úložnej lehoty zásielky, aj keď si ju druhá Zmluvná strana neprevzala.

1.5. Poskytovateľ oznámi Objednávateľovi pri podpise Zmluvy informácie k identifikácii bankového účtu (IBAN), na ktorý má Objednávateľ posielať platby podľa Zmluvy a aj akúkoľvek zmenu týchto údajov počas obdobia účinnosti tejto Zmluvy.

1.6. Jazyk Zmluvy a celej písomnej komunikácie medzi Objednávateľom a Poskytovateľom, ako aj vo vzťahu k tretím osobám je slovenský jazyk.

1.7. Kontaktné adresy pre písomnú komunikáciu a Oprávnené osoby Zmluvných strán sú uvedené v Prílohe č. 4 Zmluvy.

1.8. Všetky dokumenty a informácie, či už písomné alebo ústne, si Zmluvné strany poskytujú len na použitie na plnenie Zmluvy. Bez predchádzajúceho písomného súhlasu Objednávateľa nie je Poskytovateľ oprávnený používať tieto dokumenty a informácie na iné účely ako na účely zákazky realizovanej na základe Zmluvy. Poskytovateľ uchováva úplné a presné účtovné doklady o plneniach poskytovaných na základe tejto Zmluvy a pracovné výkazy, pokiaľ ide o služby, po dobu päť (5) rokov od vykonania úprav a zmien alebo skončenia Zmluvy.

1.9. Oprávnená osoba Poskytovateľa na požiadanie písomne poskytne projektovému manažérovi Objednávateľa, alebo osobe, ktorú splnomocní Objednávateľ, akékoľvek informácie vzťahujúce sa na plnenie Zmluvy.

Článok 2 Postúpenie práv a započítanie pohľadávok

2.1 Žiadna zo Zmluvných strán nie je oprávnená bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany postúpiť akékoľvek svoje práva alebo povinnosti vyplývajúce zo Zmluvy na tretiu stranu; tým nie je dotknuté oprávnenie Objednávateľa previesť správu pohľadávok štátu v zmysle príslušných všeobecne záväzných právnych predpisov (najmä § 10 zákona 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).

2.2 V prípade porušenia povinnosti podľa bodu 2.1. bude Zmluva o postúpení zmluvných práv alebo povinností neplatná, resp. neúčinná voči druhej Zmluvnej strane.

2.3 V prípade porušenia povinnosti podľa bodu 2.1. jednou zo Zmluvných strán, je druhá Zmluvná strana oprávnená od Zmluvy odstúpiť, a to s účinnosťou odstúpenia ku dňu, kedy bolo písomné oznámenie o odstúpení od Zmluvy doručené druhej Zmluvnej strane.

2.4 Poskytovateľ nie je oprávnený jednostranne započítať akúkoľvek svoju pohľadávku voči Objednávateľovi s pohľadávkou Objednávateľa voči Poskytovateľovi.

Článok 3 Subdodávka

3.1. Poskytovateľ je oprávnený plniť Zmluvu aj prostredníctvom svojich Subdodávateľov.

3.2. Poskytovateľ zodpovedá za plnenie Zmluvy o subdodávke Subdodávateľom tak, ako keby plnenie realizované na základe takejto Zmluvy realizoval sám.

3.3. Poskytovateľ je povinný pri uzatvorení Zmluvy uviesť zoznam Subdodávateľov, ktorý obsahuje údaje o všetkých známych Subdodávateľoch Poskytovateľa v čase uzatvorenia Zmluvy a údaje o osobe oprávnenej konať za Subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Zoznam Subdodávateľov tvorí prílohu č. 6 k Zmluve a obsahuje okrem uvedených údajov podiel plnenia zo Zmluvy v % a stručný opis časti Zmluvy, ktorá bude predmetom subdodávky.

3.4. Poskytovateľ je povinný písomne oznámiť Objednávateľovi akúkoľvek zmenu údajov o Subdodávateľovi, ktorý je uvedený v prílohe č. 6 k Zmluve najneskôr do päť (5) pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví Zmluvy.

3.5. V prípade zmeny Subdodávateľa je Poskytovateľ najneskôr tri (3) pracovné dni pred zmenou subdodávateľa povinný písomne oznámiť Objednávateľovi údaje o navrhovanom novom Subdodávateľovi a o osobe oprávnenej konať za Subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia.

3.6. Zmena Subdodávateľa sa vykoná zápisom o zmene Prílohy č. 6, ktorý nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch Zmluvných strán a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky (ďalej len „register"); to primerane platí aj o zmene Prílohy č. 4, 5 a 7 pričom vzor zápisu o zmene týchto príloh tvorí Prílohu č. 8. Osobami oprávnenými konať vo veciach zmeny Prílohy č. 4, 5, 6 a 7 podľa Prílohy č. 8 sú:

za Poskytovateľa: výkonný riaditeľ

za Objednávateľa: *riaditeľ sekcie stratégie a informatiky.*

3.7. Pre zamedzenie pochybností, ak subdodávateľ Poskytovateľa v rámci plnení povinností podľa tejto Zmluvy vytvorí akýkoľvek predmet duševného vlastníctva, tento sa nepovažuje za Dielo tretej strany, pričom Poskytovateľ je povinný zabezpečiť a zodpovedá za to, aby táto skutočnosť nemala žiadny negatívny vplyv na výlučné práva Objednávateľa v súlade s bodmi 7.1 až 7.13 VPZ.

Článok 4 Organizácia práce

4.1. Poskytovateľ sa zaväzuje dodržiavať všetky technické a bezpečnostné predpisy, zároveň zabezpečí poučenie svojich zamestnancov o všeobecných predpisoch bezpečnosti a ochrany zdravia pri práci, zodpovedá za nich a znáša prípadné dôsledky porušenia týchto predpisov. S vnútornými predpismi Objednávateľa zamestnancov Poskytovateľa preukázateľne písomne oboznámi Objednávateľ. Poskytovateľ je povinný riadiť sa pokynmi osoby zodpovednej za informačnú bezpečnosť menovanú Objednávateľom.

4.2. V prípade, ak v areáli Objednávateľa dôjde k pracovnému úrazu zamestnanca Poskytovateľa z dôvodu porušenia technických a bezpečnostných predpisov, s ktorými bol oboznámený Objednávateľom, zodpovedá v plnom rozsahu za následky výlučne Poskytovateľ.

4.3. Zamestnanci Poskytovateľa sú povinní dodržiavať zásady všeobecnej spôsobilosti tretích osôb vstupujúcich do priestorov Objednávateľa a iné interné predpisy o výkone a podmienkach prác

dodávateľských organizácií, s ktorými budú vopred preukázateľne písomne oboznámení Objednávateľom.

Článok 5 Povinnosti Objednávateľa

5.1 Objednávateľ poskytne na požiadanie Poskytovateľovi všetky informácie, ktoré má k dispozícii, ak sú potrebné na realizáciu plnení podľa Zmluvy.

5.2 Objednávateľ je povinný poskytnúť Poskytovateľovi pri plnení predmetu Zmluvy nevyhnutnú súčinnosť; povinnosť Poskytovateľa podľa bodu 6.2 VPZ tým nie je dotknutá.

Článok 6 Povinnosti Poskytovateľa

6.1 Poskytovateľ je povinný pri plnení Zmluvy postupovať na vysokej profesionálnej úrovni, so všetkou odbornou starostlivosťou, ktorú možno pri poctivom obchodnom styku od Poskytovateľa požadovať. Poskytovateľ sa zaväzuje dodržiavať pri plnení Zmluvy všetky relevantné všeobecne záväzné právne predpisy.

6.2 Poskytovateľ je povinný plniť riadne a včas svoje povinnosti podľa Zmluvy a dodržiavať pokyny Objednávateľa. Poskytovateľ je povinný upozorniť Objednávateľa bez zbytočného odkladu na nedostatočnú súčinnosť Objednávateľa, nevhodnú povahu pokynov, ak Poskytovateľ mohol túto nevhodnosť, resp. rozpor zistiť pri vynaložení všetkej odbornej starostlivosti. Ak nedostatočná súčinnosť Objednávateľa, nevhodné alebo so Zmluvou a/alebo všeobecne záväznými právnymi predpismi rozporné pokyny prekážajú v riadnom plnení Zmluvy, je Poskytovateľ povinný jej splnenie v nevyhnutnom rozsahu prerušiť do doby poskytnutia potrebnej súčinnosti Objednávateľa, zmeny predmetného pokynu alebo do doby písomného oznámenia, že Objednávateľ trvá na plnení Zmluvy podľa daných pokynov. O dobu, po ktorú bolo potrebné Zmluvu prerušiť, sa predlžuje lehota určená na jej splnenie.

6.3 Poskytovateľ je povinný poskytovať služby v súlade so Zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a vyhláškou 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, účinnými ku dňu riadneho prebrania predmetu Zmluvy a aktuálne vydanou a platnou Metodikou pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti ako aj v súlade s internými predpismi Objednávateľa.

6.4 Poskytovateľ, ktorý riadne splnil povinnosť uvedenú v bode 6.2, nezodpovedá za nemožnosť splnenia Zmluvy alebo za vady poskytnutého plnenia spôsobené nevhodnými alebo so Zmluvou a/alebo všeobecne záväznými právnymi predpismi rozpornými pokynmi, ak Objednávateľ na nich pri plnení Zmluvy písomne trval.

6.5 Poskytovateľ je povinný pri plnení Zmluvy dodržiavať zásady poctivého obchodného styku a zdržať sa akéhokoľvek konania, ktoré by mohlo byť posúdené ako konanie v rozpore s dobrými mravmi hospodárskej súťaže.

6.6 Poskytovateľ je povinný zdržať sa pri plnení Zmluvy akéhokoľvek konania, ktoré by mohlo v dôsledku konfliktu záujmov spochybniť jeho nestrannosť a ohroziť naplnenie účelu Zmluvy.

6.7 Všetky podklady poskytnuté Poskytovateľovi a evidované údaje musia byť po ukončení obchodných vzťahov bez vyzvania odovzdané Objednávateľovi alebo podľa jeho rozhodnutia vymazané alebo skartované. Táto povinnosť sa vzťahuje aj na vyhotovené kópie. Toto ustanovenie neplatí v prípade vzájomných zmlúv a Projektovej dokumentácie medzi

Zmluvnými stranami, ktoré ale naďalej nesmú byť bez súhlasu Objednávateľa sprístupnené tretej strane.

6.8 Poskytovateľ ako aj prípadní subdodávatelia sú povinní zabezpečiť ochranu osobných údajov v zmysle 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) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a kybernetickú bezpečnosť podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a podľa prílohy č. 9 a prílohy č. 10, ktoré sú neoddeliteľnou súčasťou tejto Zmluvy.

Článok 7 Práva duševného vlastníctva a povinnosť mlčanlivosti

7.1 [*Účel*] Poskytovateľ a Objednávateľ sa dohodli na tejto transparentnej úprave vzájomných práv a povinností vo vzťahu k duševnému vlastníctvu a licenčným podmienkam v súvislosti so Zmluvou za účelom zabezpečenia práv na použitie IT riešenia v prospech Objednávateľa, právnej istoty Zmluvných strán.

7.2 [*Predmety duševného vlastníctva*] Pre účely Zmluvy sa za predmety duševného vlastníctva považujú akékoľvek predmety spôsobilé byť predmetom duševného vlastníctva, najmä autorské dielo, počítačový program, databáza v zmysle zákona č. 185/2015 Z. z. Autorský zákon, vynález, úžitkový vzor, dizajn (vrátane digitálneho, napr. UI (používateľské rozhranie), GUI (Grafické používateľské rozhranie) alebo akýkoľvek iný výsledok tvorivej duševnej činnosti v zmysle v zmysle osobitných predpisov, ako aj know-how, ktoré vytvoril Poskytovateľ alebo ním poverená tretia osoba (napr. subdodávateľ, SZČO /Samostatne zárobkovo činná osoba/ a pod.) či zamestnanec Poskytovateľa na splnenie alebo v rámci plnenia povinností a záväzkov Poskytovateľa vyplývajúcich z alebo súvisiacich so Zmluvou a to bez ohľadu na to, či ide o analýzy, koncepcie, štúdie, návrhy softwarových systémov, návrhy testov a postupov pre testy softwarových systémov, analýzy požiadaviek, funkčné a technické návrhy, podklady, strojové a zdrojové kódy, procesné modely, bezpečnostný projekt a pod., ďalej ako „Predmety duševného vlastníctva“) ku ktorým Poskytovateľ poskytuje nevýhradnú licenciu na používanie v súlade s touto Zmluvou.

7.3 [*Vyhlásenia Poskytovateľa*] Poskytovateľ vyhlasuje a zodpovedá za to, že ku dňu poskytnutia nevýhradnej licencie na použitie IT riešenia alebo jeho časti:

7.3.1 Predmet duševného vlastníctva ani žiadna jeho časť nemá žiadne právne vady, nie je zaťažený právami tretích osôb a ani ich neporušuje; tým nie je dotknuté dojednanie o dielach tretích strán (bod 7.6 VPZ),

7.3.2 má s osobami, ktoré sa akýmkoľvek spôsobom prípadne podieľali na vzniku Predmetu duševného vlastníctva, vysporiadané všetky práva a súvisiace nároky týchto osôb, resp. tieto práva a nároky vysporiada na vlastný účet; tým nie je dotknuté dojednanie o dielach tretích strán (bod 7.6 VPZ),

7.4 [*Základné oprávnenia Objednávateľa*] Ak v bode 7.2 a 7.3 nie je uvedené inak, Objednávateľ je oprávnený Práva duševného vlastníctva vykonávať a používať v najväčšom možnom prípustnom rozsahu s súlade so Zmluvou.

7.5 Poskytovateľ udeľuje Objednávateľovi (i) podľa § 70 Autorského zákona nevýhradnú licenciu na použitie IT riešenia spôsobom uvedeným v Zmluve a potrebným pre vykonávanie činností Objednávateľa a naplnenia účelu Zmluvy a účelu podľa 7.1 VPZ.

7.6 [*Diela tretích strán Open source, podporné a konverzné programy*] Zmluvné strany berú na vedomie a súhlasia s tým, že k jednotlivým plneniam (vrátane ich akýchkoľvek súčastí zahŕňajúcich tiež software) poskytnutým Poskytovateľom Objednávateľovi podľa Zmluvy na základe licencií udelených Poskytovateľovi tretími osobami, ktoré k nim majú a/alebo vykonávajú autorské práva a/alebo práva priemyselného a/alebo iného duševného vlastníctva a/alebo inak poskytnutých Poskytovateľovi týmito osobami alebo Open source software, Poskytovateľ udeľuje Objednávateľovi právo na ich používanie v súlade, v rozsahu, spôsobom nevyhnutným na plnenie tejto Zmluvy.

Predchádzajúca veta:

7.6.1 sa nevzťahuje na prípady, ak licenčné alebo iné podmienky uvedených tretích strán alebo za podmienky používania a úpravy Open source software výslovne ustanovujú inak;

7.6.2 nevzťahuje na cenu licencií, tzn. pre Zmluvné strany je záväzná cena licencie k dielu tretej strany uvedená v Zmluve, ak medzi Zmluvnými stranami nie je písomne dohodnuté inak; tým nie je dotknutá povinnosť Zmluvných strán dodržiavať obmedzenia a limity uvedené v § 18 zákona o verejnom obstarávaní.

Poskytovateľ na požiadanie Objednávateľa predloží Objednávateľovi kópiu predmetných licenčných alebo iných podmienok tretích strán alebo podmienky používania a úpravy Open source software. Poskytovateľ týmto potvrdzuje, že je oprávnený poskytnúť Objednávateľovi oprávnenia a súhlasy v zmysle vyššie uvedeného, a že tým nedochádza k zásahu do práv tretích osôb 6.

7.7 [*Povinnosť súčinnosti Poskytovateľa*] Poskytovateľ je povinný umožniť výkon práv Objednávateľa podľa tohto článku VPZ, aby bol v maximálne miere naplnený účel tohto článku VPZ a Zmluvy a na požiadanie Objednávateľa poskytnúť adekvátne vysvetlenie, poučenie, upozornenie, zaškolenie Objednávateľom označeným zamestnancom Objednávateľa či tretím osobám. Poskytovateľ na požiadanie Objednávateľa poskytne súčinnosť proti nárokom, žalobám a konaniam začatým tretími stranami v prípade, ak tretia strana uplatní nároky resp. podá žalobu proti Objednávateľovi v súvislosti s Predmetmi duševného vlastníctva.

7.8 [*Povinnosť mlčanlivosti*] Zmluvné strany vyhlasujú za dôverné a zaväzujú sa rešpektovať:

7.8.1 všetky dôverné skutočnosti, obchodné a technické informácie, týkajúce sa alebo súvisiace so Zmluvou a jej predmetom, vrátane informácii podliehajúcich osobitnému zákonnému režimu, najmä podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre v platnom znení a zákona č. 95/2019 Z. z. o ITVS a o zmene a doplnení niektorých zákonov v platnom znení;

7.8.2 predmety a práva duševného vlastníctva;

7.8.3 osobné údaje tretích osôb;

7.8.4 údaje a informácie bez ohľadu na formu ich vyjadrenia, z ktorých označenia je jednoznačné, že majú utajovanú povahu a nie sú bežne dostupné;

7.8.5 akékoľvek údaje a informácie, ktoré s prihliadnutím na ich obsah, formu alebo kontext sú spôsobilé poškodiť dobré meno Objednávateľa, alebo Poskytovateľa jeho zmluvných partnerov alebo klientov, za predpokladu, že tieto subjekty majú výslovný alebo rozumne predpokladateľný záujem na utajení týchto informácií

(ďalej ako „dôverné informácie").

7.9 [*Negatívne vymedzenie*] Za dôverné sa nepovažujú a ani za ne nemôže Objednávateľ vyhlásiť tie informácie, ktoré sú bežne prístupné v príslušných odborných alebo obchodných kruhoch či

publikáciách, alebo ktoré Poskytovateľ získal (nadobudol) legálne z iných zdrojov a nejde pritom o dôverné informácie podľa bodu 7.8.3 alebo 7.8.5 VPZ. Ak sa informácie podľa predchádzajúcej vety vzťahujú len na časť dôvernej informácie, zaobchádzanie so všetkými jej ostatnými časťami spadá pod režim dôverných informácií podľa VPZ. Povinnosť mlčanlivosti Objednávateľa sa netýka jeho povinnosti sprístupňovania informácií podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a ani výkonu práv duševného vlastníctva vyplývajúcich z bodov 7.1 až 7.8 VPZ, ktoré majú bezvýnimočnú a bezpodmienečnú prednosť pred povinnosťou mlčanlivosti.

7.10 [*Základná povinnosť*] Zmluvné strany sú povinné dôverné informácie chrániť pred vyzradením, zneužitím, poškodením, zničením, stratou alebo odcudzením.

7.11 [*Doba trvania povinnosti*] Zmluvné strany sa zaväzujú, že počas trvania zmluvného vzťahu podľa Zmluvy, ako aj po dobu desať (10) rokov po skončení tohto zmluvného vzťahu, bude držať dôverné informácie v prísnej tajnosti a zabezpečí, aby nemohlo dôjsť k ich sprístupneniu tretím osobám, alebo aby nedošlo k akémukoľvek inému zneužitiu. V prípade, ak niektorá Zmluvná strana alebo jeho zmluvný partner či klient sprístupní druhej Zmluvnej strane dôverné informácie, ktoré tvoria predmety alebo práva duševného vlastníctva alebo s nimi priamo súvisia, povinnosť mlčanlivosti vo vzťahu k takýmto dôverným informáciám trvá tridsať (30) rokov po skončení zmluvného vzťahu.

7.12 [*Limitované oprávnenie*] Zmluvné strany sú oprávnené použiť dôverné informácie výhradne na účely riadneho plnenia úloh a povinností vyplývajúcich zo Zmluvy. K akémukoľvek sprístupneniu dôverných informácií tretím osobám (okrem výslovne označených osôb) je príslušná Zmluvná strana povinná vopred získať predchádzajúci výslovný písomný súhlas druhej Zmluvnej strany. ostávajú aj po uplynutí tejto doby zachované v súlade s týmto článkom VPZ.

7.13 [*Kópie a materiály*] Poskytovateľ berie na vedomie a zaväzuje sa, že v prípade ak budú poskytnuté akékoľvek materiály či dokumenty bez ohľadu na ich formu obsahujúce dôverné informácie zostávajú vo vlastníctve Objednávateľa (alebo iných oprávnených osôb). Poskytovateľ nie je bez vopred udeleného výslovného písomného súhlasu Objednávateľa oprávnený ich kopírovať. Ak nie je výslovne uvedené inak, dispozičné práva k týmto materiálom neprechádzajú na Poskytovateľa a tento je povinný vrátiť Objednávateľovi všetky relevantné materiály na vyzvanie, alebo pri skončení zmluvného vzťahu podľa Zmluvy, a to bez zbytočného odkladu.

Článok 8 Zodpovednosť za škodu a okolnosti vylučujúce zodpovednosť

8.1 Poskytovateľ sa zaväzuje nahradiť Objednávateľovi škodu, ktorú preukázateľne spôsobil pri plnení Zmluvy, maximálne však do výšky maximálnej ceny za predmet Zmluvy.

8.2 Zmluvné strany majú povinnosť sa vzájomne informovať o vzniku okolností vylučujúcich zodpovednosť. Zmluvné strany nezodpovedajú za škodu v prípade, ak nastali okolnosti vylučujúce ich zodpovednosť. Za okolnosti vylučujúce zodpovednosť sa považuje prekážka, ktorá nastala nezávisle od vôle povinnej Zmluvnej strany a bráni jej v splnení jej povinností, ak nie je možné rozumne predpokladať, že by povinná Zmluvná strana túto prekážku alebo jej následky odvrátila alebo prekonala a ďalej, že by v dobe vzniku prekážku predvídala. Zodpovednosť nevylučuje prekážka, ktorá vznikla najprv v dobe, keď povinná strana bola v oneskorení/omeškaní s plnením svojej povinnosti alebo vznikla z jej hospodárskych pomerov. Účinky okolností vylučujúcich zodpovednosť sú obmedzené len na dobu, pokiaľ trvá prekážka, s ktorou sú tieto povinnosti spojené.

8.3 Ak okolnosti vylučujúce zodpovednosť pretrvávajú po dobu viac ako stoosemdesiat (180) dní, nehľadiac na predĺženie lehoty na splnenie Zmluvy, ktoré možno Poskytovateľovi z tohto dôvodu udeliť, ktorákoľvek zo Zmluvných strán je oprávnená s jednomesačnou výpovednou lehotou vypovedať Zmluvu.

8.4 V prípade, že sa vyskytnú udalosti, ktoré jednej alebo obom Zmluvným stranám čiastočne alebo úplne neumožnia plnenie ich povinností podľa Zmluvy, sú Zmluvné strany povinné sa o tom bez zbytočného omeškania informovať a spoločne podniknúť kroky k ich prekonaniu. Nesplnenie tejto povinnosti zakladá nárok na náhradu škody pre tú stranu, ktorá sa porušenia Zmluvy v tomto bode nedopustila.

Článok 9 Urovnanie sporov

9.1 Zmluvné strany sa zaväzujú vynaložiť všetko úsilie, aby urovnali akýkoľvek spor vzťahujúci sa na Zmluvu, ktorý medzi nimi vznikne.

9.2 V prípade sporu si Zmluvné strany navzájom písomne oznámia svoje stanovisko k danému sporu a akékoľvek riešenie, ktoré považujú za prijateľné. Ak to jedna zo Zmluvných strán považuje za užitočné, Zmluvné strany sa stretnú a pokúsia sa daný spor urovnať.

9.3 Zmluvná strana odpovie na žiadosť druhej Zmluvnej strany o mimosúdne urovnanie sporu do tridsať (30) dní od prijatia takejto žiadosti. Maximálna lehota stanovená na dosiahnutie mimosúdneho urovnania sporu je stodvadsať (120) dní odo dňa prijatia žiadosti o mimosúdne urovnanie sporu. Ak sa v tejto lehote urovnanie sporu nedosiahne, môže sa každá Zmluvná strana obrátiť na príslušný súd.

Príloha č. 2 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

Opis predmetu zákazky/Zmluvy

Názov predmetu zákazky: **Poskytovanie služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou**

1. Charakteristika

Služba „overovanie údajov klientov Bánk" pre elektronickú komunikáciu medzi Sociálnou poisťovňou (ďalej len „SP") a bankami je v rámci IT (informačných technológií) riešenia (Systému) pre elektronickú komunikáciu medzi SP a bankami logicky aj fyzicky rozčlenená do dvoch celkov:

- Dátový uzol SP, prostredníctvom ktorého je zabezpečené pripojenie a elektronická komunikácia zo strany SP.

- Dátový uzol bánk, do ktorého sú pripojené všetky Banky, ktoré sa aktívne zúčastňujú projektu.

2. Technická špecifikácia cieľového riešenia

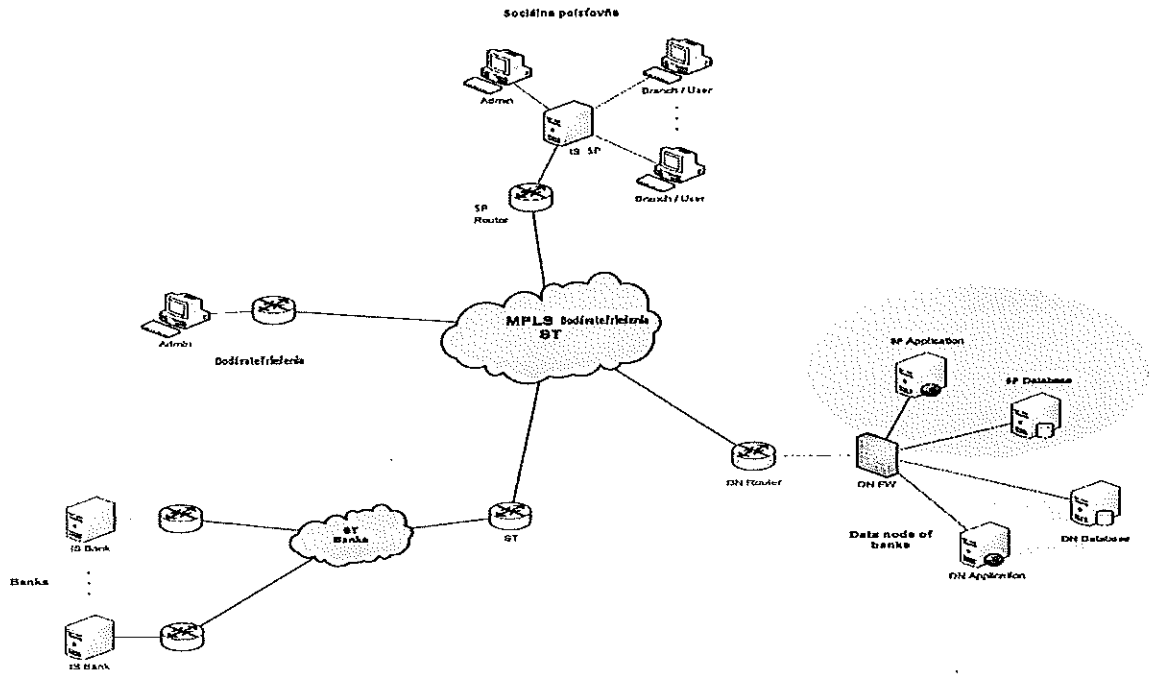
SP, ktorá bude využívať IT riešenie pre elektronickú komunikáciu medzi SP a bankami, bude pripojená k Dátovému uzlu SP prevádzkovanému poskytovateľom riešenia.
Pre pripojenie bude využívať privátnu linku. Po pripojení a autentifikácii prihlasovacích údajov SP zasiela prostredníctvom zabezpečeného pripojenia (HTTP - Hypertextový prenosový protokol) so šifrovaným SOAP (Simple Object Access Protocol) obsahom na Dátový uzol SP Žiadosť alebo Príkaz Banke, alebo viacerým určeným Bankám, v štruktúre podľa Prílohy č. 1 a Prílohy č. 2 k tejto prílohe č. 2 k Zmluve.

Dátový uzol SP spracuje Žiadosť alebo Príkaz a automaticky odošle SP potvrdenie prevzatia, prípadne chybovú správu. Žiadosť a Príkaz sú následne prenesené do Dátového uzla bánk.

Banka bude pripojená do Dátového uzla bánk už existujúcou privátnou linkou používanou pre komunikáciu so Spoločným registrom bankových informácií (ďalej len „SRBI").
Po pripojení na Dátový uzol bánk a autentifikácii prihlasovacích údajov banky si Banka prostredníctvom zabezpečeného pripojenia vyzdvihne Žiadosť alebo Príkaz zaslaný SP.

Následne po spracovaní Žiadosti odosiela obdobným spôsobom Informáciu ako odpoveď na Žiadosť na Dátový uzol bánk. Táto Informácia je presunutá na Dátový uzol SP, kde je sprístupnená cieľovému adresátovi, ktorý si ju po pripojení vyzdvihne. Týmto spôsobom sú SP sprístupnené všetky Informácie od Banky, alebo Bánk, ktorým adresoval Žiadosť.

3. Architektúra cieľového stavu



SP Dátový uzol SP
SPA aplikačný server SP, umožňuje komunikáciu cez webovú službu
SPD databáza SP, slúži na výmenu dát medzi zónami SP a DU
DU Dátový uzol Bánk
DUA aplikačný server DU, umožňuje komunikáciu Bánk cez webovú službu
DUD databáza DU v ktorej sú uložené prenášané správy (t. j. Žiadosti, Príkazy, Informácie), certifikáty s verejnými kľúčmi a prístupové oprávnenia klientov

4. Možnosti pripojenia klientov

Klientom je spoločnosť (SP alebo Banka) jednoznačne identifikovaná menom, heslom a certifikátom. Každý klient má pridelený jeden prístup.

Sociálna poisťovňa
Informačný systém (IS) SP komunikuje cez privátnu linku s webovou službou HTTP protokolom so šifrovaným SOAP obsahom a umožňuje pripojenie jednotlivých pobočiek/užívateľov

Banka
IS Banky komunikuje cez privátnu linku s webovou službou Dátového uzla HTTP protokolom so šifrovaným SOAP obsahom.

5. Bezpečnostné aspekty

Výmena dát medzi zónami „Dátový uzol SP" (SP) a „Dátový uzol bánk" (DU) prebieha jednosmerne zo strany DU. Komunikačná služba DUA sa dopytuje na nové požiadavky SP a ukladá zasielané správy. Neexistuje žiadny aktívny prístup smerom SP – DU.

Klient je pri komunikácii vždy overený prihlasovacím menom, heslom a certifikátom.
Komunikácia je zabezpečená - zasielané dáta sú šifrované od chvíle vytvorenia spojenia klient – server a nie je možné ich zneužiť.
Poskytovateľ sa bude riadiť počas celého cyklu predmetu zákazky okrem platnej legislatívy aj internými predpismi Objednávateľa a bude dodržiavať Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni.

6. Certifikáty

Každý účastník elektronickej komunikácie (vrátane serverov SPA, DUA, DUD) používa vlastný certifikát, ktorý je vydaný a ktorého podmienky používania sú definované na základe samostatnej zmluvy medzi účastníkmi elektronickej komunikácie a certifikačnou autoritou. Za bezpečnú manipuláciu a ochranu privátneho kľúča je zodpovedný jeho držiteľ, rovnako ako zodpovedá za prípadné škody spôsobené porušením tejto povinnosti.

Certifikáty zabezpečujú:

- dôvernosť informácií - neautorizované subjekty nemajú možnosť prístupu k dôverným informáciám
  - autentifikácia klienta
  - šifrovanie obsahu správ
- integritu - informácie sú zabezpečené voči neautorizovanej modifikácii digitálnym podpisom založeným na PKI (Public Key Infrastructure) (ďalej len „digitálny podpis").

Klient môže použiť samostatné certifikáty pre autentifikáciu počas nadväzovania spojenia a podpisovanie/šifrovanie obsahu správ.

Systém umožňuje:

- evidenciu certifikátov s verejnými kľúčmi,
- zaevidovanie nového certifikátu vo fáze obnovy,
- označenie certifikátu ako neplatného na žiadosť klienta (technické problémy, diskreditácia certifikátu).

Certifikáty s verejnými kľúčmi sú evidované na DUD a replikované na SPD pre zabezpečenie funkcií:

- zaslanie jednoznačného identifikátora certifikátu požadovaného klienta,
- zaslanie certifikátu podľa požadovaného jednoznačného identifikátora.

IT riešenie (Systém) Elektronickej komunikácie s bankami, ako aj systémy všetkých Bánk, boli vyvinuté s použitím certifikátu vydaného spoločnosťou D. Trust Certifikačná Autorita, a.s., (ďalej aj „DTCA") - výhradný poskytovateľ certifikačných služieb akreditovanej certifikačnej autority První certifikační autorita, a.s., Praha (ďalej aj „I.CA") v Slovenskej republike. Typ certifikátu – osobný komerčný certifikát vydaný pre právnickú osobu, HASH (haš) algoritmus SHA-2, dĺžka kryptografických kľúčov pre RSA (Rivest–Shamir–Adleman4) 2048 Bits. Certifikát je platný jeden rok.

V prípade, že sa Zmluvné strany vzájomne dohodnú na inom druhu certifikátu, ktorý bude riadne všetkými Zmluvnými stranami v rámci Elektronickej komunikácie otestovaný a funkčný, môže byť tento certifikát následne k stanovenému dátumu zmenený na strane všetkých Zmluvných strán, vrátane Bánk. Takýto certifikát si Zmluvné strany a Banky zabezpečia v zmysle Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu. Takýmto certifikátom môže byť napr. typ certifikátu – osobný komerčný certifikát vydaný pre právnickú osobu, HASH algoritmus SHA-2, dĺžka kryptografických kľúčov pre RSA 4096 Bits".

Operačné systémy Microsoft a podpora SHA-2 certifikátov

Operačný systém	**Podpora SHA-2**
Windows 10 alebo novší	Áno
Windows Server 2016 alebo novší	Áno

Podmienky používania certifikátov sú definované v zmluve medzi účastníkom/držiteľom certifikátu a certifikačnou autoritou.

Držiteľ certifikátu je povinný najmä:

a) zaobchádzať so svojim súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k zneužitiu jeho súkromného kľúča,
b) uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča,
c) v prípade prezradenia súkromného kľúča druhej osobe je povinný túto skutočnosť bezodkladne oznámiť predpísaným spôsobom certifikačnej autorite a poskytovateľovi riešenia a súčasne vykonať všetky prípustné opatrenia na zamedzenie alebo aspoň obmedzenie vzniku prípadných škôd z dôvodu neoprávneného použitia prostriedku na vytvorenie digitálneho podpisu.

Komunikácia medzi držiteľom certifikátu/účastníkom elektronickej komunikácie a poskytovateľom riešenia prebieha mailom na základe zoznamu poverených osôb. Pre potvrdenie prijatia správy bude použitý telefonický kontakt a mailom zaslaná informácia kontaktným osobám.

Zrušenie certifikátu

1. držiteľ certifikátu ukončí platnosť certifikátu zaslaním žiadosti certifikačnej autorite a zároveň o tejto skutočnosti upovedomí poskytovateľa riešenia,
2. poskytovateľ riešenia preverí požiadavku telefonátom osobe, ktorá zaslala požiadavku na t. č. uvedené v zozname kontaktných osôb,

3. v prípade potvrdenia požiadavky poskytovateľ riešenia certifikát bezodkladne zablokuje pre ďalšie použitie v systéme elektronickej komunikácie,
4. poskytovateľ riešenia bude bezodkladne informovať mailom kontaktné osoby danej spoločnosti o vybavení požiadavky,
5. v prípade zneplatnenia certifikátu bude o tejto skutočnosti poskytovateľ riešenia bezodkladne informovať všetkých účastníkov elektronickej komunikácie.

Nahlásenie používaného certifikátu:

1. účastník elektronickej komunikácie zašle poskytovateľovi riešenia sériové číslo certifikátu, účel použitia a termín predpokladaného nasadenia,
2. poskytovateľ riešenia preverí požiadavku,
3. v prípade úspešného preverenia bude certifikát zaevidovaný pre použitie podľa požiadavky,
4. poskytovateľ riešenia zašle informáciu o vybavení požiadavky.

Poskytovateľ riešenia je povinný kontrolovať dobu platnosti certifikátov.

7. Prístupy

Zoznam klientov s priradenými identifikátormi je vytvorený a aktualizovaný na DUD, replikovaný spoločne s certifikátmi s verejnými kľúčmi na SPD.

Banky – meno, heslo (hash) a certifikát, voči ktorým sa Banka autentifikuje, sú uložené na DUD.

SP – meno, heslo (hash) a certifikát, voči ktorým sa SP autentifikuje sú uložené na SPD.

8. Výmena správ

Komunikácia sa delí podľa smeru toku dát:

A. Správa zasielaná Bankou
   1. asymetrická kryptografia je použitá na tvorbu digitálneho podpisu a bezpečnú výmenu kľúčov pre symetrickú kryptografiu, ktorá je použitá na vlastné šifrovanie prenášaných údajov,
   2. webová služba potvrdí úspešné uloženie správy,
   3. výmena údajov medzi zónami DU a SP (jednosmerná zo strany DU),
   4. pri úspešnom prevzatí správy SP je nastavený príznak „*stav*“ zasielanej správy.

B. Správa zasielaná SP
   1. asymetrická kryptografia je použitá na tvorbu digitálneho podpisu a bezpečnú výmenu kľúčov pre symetrickú kryptografiu, ktorá je použitá na vlastné šifrovanie prenášaných údajov,
   2. kľúč pre symetrickú kryptografiu je zašifrovaný verejným kľúčom:
      a. príjemcu (banka) v prípade, že ide o Príkaz alebo
      b. servera DUD v prípade, že ide o Žiadosť,
   3. webová služba potvrdí úspešné uloženie správy,
   4. výmena údajov medzi zónami DU a SP (jednosmerná zo strany DU),

5. v prípade 2.b server DUD zašifruje získaný kľúč pre symetrickú kryptografiu verejným kľúčom príjemcu (banka, alebo banky) a pripraví kópiu zasielanej správy pre každú Banku uvedenú v zozname adresátov,
6. pri každom úspešnom prevzatí správy bankou (viac Bánk v prípade Žiadosti) je nastavený príznak „*stav*" zasielanej správy.

Webové služby na serveroch SPA a DUA budú dostupné nepretržite mimo plánované technické odstávky a poruchy, príjem správ bude obmedzený podľa vopred dohodnutých časov prevádzky.

9. Úroveň a meranie služieb

Dostupnosťou služieb (ďalej len „IT riešenie") sa myslí dostupnosť počas pracovných hodín od 08.00 do 17.00 hod. v pracovných dňoch, pričom IT riešenie bude dostupné s výnimkou vopred odsúhlasených a dohodnutých odstávok systému. IT riešenie nebude považované za nedostupné v prípade akýchkoľvek problémov súvisiacich s internetom alebo sieťovými prvkami, ktoré sú mimo kontroly poskytovateľa riešenia a ďalších dohodnutých prípadoch medzi Zmluvnými stranami.

Výkonnosť Dátového uzla SP je určená na základe zaznamenanej doby trvania komunikácie s SP. Doba trvania je zaznamenaná počas komunikácie klient – server, pri volaní funkcie SendMessage. Funkcia SendMessage je časťou web servisu poskytovaného aplikačným serverom. Výkonnosť Dátového uzla Bánk je určená na základe zaznamenanej doby trvania komunikácie s Bankou. Doba trvania je zaznamenaná počas komunikácie klient – server, pri volaní funkcie SendMessage. Funkcia SendMessage je časťou web servisu poskytovaného aplikačným serverom.

Výkonnosť IT riešenia bude meraná v rámci IT riešenia, akýkoľvek problém s internetom, VPN (Virtuálna privátna sieť) alebo sieťovými prvkami, ktoré sú mimo kontroly poskytovateľa riešenia nebudú zahrnuté.

Každá Žiadosť, Informácia a každý Príkaz, poslaný SP alebo bankou do IT riešenia sa rozumie ako "transakcia". Pod transakciou sa teda rozumie nová Žiadosť, nový Príkaz, opakovaná Žiadosť, opakovaný Príkaz, Informácia, ktoré sú zaslané na konkrétnu Banku a SP prostredníctvom IT riešenia.

Dostupnosť a Výkonnosť IT riešenia:

1. Predpokladaný objem transakcií
   1.1 Dátový uzol SP a Dátový uzol bánk budú dimenzované na základe predpokladaného objemu 25 000 000 (dvadsaťpäť miliónov) transakcií ročne.
   1.2 V prípade, že objem transakcií presiahne predpokladaný objem transakcií, dodávateľ riešenia oznámi túto skutočnosť Zmluvným stranám (SP a Banka) a Úroveň služieb nebude garantovaná až do uvedenia aktualizovaného IT riešenia do prevádzky – stanoveného na základe nového objemu transakcií za rok; v tomto prípade dodávateľ riešenia urobí všetko pre to, aby minimalizovalo dopad na Úroveň služieb.
2. Dostupnosť IT riešenia:

2.1 Výsledky testovania dostupnosti budú zaznamenané ako percento času počas každého kalendárneho mesiaca počas doby Dostupnosti, keď Dátový uzol Bánk a Dátový uzol SP budú dostupné podľa nasledujúceho vzorca:

2.2 D = (A – B) / A (vyjadrené v percentách).

2.3 Vzorec je kalkulovaný ako D = dostupnosť, A = všetky pracovné hodiny za kalendárny mesiac (v minútach) a B = obdobie počas, ktorého nebolo IT riešenie dostupné (v minútach) počas doby Dostupnosti v danom kalendárnom mesiaci, okrem štátnych sviatkov.

2.4 Úroveň služieb pre Dostupnosť je 96 %.

3. Výkonnosť IT riešenia

3.1 Výsledky testovania výkonnosti budú zaznamenané na báze kalendárneho mesiaca pre určenie odchýlky od cieľových časov Odpovede uvedených nižšie:

	Priemerný čas obdržania jednotlivej správy
Doba trvania funkcie SendMessage na web servise Dátového uzla SP	Menej ako alebo rovné 5.0 sekúnd v 95 % všetkých správ
Doba trvania funkcie SendMessage na web servise Dátového uzla Bánk	Menej ako alebo rovné 5.0 sekúnd v 95 % všetkých správ

3.2 Reakčná doba nebude zahŕňať čas potrebný k prenosu odpovede cez internet alebo VPN (Virtuálna privátna sieť).

10. Parametre minimálne požadovanej úrovne služieb

Garantovaná Dostupnosť a Výkonnosť IT riešenia je zabezpečená od 8.00 hod. – 17.00 hod. počas pracovných dní. Žiadosti prijíma IT riešenie na Dátový uzol SP počas pracovných dní od 6.00 – 16.00 hod. Príkazy prijíma IT riešenie na Dátový uzol SP počas pracovných dní od 8.00 – 16.00 hod.

Poskytovateľ služieb bude informovať Zmluvné strany o plánovaných odstávkach systému minimálne tri (3) pracovné dni vopred. V prípade neplánovanej nedostupnosti systému bude poskytovateľ riešenia informovať objednávateľa a banky najneskôr do 1 hod. od zistenia neplánovaného výpadku zo strany poskytovateľa riešenia.

V prípade, že poskytovateľ má vedomosť o tom, že nastane technický výpadok IT riešenia a bude trvať viac ako 48 hodín, je povinný ihneď upovedomiť objednávateľa a banky o tomto výpadku, najneskôr do 1 hod. od zistenia tejto skutočnosti zaslaním informačného emailu na kontaktné adresy objednávateľa a bánk. Časový plán, ako aj začiatok prác na odstránení poruchy a doba trvania odstránenia poruchy, je počítaný na základe pracovných hodín poskytovateľa riešenia (08.00 – 17.00 hod. počas pracovných dní).

V prípade nahlásenia poruchy do 16.00 hod, bude doba potvrdenia prevzatia požiadavky na toto oznámenie poskytnutá do 1 pracovnej hodiny prostredníctvom kontaktných emailov a servisným hlásením.
Ak bude porucha nahlásená objednávateľom po 16.00 hod., bude doba potvrdenia prevzatia požiadavky na toto oznámenie poskytnutá objednávateľovi nasledujúci pracovný deň, najneskôr však do 9.00 hod.

Maximálne hodnoty časových limitov pre riešenie požiadaviek na odstránenie vád/porúch/výpadku:

Tabuľka č. 1. Definícia reakčných a servisných dôb

Priorita	Doba potvrdenia prevzatia požiadavky	Reakčná doba	Servisná doba
Kritická	60 minút	4 hodiny	2 pracovné dni
Vysoká	60 minút	16 hodín	5 pracovných dní
Normálna	60 minút	24 hodín	10 pracovných dní

Triedenie vád/porúch/výpadku podľa stupňa ich závažnosti bude nasledovné:

- **kritická priorita** - kritické zlyhanie systému, ktoré znemožňuje prácu so systémom, znemožňuje používanie systému; alebo celoplošný problém, jeho okamžité riešenie je nevyhnutné pre 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 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 fungovanie systému, funkcionalita existuje, ale zhoršený je jeden parameter.

Prílohy:

Príloha č. 1 *k Prílohe č. 2 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou,* **Štruktúra_Žiadosť_Informácia**

Príloha č. 2 *k Prílohe č. 2 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou,* **Štruktúra_Príkazy**

Príloha č.1 *k Prílohe č. 2 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou,* **Štruktúra_Žiadosť_Informácia**

TypeID	Typ správy
2	žiadosť - stavy účtov
3	iná žiadosť
12	informácia - stavy účtov
13	iná informácia
501	príkaz na začatie vymáhania pohľadávok (exekúcie)
502	zmena_príkaz na začatie vymáhania pohľadávok (exekúcie)
503	exekučný príkaz
504	zmena_exekučný príkaz
505	súhlas SP s uvoľnením sumy nepodliehajúcej exekúcii
506	zrušenie exekučného príkazu
507	zastavenie_odblokovanie
508	odklad exekúcie_zrušenie odkladu

Identifikácia povinného		
PersonTypeID	**typ**	**povinne vyplnené položky**
1	FO s prideleným RČ	rodné číslo
2	FO podnikateľ	rodné číslo, IČO
3	PO s prideleným IČO	IČO
4	FO bez prideleného RČ	meno, priezvisko, dátum narodenia, kód krajiny (cudzozemec)
5	PO zahraničná bez prideleného IČO	názov, kód krajiny

Country code
Kód OSN podľa aktuálnej Vyhlášky štatistického úradu Slovenskej republiky, ktorou sa vydáva Štatistický číselník krajín použije sa 3-miestny číselný kód, element <Code>

Príloha č. 2 *k Prílohe č. 2 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou* **Štruktúra_Príkazy**

Definícia štruktúr Príkazov
Každý zasielaný Príkaz pozostáva zo záhlavia (obálky) a samotného obsahu Príkazu
Štruktúra záhlavia je definovaná v hárku Záhlavie
Štruktúra obsahu príkazov je definovaná v jednotlivých hárkoch
Počas celého priebehu komunikácii je samotný obsah príkazu zašifrovaný a poskytovateľ do neho nebude vstupovať a zasahovať nijakým spôsobom
Poskytovateľ prijme od odosielateľa Príkaz v štruktúre obálky odosielanej správy a odovzdá Príkaz adresátovi v štruktúre obálky prijímanej správy.
Údaje v obálke prijímanej správy sú vytvorené na základe údajov z obálky odosielanej správy s doplnenými a pozmenenými údajmi len v tej miere, aby bola správa spracovateľná technickými prostriedkami na strane adresáta.

Príloha č. 3 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

CENOVÁ KALKULÁCIA

Tabuľka č. 1

Predmet Zmluvy	**Merná jednotka (MJ)**	**Počet MJ**	**Cena za MJ v EUR bez DPH**	**DPH za MJ 20%**	**Cena za MJ v EUR s DPH**	**Cena spolu za počet MJ *(cena za predmet Zmluvy)* v EUR bez DPH**	**DPH za počet MJ 20 %**	**Cena spolu za počet MJ *(cena za predmet Zmluvy)* v EUR s DPH**
a	b	c	d	e	f	g = c * d	h = c * e	i = c * f
Poskytovanie služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou podľa čl. III bodu 1 Zmluvy	Rok (12 mesiacov)	1	105 000,- eur	21 000,- eur	126 000,- eur	105 000,- eur	21 000,- eur	**126 000,- eur**

V Bratislave dňa

Ing. Ján Budinský, konateľ

Mgr. Petr Kučera, konateľ

Natália Shchelovanova, konateľ

Príloha č. 4 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

OPRÁVNENÉ OSOBY

Za stranu Objednávateľa:

Projektový manažér: *riaditeľ odboru pohľadávok*

Za stranu Poskytovateľa:

Projektový manažér: *Ing.* [redacted] *Project Manager*

Príloha č. 5 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

VZOR POŽIADAVKY 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:

Záznam riešiteľa:

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

<MAXIMOEMAILCONTENT>
<LSNRACTION>UPDATE</LSNRACTION>
<LSNRAPPLIESTO>SR</LSNRAPPLIESTO>
<TICKETID></TICKETID>
<CLASS>SR</CLASS>
<EXTERNALSYSTEM_TICKETID></EXTERNALSYSTEM_TICKETID>
<YSTATUS></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. 6 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

ZOZNAM SUBDODÁVATEĽOV

Názov, obchodné meno:
Adresa:
IČO:

Na poskytovaní plnenia Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BAsa:

a) nebudú podieľať subdodávatelia a celý predmet Zmluvy uskutočníme vlastnými kapacitami,
b) budú podieľať nasledovní subdodávatelia:*

P. č.	Meno a priezvisko alebo obchodné meno alebo názov subdodávateľa Adresa sídla alebo miesta podnikania	IČO	Meno a priezvisko, adresa pobytu a dátum narodenia osoby oprávnenej konať za subdodávateľa	Podiel plnenia zo Zmluvy v %	Predmet subdodávok
1.					
2.					
3.					

V ....., dňa

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

Príloha č. 7 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č. 52396-3/2024-BA

Protokol o paušálnej podpore

(VZOR)

Poskytovateľ:

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

Na základe Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č. ... zo dňa ... Poskytovateľ vykonal služby za obdobie ... štvrťroku v roku ..... V rámci týchto služieb boli predmetom riešenia nasledujúce vady:

Dátum evidencie	Detailný popis činnosti / predmet činnosti	Stav riešenia	Čas riešenia/počet hodín	Poznámka
		Otvorený		
		Uzatvorený		

Na znak súhlasu s obsahom tohto protokolu o paušálnej podpore ho obe Zmluvné strany podpísali. Protokol o paušálnej podpore je vyhotovený v dvoch vyhotoveniach, pričom každá Zmluvná strana dostane jeden.

V ....., dňa

Za Poskytovateľa:

.....

projektový manažér

V Bratislave, dňa

Za Objednávateľa:

.....

projektový manažér

Príloha č. 8 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

ZÁPIS
O ZMENE PRÍLOHY
(VZOR)

k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BAuzatvorenej podľa § 269 ods. 2 Obchodného zákonníka (ďalej len „Zmluva“) medzi:

poskytovateľom:.....
....., *IČO:* .....
(ďalej len „poskytovateľ“)
a
objednávateľom: ***Sociálna poisťovňa**, Ul. 29. augusta č. 8 a 10, 813 63 Bratislava, IČO: 30807484*
(ďalej len „objednávateľ“)
(ďalej spolu ako „Zmluvné strany“)

V súlade s článkom XX bodom X.X Zmluvy, v ktorom sa Zmluvné strany dohodli o spôsobe zmeny prílohy č. X k Zmluve „...“, Zmluvné strany v zastúpení ich oprávnenými zástupcami podpisujú tento zápis, ktorým sa mení príloha č. X k Zmluve „...“, ktorá tvorí prílohu k tomuto zápisu.

Dôvod potreby uskutočnenia zmeny prílohy č. X k Zmluve „...“:

.....
.....

Tento zápis je neoddeliteľnou súčasťou Zmluvy.

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

Nadobudnutím účinnosti tohto zápisu sa v celom rozsahu mení znenie prílohy č. X k Zmluve „č.: 52396-3/2024-BA“.

Za poskytovateľa:

..... dňa

.....

.....

Za objednávateľa:

Bratislava dňa

.....

riaditeľ sekcie stratégie a informatiky

Príloha:

Príloha č. X k Zmluve „...“

Príloha č. 9 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

Sprostredkovateľská zmluva

uzatvorená podľa čl. 28 ods. 3 nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane osobných údajov) a podľa § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Zmluvné strany

Prevádzkovateľ

Názov:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta č. 8 a 10 813 63 Bratislava
V zastúpení:	Ing. Michal Tariška generálny riaditeľ Sociálnej poisťovne
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA
IČO:	30807484
DIČ:	2020592332
IČ DPH:	SK2020592332

(ďalej len „Prevádzkovateľ")

a

Sprostredkovateľ

Obchodné meno:	**CRIF – Slovak Credit Bureau, s.r.o**
Sídlo:	Mlynské nivy 14, 821 09 Bratislava
Štatutárny orgán:	Ing. Ján Budinský, konateľ Mgr. Petr Kučera, konateľ Natália Shchelovanova, konateľ
IČO:	35886013
DIČ:	2021842042
IČ pre DPH:	SK2021842042
Bankové spojenie:	
IBAN:	
SWIFT:	

Zapísaný v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sro, vložka č. 31737/B.

(ďalej len „Sprostredkovateľ")

(spolu ďalej ako „Zmluvné strany")

Preambula

Zmluvné strany spolu uzatvárajú „Zmluvu o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BApodľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, predmetom ktorej je technické zabezpečenie elektronickej komunikácie medzi bankami a Sociálnou poisťovňou, ktorú zabezpečuje Sprostredkovateľ (ďalej len „zmluva o poskytovaní služieb, alebo „Zmluva o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie"). Vzhľadom na spracovanie osobných údajov zamestnancov 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 – identifikovaná, alebo identifikovateľná fyzická osoba, ktorej sa spracúvané osobné údaje týkajú – dotknutí zamestnanci 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. Prevádzkovateľ touto Zmluvou poveruje Sprostredkovateľa spracovaním osobných údajov Dotknutých osôb v mene Prevádzkovateľa v rozsahu osobných údajov, spracúvanie ktorých je potrebné pre účely plnenia zmluvy o poskytovaní služieb .
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou zmluvy o poskytovaní služieb po splnení povinností uvedených v tejto Zmluve a

výlučne na účel vykonávania technického zabezpečenia elektronickej komunikácie medzi bankami a Prevádzkovateľom.

3. Účel spracúvania osobných údajov je vymedzený v zákone č. 461/2003 Z. z. o sociálnom poistení, v Nariadení (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, v Nariadení (ES) Európskeho parlamentu a Rady č. 987/2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, podľa ktorých je Prevádzkovateľ oprávnený spracúvať osobné údaje svojich klientov za účelom výkonu sociálneho poistenia.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje výhradne pre poskytovanie služieb Prevádzkovateľovi, a to na základe pokynov Prevádzkovateľa podľa podmienok stanovených v tejto Zmluve v súlade so všeobecne záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov. Za pokyny Prevádzkovateľa sa považujú pokyny uvedené v tejto Zmluve, v v zmluve o poskytovaní služieb, prípadne iné písomne zdokumentované pokyny.
5. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu zmluvy o poskytovaní služieb je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom konkrétnu zákonnú povinnosť ustanovuje zmluva o poskytovaní služieb osobitne a § 78 ods. 3 ZOOU.

Čl. III
Zoznam osobných údajov a okruh dotknutých osôb

1. Zmluva, v rámci plnenia ktorej je sprostredkovateľ poverený spracúvať osobné údaje zamestnancov prevádzkovateľa: Zmluva č.: 52396-3/2024-BA o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou."
2. Zoznam osobných údajov, ktoré môžu byť v prípade potreby realizácie predmetu zmluvy o poskytovaní služieb predmetom spracúvania:
   rodné číslo, meno, priezvisko fyzickej osoby (FO), dátum narodenia, kód krajiny (cudzozemec), meno a priezvisko zamestnanca Prevádzkovateľa, adresa zamestnávateľa.
3. Spracúvané osobné údaje sú povahy:
   iné osobné údaje v rozsahu bodu 2 tohto článku.
   Spracúvané osobné údaje sú typu:
   Bežné osobné údaje.
   Údaje ekonomického charakteru.
4. Sprostredkovateľ spracúva osobné údaje fyzických osôb uvedené v bode 2 tohto článku (ďalej „dotknuté osoby").

Čl. IV
Spôsob výkonu Zmluvy a oprávnenia Prevádzkovateľa

1. Sprostredkovateľ vykonáva spracúvanie osobných údajov prostredníctvom služby zabezpečujúcej elektronickú komunikáciu medzi Prevádzkovateľom a Bankami v rámci projektu osobitného informačného systému.
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 a vedenia ekonomickej, prevádzkovej, personálnej 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) vyhľadávanie,
e) prehliadanie,
f) preskupovanie alebo kombinovanie,
g) vymazanie alebo likvidácia,
h) poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom

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

Čl. VII
Povinnosti Sprostredkovateľa

1. Sprostredkovateľ sa pri spracúvaní osobných údajov podľa tejto Zmluvy zaväzuje najmä:
   a) Postupovať s náležitou starostlivosťou a v súlade s GDPR, ZOOU a súvisiacimi všeobecne záväznými právnymi predpismi Slovenskej republiky, dodržiavať povinnosti vyplývajúce z tejto Zmluvy a pokynov prevádzkovateľa, a dodržiavať zásady ochrany osobných údajov zverejnené Prevádzkovateľom,
   b) akékoľvek spracúvanie osobných údajov vykonávať len za účelom plnenia predmetu tejto Zmluvy a Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou a len v rozsahu nevyhnutnom na ich plnenie,

c) údaje dotknutých osôb nezverejňovať, nešíriť či neodovzdávať ďalším osobám,
d) zaistiť, aby jeho zamestnanci a ďalšie osoby, ktoré využije na plnenie podľa tejto Zmluvy, dodržiavali podmienky stanovené GDPR, vnútroštátnymi predpismi a touto Zmluvou a boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti,
e) ak všeobecne záväzné právne predpisy neustanovujú inak, osobné údaje, s ktorými sa dostal do styku v súvislosti s realizáciou Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou nezverejňovať, neposkytovať a nesprístupňovať tretím stranám,
f) zachovávať mlčanlivosť a zabezpečiť diskrétnosť pri akomkoľvek spracúvaní osobných údajov,
g) ak Zmluva o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou 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 o poskytovaní služieb, zmazať zo všetkých elektronických, hmotných alebo iných nosičov informácii (napr. pevné disky počítačov, USB kľúče, CD, DVD, dokumenty v papierovej podobe) alebo tieto nosiče zlikvidovať tak, aby nedošlo k úniku týchto údajov,
i) poučiť svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby"), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných údajov, ako aj o iných právach a povinnostiach sprostredkovateľa upravených Zmluvou alebo ustanovených všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov, o zodpovednosti za ich porušenie, a to všetko pred uskutočnením prvej operácie s osobnými údajmi,
j) zachovávať mlčanlivosť o osobných údajoch dotknutých osôb a o bezpečnostných opatreniach prijatých na zabezpečenie ochrany osobných údajov, a to aj po skončení tohto zmluvného vzťahu,
k) je povinný nakladať s údajmi ako s informáciami dôvernými v zmysle zákona 513/1991 Zb. (Obchodný zákonník) a jeho následných novelizácií a je povinný zaviazať týmito povinnosťami aj osoby, ktoré by dojednal na činnosti na plnenie podľa tejto Zmluvy (zamestnancov či iných pracovníkov),
l) plniť predmet Zmluvy len prostredníctvom riadne a preukázateľne poučených alebo vyškolených oprávnených osôb pre účel plnenia predmetu zmluvy o poskytovaní služieb a z nej vyplývajúceho rozsahu a podmienok spracúvania osobných údajov,
m) spracúvať osobné údaje oprávnenými osobami konajúcimi za sprostredkovateľa len v rozsahu pokynov prevádzkovateľa v zmysle čl. 32 GDPR vrátane prípadnej pseudonymizácie a šifrovania s ohľadom na okolnosti konkrétneho prípadu a v rozsahu nevyhnutnom na dosiahnutie účelu spracúvania osobných údajov, ako je uvedené v čl. II tejto Zmluvy a pokynu prevádzkovateľa udeleného osobou oprávnenou konať v danom rozsahu za prevádzkovateľa, alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
n) v prípade sťažností alebo sporu týkajúceho sa spracúvania osobných údajov pri plnení predmetu Zmluvy, bezodkladne informovať prevádzkovateľa o tejto skutočnosti a spolupracovať pri riešení sťažnosti alebo sporu s prevádzkovateľom,
o) nepoužiť spracúvané osobné údaje v mene prevádzkovateľa pre vlastnú potrebu, pokiaľ všeobecne záväzné platné právne predpisy neustanovujú inak,

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

2. Sprostredkovateľ je pri spracúvaní osobných údajov podľa tejto Zmluvy ďalej povinný bezodkladne informovať Prevádzkovateľa o
   a) poskytnutí a sprístupnení osobných údajov tretej strane spolu s odôvodnením a určením všeobecne záväzného právneho predpisu, ktorý sprostredkovateľovi ukladá povinnosť poskytnúť, sprístupniť alebo zverejniť osobné údaje dotknutých osôb spracúvaných v mene prevádzkovateľa,
   b) skutočnostiach zabraňujúcich plneniu povinností podľa tejto Zmluvy,
   c) akomkoľvek porušení povinností podľa Zmluvy alebo porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov,
   d) akomkoľvek porušení ochrany osobných údajov,
   e) akomkoľvek porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov zo strany prevádzkovateľa, ak sa podľa názoru sprostredkovateľa pokynom prevádzkovateľa tieto predpisy porušujú.
3. V prípade, ak sprostredkovateľ obdržal žiadosť dotknutej osoby, ktorá si uplatňuje voči prevádzkovateľovi svoje práva podľa článkov 15 až 22 GDPR a § 21 až § 28 ZOOU (napr. právo na prístup k údajom, právo na výmaz alebo opravu osobných údajov), je povinný bezodkladne, najneskôr však do troch pracovných dní od jej prijatia, takúto žiadosť zaslať prevádzkovateľovi prostredníctvom emailovej adresy: zodpovedna.osoba@socpoist.sk, spolu so žiadosťou je sprostredkovateľ povinný prevádzkovateľovi zaslať aj ďalšie relevantné informácie týkajúce sa predmetnej žiadosti, ktoré by mohli mať vplyv na postup vybavenia žiadosti dotknutej osoby zo strany prevádzkovateľa.
4. Sprostredkovateľ je povinný pomáhať prevádzkovateľovi pri zabezpečení plnenia povinností prevádzkovateľa v oblasti bezpečnosti spracúvania, zisťovania porušení ochrany osobných údajov, posudzovania vplyvu na ochranu osobných údajov a poskytovať informácie, ktoré sú mu dostupné.
5. Sprostredkovateľ je povinný dôsledne chrániť spracúvané osobné údaje podľa svojho najlepšieho vedomia, v súlade s ustanoveniami GDPR a ZOOU.
6. Oprávnené osoby sprostredkovateľa resp. subdodávateľa, ktoré budú mať prístup k osobným údajom sú viazaní povinnosťou mlčanlivosti o týchto údajoch a to aj po zániku štátnozamestnaneckého pomeru, pracovného pomeru uzatvoreného v súlade so zákonníkom práce resp. v súlade so zákonom o výkone práce vo verejnom záujme alebo dohody o práci vykonávanej mimo pracovného pomeru v súlade so zákonníkom práce.
7. Oprávnené osoby sprostredkovateľa sú oboznámené so spôsobom oznamovania podozrení z bezpečnostných incidentov v súvislosti s informačným systémom a spracúvanými osobnými údajmi. Oprávnené osoby sprostredkovateľa sú poučené, aby bezodkladne oznamovali určenej osobe prevádzkovateľa akékoľvek podozrenie z bezpečnostného incidentu, ktoré by mohlo mať dopad na bezpečnosť informačného systému s osobnými údajmi. Sprostredkovateľ je povinný bezodkladne prijať relevantné opatrenia k náprave, o bezpečnostnom incidente informovať zodpovednú osobu prevádzkovateľa a e-mailom na adresu: zodpovedna.osoba@socpoist.sk.
8. Sprostredkovateľ je povinný spracovať a dokumentovať prijaté a vykonané technicko-organizačné opatrenia na zaistenie ochrany osobných údajov v súlade s právnymi predpismi EÚ a Slovenskej republiky, k tomu sa vzťahujúcimi. Sprostredkovateľ je povinný spolupracovať s Prevádzkovateľom a byť mu nápomocný pri zaisťovaní plnenia jeho povinností pri prevencii rizík a ďalších povinností Prevádzkovateľa podľa ustanovení čl. 32 – 36 GDPR. K vyžiadaniu Prevádzkovateľa je mu nápomocný technickými a organizačnými prostriedkami pri plnení povinností Prevádzkovateľa reagovať na žiadosti o výkon práv Dotknutej osoby stanovených

v kapitole III. GDPR (informácie a prístup k osobným údajom, oprava a výmaz, právo na obmedzenie spracovania atď.).

9. Sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na doloženie toho, že boli splnené povinnosti sprostredkovateľa a stanovené ustanoveniami GDPR a umožní audity, vrátane inšpekcií, vykonávané prevádzkovateľom alebo iným audítorom, ktorého prevádzkovateľ poveril. Pri vykonávaní auditov bude spolupracovať s prevádzkovateľom alebo ním určeným audítorom. Prevádzkovateľ je oprávnený vykonať inšpekciu plnenia povinností sprostredkovateľa a audit bez predchádzajúceho upozornenia. Ne spolupráca 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 spracúvaním 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 Spracúvanie osobných údajov subdodávateľmi sprostredkovateľa do budúcna je možné po ich odsúhlasení prevádzkovateľom. Budúci 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 preukázateľne spôsobil 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, maximálne však do výšky maximálnej ceny za predmet Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou.
3. Ochrana osobných údajov podľa Zmluvy trvá aj po ukončení zmluvného vzťahu založeného touto Zmluvou a zaväzuje aj právnych nástupcov zmluvných strán. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá prevádzkovateľovi vznikla porušením povinností sprostredkovateľa.
4. Sprostredkovateľ je poverený spracúvať osobné údaje po dobu platnosti tejto Zmluvy. Okamihom skončenia jej platnosti už sprostredkovateľ nesmie disponovať žiadnymi osobnými údajmi. Sprostredkovateľ je povinný vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje, v prípade že ich spracovával, po ukončení poskytovania služieb týkajúcich sa plnenia zmluvy o poskytovaní služieb a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov, o čom vyhotoví písomné vyhlásenie, ktoré je povinný doručiť prevádzkovateľovi najneskôr do dvoch pracovných dní od skončenia platnosti Zmluvy.
5. Kontakt na zástupcu prevádzkovateľa zodpovedného za ochranu osobných údajov: zodpovedna.osoba@socpoist.sk
6. Kontakt na zástupcu sprostredkovateľa: dpo.sk@crif.com.

Čl. X
Trvanie a ukončenie Zmluvy

1. Táto Zmluva sa uzatvára po dobu trvania spolupráce Prevádzkovateľa a Sprostredkovateľa v zmysle Zmluvy č.: 52396-3/2024-BA o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou.

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 oprávnených zástupcov oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej 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 zmluvy o poskytovaní služieb je možné ukončiť túto Zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane.
5. Práva a povinnosti neupravené touto Zmluvou sa budú riadiť príslušnými ustanoveniami právnych predpisov platných na území SR.
6. Zmluvné strany štandardne komunikujú prostredníctvom elektronickej pošty. V prípadoch, keď to vyžaduje zmluva, všeobecne záväzný právny predpis alebo jedna zo zmluvných strán, doručí sa aj listinná podoba požiadavky, súhlasu a pod.
7. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto Zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.
8. Zmeny a doplnenia tejto Zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k zmluve.
9. Táto Zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.
10. Zmluvné strany vyhlasujú, že túto Zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave dňa

Za Prevádzkovateľa:

V Bratislave dňa

Za Sprostredkovateľa:

.....

Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

.....

Ing. Ján Budinský
konateľ
CRIF – Slovak Credit Bureau, s.r.o

.....

Mgr. Petr Kučera
konateľ
CRIF – Slovak Credit Bureau, s.r.o

.....

Natalia Shchelovanova
konateľ
CRIF – Slovak Credit Bureau, s.r.o

Príloha č. 10 k Zmluve o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou č.: 52396-3/2024-BA

Zmluva
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

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

Čl. I
Zmluvné strany

Prevádzkovateľ

Názov:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta č. 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Tariška, generálny riaditeľ Sociálnej poisťovne
IČO:	308 07 484
DIČ:	2020592332
IČ DPH:	SK2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA

(ďalej len „prevádzkovateľ")

a

Dodávateľ

Obchodné meno:	**CRIF – Slovak Credit Bureau, s.r.o**
Sídlo:	Mlynské Nivy 14, 821 09 Bratislava
Štatutárny orgán:	Ing. Ján Budinský, konateľ Mgr. Petr Kučera, konateľ Natalia Shchelovanova, konateľ
IČO:	35886013
DIČ:	2021842042
IČ pre DPH:	SK2021842042
Bankové spojenie:	
IBAN:	
SWIFT:	

Zapísaný v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sro, vložka č. 31737/B.

(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 výkon činností poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa, ako prevádzkovateľa základnej služby.
2. Zmluvné strany spolu uzatvárajú „Zmluvu č.: 52396-3/2024-BA o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou" podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „zmluva na výkon činností"), predmetom ktorej je technické zabezpečenie elektronickej komunikácie medzi bankami a Sociálnou poisťovňou. 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 Technické zabezpečenie elektronickej komunikácie medzi bankami a Sociálnou poisťovňou.

Čl. IV
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné politiky prevádzkovateľa ak bol s nimi riadne oboznámený.
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. e), f), h), j) a k) 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 riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie stratégie a 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

1. 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 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, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov dodávateľa, pričom maximálna výška náhrady preukázateľnej škody Dodávateľa Prevádzkovateľovi v zmysle tejto Zmluvy je maximálna cena za predmet plnenia Zmluvy o poskytovaní služieb pri technickom zabezpečení elektronickej komunikácie medzi bankami a Sociálnou poisťovňou.
8. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.
9. Po ukončení tejto zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

Čl. XI
Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom UPVS, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti je: riaditeľ odboru bezpečnosti informačných systémov.
3. Kontaktná osoba dodávateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je: Ing. Martin Dolog
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: bis@socpoist.sk.
5. Kontakt na zástupcu dodávateľa na úseku kybernetickej bezpečnosti je: m.dolog@crif.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. 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.
4. 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.
5. 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.
6. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve.
7. 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.
8. Neoddeliteľnou súčasťou tejto zmluvy je
   Príloha č. 1 – Bezpečnostné politiky
   Príloha č. 2 – Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni.
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 Bratislave, dňa

Za dodávateľa:

.....

Ing. Ján Budinský
konateľ
CRIF – Slovak Credit Bureau, s.r.o

.....

Mgr. Petr Kučera
konateľ
CRIF – Slovak Credit Bureau, s.r.o

.....

Natalia Shchelovanova,
konateľ
CRIF – Slovak Credit Bureau, s.r.o

Príloha č. 1 k Prílohe č. 10

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 stratégie a 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 stratégie a 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 odboru 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 stratégie a 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 stratégie a 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. 10

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 verzií 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-FI) 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 filtrovaná 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 v znení neskorších predpisov
- Trestný zákon č. **300/2005** Z. z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí) v znení neskorších predpisov
- Zákon č. **45/2011** Z. z. o kritickej infraštruktúre v znení neskorších predpisov
- Zákon č. **305/2013** Z. z. o elektronickej podobe výkonu pôsobnosti OVM a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
- Zákon č. **272/2016** Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov
- Zákon č. **18/2018** Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov 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 v znení neskorších predpisov (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 v znení neskorších predpisov
- 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 v znení neskorších predpisov
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy verejnej správy
- 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
- 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

- 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 v znení neskorších predpisov
- 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.

Logovací štandard.docx