

Z m l u v a
o poskytovaní technickej podpory pre Centrálny dochádzkový systém
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v znení
neskorších predpisov

Článok I
Zmluvné strany

Poskytovateľ:	Eviden Slovakia s.r.o.
Sídlo:	Pribinova 19/7828, 811 09 Bratislava
V mene poskytovateľa koná:	Ing. Pavel Struhárik, konateľ
Bankové spojenie:	XXXXXX
IBAN:	XXXXXX
SWIFT:	XXXXXX
IČO:	45 650 276
DIČ:	2023110661
IČ DPH:	SK2023110661

Spoločnosť zapísaná v Obchodnom registri Mestského súdu Bratislava III., Oddiel: Sro, vložka č. 66638/B.
(ďalej len „poskytovateľ“)

a

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

(Sociálna poisťovňa je osobou registrovanou pre daň podľa § 7 ods. 2 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov)
(ďalej len „objednávateľ“)

(Objednávateľ a poskytovateľ jednotlivo ďalej ako „**zmluvná strana**“ a spoločne ďalej ako „**zmluvné strany**“)

Východiskovým podkladom na uzatvorenie tejto zmluvy o poskytovaní technickej podpory pre Centrálny dochádzkový systém (ďalej len „zmluva“) sú súťažné podklady a ponuka poskytovateľa zo dňa 28.07.2023, predložená do verejnej súťaže vyhlásenej vo Vestníku verejného obstarávania č. 131/2023 dňa 06.07.2023 pod značkou 22151-MSS v rámci zadávania

nadlimitnej zákazky podľa zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“).

Článok II

Predmet zmluvy

- 2.1 Predmetom zmluvy je záväzok poskytovateľa poskytovať služby technickej podpory pre aplikačné programové vybavenie (ďalej aj ako „APV“) pre Centrálny dochádzkový systém (ďalej aj ako „CDS“), zapracovať zmenové požiadavky v prípade požiadavky do centrálného dochádzkového systému, zabezpečiť prípadný upgrade, dodávku, resp. výmenu hardwaru (ďalej aj ako „HW“) komponentov dochádzkového systému vrátane plnej integrácie do existujúceho systému v rozsahu:
 - 2.1.1 podpora softvéru,
 - 2.1.2 technická podpora komponentov pre dochádzkový a prístupový systém,
 - 2.1.3 hardvérové rozšírenie prístupového systému,
 - 2.1.4 implementácia spracovania cestovných príkazov ako integrálnej súčasti systému CDS,
 - 2.1.5 úpravy aplikácie iCard,podľa požiadaviek uvedených v prílohe č. 1 k zmluve, ktorá tvorí neoddeliteľnú súčasť tejto zmluvy.
- 2.2 Poskytovateľ sa zaväzuje poskytovať predmet zmluvy počas jej platnosti a účinnosti v celom rozsahu, špecifikácii, termínoch, kvalite, funkcionalite, riadne a včas a objednávatel' sa zaväzuje poskytované služby prevziať a uhradiť za poskytované služby cenu podľa podmienok dohodnutých v tejto zmluve.
- 2.3 Poskytovateľ sa zaväzuje poskytovať objednávateľovi predmet zmluvy podľa bodov 2.1.3 až 2.1.5 tohto článku zmluvy na základe požiadaviek podľa aktuálnych potrieb objednávateľa riadne a včas v dohodnutej kvalite, termíne a množstve. Poskytovateľ berie na vedomie, že (i) objednávateľ je oprávnený na základe svojich potrieb určovať rozsah, a že (ii) rozsah predmetu zmluvy počas platnosti tejto zmluvy nemožno považovať za záväzný v žiadnom rozsahu, (iii) objednávateľ nie je povinný objednať celé množstvo podľa tejto zmluvy, ani vyčerpať celkový finančný limit predmetu zmluvy. Celkové odobrané množstvo podľa tejto zmluvy bude závisieť výlučne od potrieb objednávateľa počas platnosti a účinnosti tejto zmluvy. Pre vylúčenie pochybnosti zmluvné strany berú na vedomie, že objednávateľ nemusí zrealizovať žiadnu objednávku. Neobjednanie služieb objednávateľom v celom rozsahu a množstve nezakladá právo poskytovateľa uplatniť si nárok na náhradu škody a ani od zmluvy odstúpiť.

Článok III

Termín, miesto a spôsob plnenia

- 3.1 Poskytovateľ sa zaväzuje poskytovať podporu podľa článku II bodov 2.1.1 a 2.1.2 zmluvy a prílohy č. 1 k tejto zmluve počas platnosti a účinnosti tejto zmluvy, t. j. 36 mesiacov odo dňa nadobudnutia účinnosti zmluvy.
- 3.2 Poskytovateľ sa zaväzuje poskytovať predmet zmluvy podľa čl. II bodov 2.1.3 až 2.1.5 tejto zmluvy v dohodnutom rozsahu a termíne plnenia stanovenom v schválenej požiadavke objednávateľa, ktorá bude zadávaná podľa nasledujúceho bodu.

- 3.3 Objednávateľ komunikuje so všetkými externými dodávateľmi prostredníctvom automatizovaného komunikačného nástroja Service desk, prostredníctvom ktorého predloží poskytovateľovi požiadavku (ďalej aj ako „ticket“), ktorá bude obsahovať:
- špecifikáciu požadovanej služby/tovaru,
 - rozsah/počet požadovaných služieb/tovaru,
 - navrhovaný termín poskytnutia/dodania služby/tovaru.
- 3.4 Ku každej požiadavke (ticketu) vypracuje poskytovateľ najneskôr do päť (5) pracovných dní od jej predloženia ponuku predmetu požiadavky na základe dohodnutej cenovej kalkulácie predmetu zmluvy podľa Prílohy č. 2.
- 3.5 Pri tikete, ktoré poskytovateľ nemôže v požadovanom termíne zrealizovať, sa objednávateľ a poskytovateľ dohodnú na záväznom termíne poskytnutia/dodania služby/ tovaru.
- 3.6 Objednávateľ do päť (5) pracovných dní schváli/neschváli predloženú ponuku.
- 3.7 Dokladom o začatí poskytovania služieb technickej podpory podľa čl. II bodov 2.1.1 a 2.1.2 je odovzdávací/preberací protokol podpísaný oprávnenými zástupcami oboch zmluvných strán do piateho dňa od nadobudnutia účinnosti tejto zmluvy.
- 3.8 Dokladom o poskytnutí predmetu zmluvy podľa čl. II bodov 2.1.3 až 2.1.5 je akceptačný protokol podpísaný oprávnenými zástupcami oboch zmluvných strán.
- 3.9 Miestom plnenia predmetu zmluvy je Sociálna poisťovňa, ústredie a pobočky na území SR uvedené v Prílohe č. 1.

Článok IV

Cena

- 4.1 Cena za predmet zmluvy je stanovená dohodou zmluvných strán v eurách podľa ustanovení 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 č. 18/1996 Z. z. o cenách v znení neskorších predpisov.
- 4.2 Celková maximálna cena za predmet zmluvy je zmluvnými stranami dohodnutá vo výške:
- | | |
|--------------------------|------------|
| cena v EUR bez DPH | 676 558,50 |
| 20% sadzba DPH v EUR | 135 311,70 |
| celková cena v EUR s DPH | 811 870,20 |
- z toho

4.2.1 Cena za služby podpory softvéru podľa čl. II bodu 2.1.1 počas platnosti zmluvy je zmluvnými stranami dohodnutá **paušálnou cenou za jeden kalendárny mesiac** nasledovne:

cena v EUR bez DPH	8 600,00
20 % sadzba DPH v EUR	1 720,00
celková cena v EUR s DPH	10 320,00

Celková cena za obdobie 36 kalendárnych mesiacov je dohodnutá nasledovne:

cena v EUR bez DPH	309 600,-
20% sadzba DPH v EUR	61 920,-
celková cena v EUR s DPH	371.520,-

4.2.2 Cena za služby technickej podpory komponentov pre dochádzkový a prístupový systém podľa čl. II bodu 2.1.2 počas platnosti zmluvy je zmluvnými stranami dohodnutá **paušálnou cenou za jeden kalendárny mesiac** nasledovne:

cena v EUR bez DPH	1.000,-
20% sadzba DPH v EUR	200,-
celková cena v EUR s DPH	1.200,-

Celková cena za obdobie 36 kalendárnych mesiacov je dohodnutá nasledovne:

cena v EUR bez DPH	36.000,-
.. % sadzba DPH v EUR	7.200,-
celková cena v EUR s DPH	43.200,-

4.2.3 Cena za hardvérové rozšírenie prístupového systému podľa čl. II bodu 2.1.3 je dohodnutá ako súčin dohodnutej ceny sadzby za 1 mernú jednotku a skutočne dodaného počtu merných jednotiek podľa potvrdených akceptačných protokolov o prevzatí predmetu zmluvy. Zmluvné strany berú na vedomie, že celková cena za hardvérové rozšírenie prístupového systému je maximálna a zo strany Poskytovateľa nenárokovateľná, pretože vždy sa pri jej výpočte vychádza v každom jednotlivom prípade zo skutočných potrieb Objednávateľa a skutočne realizovaného rozsahu predmetu zmluvy:

cena v EUR bez DPH	105.958.50,-
20 % sadzba DPH v EUR	21.191.70,-
celková cena v EUR s DPH	12.7150.20,-

4.2.4 Cena za implementáciu spracovania cestovných príkazov ako integrálnej súčasti systému CDS podľa čl. II bodu 2.1.4 je zmluvnými stranami dohodnutá ako súčin dohodnutej ceny sadzby za 1 mernú jednotku a skutočne dodaného počtu merných jednotiek podľa potvrdených akceptačných protokolov o prevzatí predmetu zmluvy. Zmluvné strany berú na vedomie, že celková cena za implementáciu spracovania cestovných príkazov je maximálna a zo strany Poskytovateľa nenárokovateľná, pretože vždy sa pri jej výpočte vychádza v každom jednotlivom prípade zo skutočných potrieb Objednávateľa a skutočne realizovaného rozsahu predmetu zmluvy:

cena v EUR bez DPH	25.000,-
.. % sadzba DPH v EUR	5.000,-
celková cena v EUR s DPH	30.000,-

4.2.5 Cena za mobilnú iCardED aplikáciu podľa čl. II bodu 2.1.5 je zmluvnými stranami dohodnutá ako súčin dohodnutej ceny sadzby za 1 mernú jednotku a skutočne dodaného počtu merných jednotiek podľa potvrdených akceptačných protokolov o prevzatí predmetu zmluvy. Zmluvné strany berú na vedomie, že celková cena za mobilnú iCardED aplikáciu je maximálna a zo strany Poskytovateľa nenárokovateľná, pretože vždy sa pri jej výpočte vychádza v každom jednotlivom prípade zo skutočných potrieb Objednávateľa a skutočne realizovaného rozsahu predmetu zmluvy:

cena v EUR bez DPH	200.000,-
--------------------	-----------

20 % sadzba DPH v EUR	40.000,-
celková cena v EUR s DPH	240.000,-

Podrobná cenová kalkulácia predmetu zmluvy je uvedená v prílohe č. 2 k tejto zmluve.

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

- 4.3 Dohodnutá zmluvná cena zahŕňa všetky náklady poskytovateľa spojené s poskytovaním technickej podpory podľa požiadaviek objednávateľa, ktoré sú uvedené v tejto zmluve a v prílohách č. 1 a 2 k tejto zmluve vrátane všetkých daní, cla, poplatkov, licenčných poplatkov, platieb vybraných v rámci uplatňovania nesadzobných opatrení ustanovených osobitnými predpismi, ako aj iných nákladov súvisiacich s plnením predmetu zmluvy napr. nákladov na licencie tretích strán. Poskytovateľ nie je oprávnený požadovať akúkoľvek inú úhradu za prípadné dodatočné náklady, ktoré si nezapočítal do celkovej ceny za predmet zmluvy.

Článok V

Platobné podmienky

- 5.1 Zmluvné strany sa dohodli že úhrada za predmet zmluvy, resp. jej časti v rozsahu podľa článku IV bude realizovaná bezhotovostným platobným stykom bez poskytnutia zálohovej platby na základe faktúr vystavených poskytovateľom. Poskytovateľ berie na vedomie a súhlasí, že nie je oprávnený požadovať zaplatenie ceny na iný bankový účet než ten, ktorý je uvedený v záhlaví zmluvy; k zmene bankového účtu, na ktorý bude objednávateľ uhrádzať svoje splatné záväzky zo zmluvy môže dôjsť iba uzavretím dodatku k zmluve, predmetom ktorého bude zmena čísla IBAN a/alebo kódu SWIFT (BIC) bankového účtu poskytovateľa v záhlaví zmluvy.
- 5.2 Objednávateľ uhradí paušálnu cenu dohodnutú za jeden kalendárny mesiac v článku IV bodoch 4.2.1 a 4.2.2 za služby technickej podpory podľa článku II bodov 2.1.1 a 2.1.2 tejto zmluvy na základe faktúr vystavených poskytovateľom do päť (5) pracovných dní po uplynutí príslušného kalendárneho mesiaca. V prípade, ak plnenie nebude poskytované za celý kalendárny mesiac, poskytovateľ vystaví faktúru na alikvotnú časť paušálnej platby podľa článku IV bodov 4.2.1 a 4.2.2. Podkladom k schvaľovaniu prvej faktúry musí byť odovzdávací/preberací protokol o začatí poskytovania služieb technickej podpory podľa čl. II bodov 2.1.1 a 2.1.2 podpísaný oprávnenými zástupcami oboch zmluvných strán. Splatnosť faktúry je najneskôr do tridsať (30) dní odo dňa jej doručenia do podateľne Objednávateľa.
- 5.3 Objednávateľ uhradí cenu za plnenia uvedené v článku II bodov 2.1.3 až 2.1.5 tejto zmluvy na základe faktúry vystavenej poskytovateľom do desiatich (10) dní od prevzatia objednaných plnení. Prílohou faktúry musí byť akceptačný protokol o ich prevzatí podpísaný oprávnenými zástupcami oboch zmluvných strán. Splatnosť faktúry je najneskôr do tridsať (30) dní odo dňa jej doručenia do podateľne Objednávateľa.
- 5.4 Objednávateľ je oprávnený započítať akúkoľvek svoju i nesplatnú pohľadávku, ktorú má voči poskytovateľovi, s pohľadávkou, i nesplatnou, ktorá vznikne z tejto zmluvy poskytovateľovi voči objednávateľovi. Zápočet pohľadávok môže objednávateľ uplatniť pri úhrade faktúry poskytovateľa.
- 5.5 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.

- 5.6 Poskytovateľ sa zaväzuje vyhotovené faktúry 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 ich vyhotovení; takto predložená faktúra nesmie byť vo forme obrázku, ale musí byť strojovo čitateľná. Poskytovateľ vyhlasuje, že obsah faktúr zaslaných poštou sa bude zhodovať s obsahom faktúr zaslaných v elektronickej podobe na e-mailovú adresu objednávateľa. Miesto doručenia faktúr v listinnej podobe v listinnej forme je Sociálna poisťovňa, ústredie, Ul. 29. augusta 8 a 10, 813 63 Bratislava. Všetky faktúry a objednávky vyplývajúce z tejto zmluvy podliehajú povinnosti zverejnenia zo strany objednávateľa.
- 5.7 V prípade, že faktúra vystavená poskytovateľom nebude obsahovať všetky zákonom stanovené náležitosti alebo bude obsahovať nesprávne alebo neúplné údaje, objednávateľ má právo takúto faktúru vrátiť poskytovateľovi na jej doplnenie, resp. opravu a poskytovateľ je povinný podľa charakteru nedostatku vystaviť novú, opravenú, resp. doplnenú faktúru s novou lehotou splatnosti. Poskytovateľ je zároveň povinný bezodkladne poslať opravenú alebo novú faktúru znovu aj v elektronickej podobe na e-mailovú adresu uvedenú v bode 5.6 tohto článku zmluvy.

Článok VI

Práva duševného vlastníctva

- 6.1 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 právnej istoty zmluvných strán, ako aj efektívneho a flexibilného používania, spravovania a podpory APV a CDS.
- 6.2 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 v znení neskorších predpisov, vynález, úžitkový vzor, dizajn 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 a pod.) či zamestnanec poskytovateľa na splnenie alebo v rámci plnenia povinností a záväzkov poskytovateľa vyplývajúcich z alebo súvisiacich so zmluvou.
- 6.3 Práva k, na, z alebo inak týkajúce sa predmetov duševného vlastníctva vytvorených poskytovateľom alebo ním poverenou treťou osobou (napr. subdodávateľ, SZČO a pod.) či zamestnancom poskytovateľa na základe tejto zmluvy (ďalej ako „práva duševného vlastníctva“), v celom rozsahu, resp. v rozsahu prípustnom podľa platných právnych predpisov, patria objednávateľovi, resp. ich poskytovateľ bezodplatne prevádza na objednávateľa dňom účinnosti zmluvy, ak neboli prevedené už predtým.
- 6.4 Poskytovateľ vyhlasuje a zodpovedá za to, že ku dňu prevodu, prechodu, odovzdania alebo poskytnutia práv duševného vlastníctva alebo ich časti
- a) predmet duševného vlastníctva ani žiadna jeho časť nemá žiadne právne vady, nie je zaťažovaný právami tretích osôb a ani ich neporušuje; tým nie je dotknuté dojednanie o dielach tretích strán podľa bodu 6.5,
 - b) 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 podľa bodu 6.7.

- 6.5 Poskytovateľ sa zaväzuje k jednotlivým plneniam (vrátane ich akýchkoľvek súčastí zahŕňajúcich tiež software) dodaným alebo poskytnutým poskytovateľom objednávateľovi podľa tejto 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 poskytovateľ udeľuje objednávateľovi právo na ich používanie a úpravu APV a CDS v súlade, v rozsahu, spôsobom a za ďalších podmienok, za ktorých boli tieto plnenia dodané/poskytnuté poskytovateľovi príslušnou treťou osobou.
- 6.6 Poskytovateľ udeľuje objednávateľovi súhlas, aby podľa vlastného uváženia objednávateľ previedol alebo postúpil práva duševného vlastníctva na tretie osoby, prípadne im objednávateľ udelil súhlas používať predmety duševného vlastníctva (sublicenciu) s prípadným právom udeliť sublicenciu, tak aby tieto tretie osoby mohli nadobudnúť, vykonávať práva duševného vlastníctva alebo používať predmety duševného vlastníctva v obdobnom rozsahu ako objednávateľ. V prípade zániku objednávateľa, prechádzajú všetky práva podľa tohto článku na právneho nástupcu objednávateľa.
- 6.7 Tento článok zmluvy sa nevzťahuje na:
- a) štandardný krabicový softvér, na použitie ktorého sa uplatnia licenčné alebo iné podmienky výrobcu;
 - b) sa 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.
- 6.8 Poskytovateľ predloží objednávateľovi kópiu predmetných licenčných alebo iných podmienok tretích strán, resp. licenčných podmienok vzťahujúcich sa na štandardný krabicový softvér najneskôr do dvoch pracovných dní od účinnosti zmluvy. 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. Ak sa toto vyhlásenie ukáže ako nepravdivé, poskytovateľ je povinný nahradiť objednávateľovi náhradu škody, ktorá v tejto súvislosti objednávateľovi vznikne a to vrátane prípadných nákladov na vedenie súdneho sporu.

Článok VII

Zmluvné pokuty a úrok z omeškania

- 7.1 V prípade, ak poskytovateľ neposkytne predmet zmluvy v dohodnutej špecifikácii, rozsahu, kvalite, funkcionalite, riadne a včas podľa článku II bodu 2.1 tejto zmluvy, podľa prílohy č. 1 k tejto zmluve a článku III tejto zmluvy, objednávateľ je oprávnený uplatniť si nárok na zmluvnú pokutu vo výške 500,- EUR za každý, aj začatý deň omeškania a za každé jedno porušenie. Poskytovateľ sa zaväzuje, že takúto zmluvnú pokutu zaplatí objednávateľovi najneskôr do tridsať (30) dní odo dňa jej uplatnenia objednávateľom.
- 7.2 V prípade omeškania poskytovateľa s odstránením väd (chýb) počas záručnej doby podľa článku X bodu 10.5 zmluvy, objednávateľ je oprávnený uplatniť si nárok na zmluvnú pokutu vo výške 100,- EUR, za každú, aj začatú hodinu omeškania. Poskytovateľ sa zaväzuje, že

takúto zmluvnú pokutu zaplatí objednávateľovi najneskôr do tridsať (30) dní odo dňa jej uplatnenia objednávateľom.

- 7.3 V prípade omeškania objednávateľa s úhradou faktúry v dohodnutej lehote je poskytovateľ oprávnený uplatniť si nárok na úrok z omeškania maximálne vo výške určenej nariadením vlády Slovenskej republiky č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení nariadenia vlády č. 303/2014 Z. z. Objednávateľ sa zaväzuje, že takýto úrok z omeškania zaplatí poskytovateľovi najneskôr do tridsať (30) dní odo dňa doručenia jeho vyúčtovania na základe faktúry.
- 7.4 Poskytovateľ sa zaväzuje nahradiť objednávateľovi všetku škodu, ktorú mu spôsobil ako dôsledok neposkytnutia služieb technickej podpory riadne a včas podľa článku II a III tejto zmluvy a podľa prílohy č. 1 k tejto zmluve. Uplatnením zmluvnej pokuty objednávateľom, resp. jej uhradením poskytovateľom sa poskytovateľ nezbavuje povinnosti pokračovať v plnení predmetu zmluvy.
- 7.5 Objednávateľ má právo uplatniť si nárok na dohodnuté zmluvné pokuty voči poskytovateľovi aj po odovzdaní predmetu zmluvy, ak dodatočne zistí, že poskytovateľ porušil záväzky dohodnuté v zmluve.
- 7.6 Uhradením zmluvnej pokuty nezaniká nárok objednávateľa na náhradu škody, ktorá prevyšuje výšku zmluvnej pokuty a nezaniká povinnosť pre porušenie ktorej bola sankcia uložená.
- 7.7 Zmluvné strany sa dohodli, že zodpovednosť za škodu pri plnení záväzkov z tejto zmluvy sa bude riadiť príslušnými ustanoveniami Obchodného zákonníka.
- 7.8 Zmluvné strany súhlasia so započítaním vzájomných pohľadávok v súlade s § 364 Obchodného zákonníka. Zmluvné strany dohodli, že objednávateľ je oprávnený započítať zmluvné pokuty podľa tohto článku zmluvy proti dohodnutej cene za predmet zmluvy alebo jej časti.

Článok VIII

Skončenie zmluvy

- 8.1 Zmluva môže skončiť:
- a) uplynutím doby, na ktorú bola uzatvorená,
 - b) písomnou dohodou zmluvných strán,
 - c) výpoveďou ktorejkoľvek zo zmluvných strán,
 - d) odstúpením od zmluvy ktoroukoľvek zo zmluvných strán.
- 8.2 Zmluvný vzťah môže byť skončený písomnou dohodou zmluvných strán alebo výpoveďou ktorejkoľvek zo zmluvných strán aj bez uvedenia dôvodu. Zmluvné strany sa dohodli na (6) šesťmesačnej výpovednej lehote, ktorá začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po doručení písomnej výpovede druhej zmluvnej strane.
- 8.3 Objednávateľ je oprávnený od zmluvy odstúpiť:
- a) v prípade podstatného porušenia tejto zmluvy poskytovateľom; za podstatné porušenie sa považuje:
 - i. ak poskytovateľ neposkytne služby, ktoré sú predmetom zmluvy v dohodnutom rozsahu, kvalite, špecifikácii riadne a včas a za podmienok dohodnutých v tejto zmluve a v prílohách č. 1 a 2 k tejto zmluve,
 - ii. neodstránenie vady predmetu zmluvy počas záručnej doby v termíne dohodnutom v tejto zmluve,
 - iii. nedodržanie bezpečnostných požiadaviek podľa článku IX tejto zmluvy,

- b) v prípade nepodstatného porušenia zmluvy, len ak poskytovateľ nesplní svoju povinnosť ani v dodatočne primeranej lehote, ktorá mu bola poskytnutá,
 - c) v prípade opakovaného porušenia akýchkoľvek povinností vyplývajúcich z tejto zmluvy alebo všeobecne záväzných právnych predpisov; za opakované porušenie sa považuje preukázateľné porušenie dvakrát a viac,
 - d) podľa § 19 zákona o verejnom obstarávaní.
- 8.4 Odstúpeniu objednávateľa od zmluvy musí predchádzať upozornenie poskytovateľa na neplnenie zmluvných povinností a na možnosť skončenia tejto zmluvy odstúpením.
- 8.5 Poskytovateľ môže od zmluvy odstúpiť v prípade, ak je objednávateľ v omeškaní s úhradou riadne vystavenej faktúry o viac ako 30 dní odo dňa jej doručenia do podateľne objednávateľa. Skončeniu zmluvy musí predchádzať upozornenie na neplnenie platobných povinností objednávateľa a na možnosť ukončenia tejto zmluvy odstúpením.
- 8.6 Odstúpenie od zmluvy bude účinné dňom doručenia písomného oznámenia o odstúpení druhej zmluvnej strane.
- 8.7 Vypovedaním zmluvy nevzniknú objednávateľovi žiadne dodatočné záväzky voči poskytovateľovi.
- 8.8 Odstúpenie od zmluvy sa nedotýka nárokov zmluvných strán na náhradu škody vyplývajúcu z tejto zmluvy.
- 8.9 V prípade, ak tento zmluvný vzťah skončí spôsobom podľa bodu 8.1 písm. b) až d) tohto článku zmluvy v priebehu príslušného mesiaca, poskytovateľ má nárok iba na alikvotnú čiastku z príslušného mesačného paušálneho poplatku v zmysle čl. IV bod 4.2.1 a 4.2.2 tejto zmluvy.
- 8.10 Úplná alebo čiastočná zodpovednosť zmluvnej strany bude vylúčená v prípadoch zásahu vyššej moci.
- 8.11 Pod vyššou mocou sa rozumejú okolnosti, ktoré nastanú po uzatvorení zmluvy ako výsledok nepredvídateľných a zmluvnými stranami neovplyvniteľných prekážok. V prípade, že takáto okolnosť bude brániť v plnení povinností podľa zmluvy poskytovateľovi alebo objednávateľovi, bude povinná zmluvná strana dotknutá vyššou mocou zbavená zodpovednosti za čiastočné alebo úplné nesplnenie záväzkov vyplývajúcich z tejto zmluvy primerane počas doby, po ktorú pôsobili tieto okolnosti.

Článok IX

Ochrana dôverných informácií a kybernetická bezpečnosť

- 9.1 Zmluvné strany, ich zamestnanci ako aj ich subdodávatelia a ich zamestnanci sú povinní zachovávať v tajnosti všetky dôverné informácie, ktoré sú uvedené v tejto zmluve a v jej prílohách a/alebo ktoré budú uvedené v jej dodatkoch a prílohách, a/alebo ktoré im boli poskytnuté, alebo ktoré inak získali v súvislosti so zmluvou, alebo s ktorými sa oboznámili počas plnenia zmluvy, resp. ktoré súvisia s predmetom plnenia, s údajmi, ktoré podliehajú ochrane podľa zákona č. 18/2018 podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenia o ochrane údajov) (GDPR) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s údajmi získanými v rámci predzmluvných rokovaní, ktoré súvisia s touto zmluvou, s výnimkou nasledujúcich prípadov:
- a) ak je poskytnutie informácie od dotknutej zmluvnej strany uložené na základe všeobecne

- záväzných právnych predpisov alebo na základe povinnosti uloženej postupom podľa všeobecne záväzných právnych predpisov (napr. zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov,
- b) ak je informácia verejne dostupná z iného dôvodu, ako je porušenie povinnosti mlčanlivosti dotknutou zmluvnou stranou, informácie, ktoré už sú v deň podpísania zmluvy verejne známe, alebo ktoré je možné už v deň podpísania tejto zmluvy získať z bežne dostupných informačných prostriedkov,
 - c) ak sa jedná o informácie, ktoré sa stanú po podpísaní zmluvy verejne známymi, alebo ktoré možno po tomto dni získať z bežne dostupných informačných prostriedkov,
 - d) ak je informácia poskytnutá odborným poradcom dotknutej zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti, alebo ak sa voči dotknutej zmluvnej strane zaviazali povinnosťou mlčanlivosti,
 - e) ak je to potrebné pre účely akéhokoľvek súdneho, rozhodcovského, správneho alebo iného konania, ktorého je dotknutá zmluvná strana účastníkom,
 - f) ak je informácia poskytnutá so súhlasom druhej zmluvnej strany.
- 9.2 Poskytovateľ ako sprostredkovateľ súčasne s touto zmluvou uzavrie s objednávatelom ako prevádzkovateľom sprostredkovateľskú zmluvu v zmysle článku 28 Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR) a/alebo podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení, ktorá tvorí prílohu č. 6 k tejto zmluve.
- 9.3 Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej zmluvnej strany nevyužijú pre seba alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k dôverným informáciám. Za tretie osoby sa nepokladajú členovia orgánov zmluvných strán, subdodávatelia, audítori alebo právni poradcovia zmluvných strán, ktorí sú ohľadne im sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.
- 9.4 Zmluvné strany, subdodávatelia a ich zamestnanci sa zaväzujú, že všetky zúčastnené osoby a subjekty budú s poskytnutými informáciami a zistenými skutočnosťami nakladať ako s dôvernými informáciami.
- 9.5 Poskytovateľ sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov realizujúcich predmet plnenia zmluvy dodržiavanie:
- a) povinnosti ochrany dôverných informácií a záväzku mlčanlivosti o údajoch, s ktorými počas plnenia predmetu zmluvy pre objednávatel'a prišli do styku, a to aj po ukončení pracovného, resp. služobného pomeru,
 - b) zákazu využitia dôverných informácií, s ktorými prišli do styku pre osobnú potrebu, zákazu ich zverejnenia, poskytnutia a sprístupnenia s výnimkou orgánov činných v trestnom konaní.
- 9.6 Požiadavka v bode 9.5 tohto článku zmluvy bude zabezpečená podpísaním vyhlásenia o mlčanlivosti zo strany príslušného zamestnanca.
- 9.7 Všetky podklady s dôvernými informáciami poskytnuté poskytovateľovi a evidované údaje musia byť po ukončení obchodných vzťahov bez vyzvania odovzdané objednávatel'ovi alebo podľa jeho rozhodnutia vymazané alebo skartované. Táto povinnosť sa vzťahuje aj na vyhotovené kópie. Toto ustanovenie neplatí v prípade vzájomných zmlúv a projektovej

dokumentácie medzi zmluvnými stranami, ktoré ale nesmú byť bez súhlasu objednávateľa sprístupnené tretej osobe inak, ako to dovoľuje táto zmluva.

- 9.8 Poskytovateľ sa zaväzuje, že sa v žiadnom prípade bez vedomia objednávateľa nepokúsi získať prístup k informáciám, ktoré:
- a) sú prenášané na poskytovanú infraštruktúru a sú súčasťou prenášaných údajov,
 - b) nie sú pre neho potrebné na výkon poskytovanej služby a ani ich žiadnym spôsobom nezneužije v prípade, ak sa k nim neoprávnené dostane.
- 9.9 Poskytovateľ sa zaväzuje, že pred každým plánovaným servisným zásahom zašle na adresu dispecing@socpoist.sk zoznam zamestnancov poskytovateľa, vykonávajúcich servisný zásah, s termínom prístupu do informačného systému Sociálnej poisťovne v štruktúre podľa prílohy č. 5 k tejto zmluve a pri každom neplánovanom (operatívnom) zásahu vyplní a zašle požadované údaje pokiaľ možno pred, inak ihneď po vykonaní zásahu.
- 9.10 Zmluvné strany sa zaväzujú, že budú ochraňovať dôverné informácie druhej zmluvnej strany s rovnakou starostlivosťou, ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti.
- 9.11 Ustanovenia predchádzajúcich bodov budú platiť aj po dobe platnosti a účinnosti zmluvy, a to až do doby, kedy sa informácie stanú verejne známymi.
- 9.12 Poskytovateľ súčasne s touto zmluvou uzavrie ako tretia osoba s Objednávatelom ako prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorá zmluva tvorí prílohu č. 7 k tejto zmluve.

Čl. X

Záručné podmienky a zodpovednosť za vady

- 10.1 Poskytovateľ sa zaväzuje, že poskytne predmet zmluvy podľa podmienok dohodnutých v tejto zmluve a v prílohách k tejto zmluve.
- 10.2 Poskytovateľ sa zaväzuje, že na predmete tejto zmluvy podľa tejto zmluvy nie sú žiadne právne vady a vyhlasuje, že je oprávnený vykonávať a udeliť všetky práva spojené s dodaním predmetu zmluvy a zodpovedá za ich nerušený výkon objednávateľom.
- 10.3 V prípade, že tretia osoba akýmkoľvek spôsobom uplatní práva na dodaný predmet zmluvy, ktoré sú nezlučiteľné s právami vykonávanými objednávateľom, poskytovateľ sa zaväzuje vykonať všetky opatrenia potrebné na nápravu a nerušený výkon práv objednávateľa, vrátane prípadných návrhov na začatie súdneho konania.
- 10.4 Poskytovateľ poskytne objednávateľovi na realizované služby technickej podpory záručnú dobu 24 mesiacov, ktorá začne plynúť od ich protokolárneho odovzdania a prevzatia podľa článku III bodov 3.1 a 3.2 zmluvy. Záruka sa vzťahuje na prevádzkyschopnosť a funkčnosť predmetu zmluvy za predpokladu riadnej starostlivosti a údržby predmetu zmluvy objednávateľom.
- 10.5 Poskytovateľ sa zaväzuje, že počas záručnej doby bezplatne (vrátane dopravy) odstráni vady predmetu zmluvy najneskôr do 48 hodín od telefonického hlásenia vady (poruchy), následne potvrdenej e-mailovou správou na dohodnutej e-mailovej adrese objednávateľa podľa bodu 10.8 tohto článku zmluvy.
- 10.6 Odstránením vád sa rozumie zabezpečenie prevádzkyschopnosti predmetu zmluvy tak, aby bola zabezpečená minimálne v takom rozsahu a kvalite ako pred vznikom vady (poruchy).

- 10.7 Poskytovateľ určí zodpovedných zamestnancov na kontakt s objednávateľom a spôsob komunikácie pri zabezpečovaní záručného servisu a predloží objednávateľovi najneskôr do dvoch pracovných dní od účinnosti zmluvy.
- 10.8 Ak pôjde o vadu, ktorá by mohla spôsobiť alebo spôsobila na predmete zmluvy vznik havarijného stavu, poskytovateľ sa zaväzuje nastúpiť na odstránenie väd bezodkladne od ich oznámenia objednávateľom, ktoré v tomto prípade môže byť telefonické na čísle alebo prostredníctvom e-mailu@.....
- 10.9 Pri zodpovednosti za vady sa zmluvné strany budú riadiť ustanoveniami § 422 a nasl. Obchodného zákonníka, ktoré upravujú nároky zo zodpovednosti za vady tovaru.

Článok XI

Osobitné ustanovenia

- 11.1 Poskytovateľ (v prípade skupiny dodávateľov každý člen skupiny dodávateľov), jeho subdodávateľia a subdodávateľia podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov (ďalej len „zákon o registri partnerov verejného sektora“), ktorí sú uvedení v prílohe č. 3 k zmluve musia byť v čase uzavretia zmluvy, v súlade s § 11 ods. 1 zákona o verejnom obstarávaní zapísaní v registri partnerov verejného sektora podľa zákona o registri partnerov verejného sektora, ak im zákon o registri partnerov verejného sektora takúto povinnosť ukladá. Objednávateľ neuzatvorí túto zmluvu s poskytovateľom, ak v čase uzavretia zmluvy nebude mať poskytovateľ, jeho subdodávateľia alebo subdodávateľia podľa zákona o registri partnerov verejného sektora splnenú podmienku zápisu v registri partnerov verejného sektora, alebo ak on, jeho subdodávateľia alebo subdodávateľia podľa zákona o registri partnerov verejného sektora, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora, majú v registri partnerov verejného sektora zapísaného konečného užívateľa výhod, ktorým je osoba podľa § 11 ods. 1 písmena c) zákona o verejnom obstarávaní, alebo ak poskytovateľovi bude uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní.
- 11.2 Objednávateľ môže podľa § 19 ods. 3 zákona o verejnom obstarávaní odstúpiť od zmluvy, ak poskytovateľ v čase uzatvorenia zmluvy nebol zapísaný v registri partnerov verejného sektora alebo ak bol vymazaný z registra partnerov verejného sektora alebo ak mu bol právoplatne uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní. Ak sa po uzavretí zmluvy stala konečným užívateľom výhod poskytovateľa, jeho subdodávateľa, osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní, môže objednávateľ odstúpiť od zmluvy po uplynutí 30 dní odo dňa, keď táto skutočnosť nastala, ak táto skutočnosť stále trvá.
- 11.3 Na plnenie predmetu zmluvy môže poskytovateľ využiť subdodávateľov. Poskytovateľ je povinný pri uzatvorení zmluvy uviesť zoznam subdodávateľov, ktorý obsahuje údaje o všetkých známych subdodávateľoch poskytovateľa v čase uzatvorenia tejto zmluvy a údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Zoznam subdodávateľov tvorí prílohu č. 3 k tejto zmluve a obsahuje okrem uvedených údajov aj podiel plnenia zo zmluvy v % a stručný opis časti zmluvy, ktorá bude predmetom subdodávky.

- 11.4 Poskytovateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi, ktorý je uvedený v prílohe č. 3 k tejto zmluve najneskôr do piatich (5) pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví zmluvy.
- 11.5 V prípade zmeny subdodávateľa je poskytovateľ povinný najneskôr tri (3) pracovné dni pred zmenou subdodávateľa písomne oznámiť objednávateľovi údaje o navrhovanom novom subdodávateľovi a o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Na nového subdodávateľa sa vzťahuje povinnosť byť zapísaný v registri partnerov verejného sektora podľa zákona o registri partnerov verejného sektora. Zmena nového subdodávateľa sa vykoná zápisom o zmene prílohy č. 3 k zmluve, ktorý nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jeho zverejnenia v registri; vzor zápisu o zmene prílohy k zmluve tvorí prílohu č. 4 k tejto zmluve; osobami oprávnenými konať vo veciach zmeny prílohy č. 3 k zmluve sú:
za poskytovateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
XY	Projektový manažér	XXX	XXX.XXX@eviden.com	XXX

za objednávateľa:

Titul/meno/Priezvisko	Funkcia	Korešpondenčná adresa pre písomný kontakt	E-mail	Telefón
XY	Vedúci	XXX	XXX.XXX@socpoist.sk	XXX

- 11.6 Navrhovaný subdodávateľ musí spĺňať podmienky účasti týkajúce sa osobného postavenia podľa § 32 zákona o verejnom obstarávaní a nesmú u neho existovať dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7 a 8 zákona o verejnom obstarávaní.
- 11.7 Využitím subdodávateľov nie je dotknutá zodpovednosť poskytovateľa za plnenie predmetu zmluvy.
- 11.8 Ak sa poskytovateľ v súvislosti s plnením povinností podľa zmluvy dostane do súdneho konania s treťou osobou, alebo by takéto súdne konanie hrozilo, bezodkladne o tom vyrozumie objednávateľa. Objednávateľ bude povinný na požiadanie poskytovateľa dať ihneď k dispozícii poskytovateľovi všetky potrebné informácie a podklady. Táto povinnosť vznikne príslušným vyrozumením. Uvedená povinnosť bude platiť recipročne aj pre poskytovateľa, pokiaľ by sa do takéhoto konania dostal objednávateľ. Vzájomná podpora sa poskytne iba v prípadoch, ak nedošlo k porušeniu všeobecne záväzných právnych predpisov v súvislosti s plnením zmluvy.
- 11.9 Poskytovateľ je povinný bezodkladne písomne oznámiť objednávateľovi začatie akéhokoľvek súdneho, rozhodcovského, exekučného, konkurzného, reštrukturalizačného alebo obdobného konania, ktoré sa začalo proti nemu alebo ktoré sám inicioval v súvislosti s predmetom tejto zmluvy. Ďalej je povinný bezodkladne oznámiť objednávateľovi, ak

- niektorý z veriteľov poskytovateľa podal proti nemu návrh na vyhlásenie konkurzu a návrh na povolenie reštrukturalizácie alebo vstup do likvidácie a jej ukončenie.
- 11.10 Poskytovateľ nepostúpi, bez predchádzajúceho písomného súhlasu druhej zmluvnej strany, ani inak neprevedie pohľadávky, práva a povinnosti vyplývajúce z tejto zmluvy v celku ani v jej časti inému subjektu.
- 11.11 Skončením zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce zo zmluvy s výnimkou ustanovení, ktoré sa týkajú nároku na náhradu škody vzniknutej porušením tejto zmluvy, nároku na zaplatenie zmluvnej pokuty podľa ustanovení tejto zmluvy, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení zmluvy, napr. záruka, ochrana dôverných informácií, informačná a kybernetická bezpečnosť.
- 11.12 Zmluvné strany sa dohodli, že všetky spory, ktoré vzniknú v súvislosti s plnením tejto zmluvy, budú riešiť predovšetkým dohodou. Prípadné spory, o ktorých sa zmluvné strany nedohodli, budú postúpené na rozhodnutie vecne a miestne príslušnému súdu.
- 11.13 Poskytovateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu svojich identifikačných a kontaktných údajov.
- 11.14 Zmluvu je možné meniť počas jej trvania bez nového verejného obstarávania v súlade s ustanovením § 18 zákona o verejnom obstarávaní. Zmena zmluvy musí byť písomná.
- 11.15 Poskytovateľ vyhlasuje, že ku dňu uzavretia tejto zmluvy je/nie je závislou osobou voči objednávateľovi v zmysle § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov. Každú zmenu súvisiacu s personálnym, ekonomickým alebo iným prepojením voči objednávateľovi v súvislosti s ustanovením § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov je poskytovateľ povinný objednávateľovi písomne oznámiť a to do 5 dní odo dňa vzniku zmeny.

Článok XII

Záverečné ustanovenia

- 12.1 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. Poskytovateľ berie na vedomie povinnosť objednávateľa zverejniť túto zmluvu ako aj jednotlivé faktúry vyplývajúce z tejto zmluvy a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy vrátane jej príloh v plnom rozsahu.
- 12.2 Táto zmluva sa uzatvára na dobu určitú 36 mesiacov odo dňa nadobudnutia jej účinnosti. Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky.
- 12.3 Zmluvu je možné meniť alebo dopĺňať iba formou písomných dodatkov, ktoré budú jej neoddeliteľnou súčasťou. Písomná zmena alebo doplnenie prílohy č. 3 k zmluve sa bude vykonávať formou zápisu o zmene prílohy podľa vzoru uvedeného v prílohe č. 4 k zmluve. Zmluvu je možné meniť okrem dôvodov uvedených v tejto zmluve len v prípade, ak zmeny a doplnenia nebudú v rozpore s ustanovením § 18 zákona o verejnom obstarávaní a európskou legislatívou.
- 12.4 Zmluvné strany sa v súlade s ustanovením § 262 ods. 1 Obchodného zákonníka dohodli, že záväzkový vzťah založený touto zmluvou sa spravuje ustanoveniami Obchodného zákonníka, zákona o verejnom obstarávaní, zákona č. 185/2015 Z. z. Autorský zákon

a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky a európskou legislatívou.

12.5 Neoddeliteľnou súčasťou tejto zmluvy sú prílohy:

- príloha č. 1 Špecifikácia predmetu zmluvy
- príloha č. 2 Podrobná cenová kalkulácia predmetu zmluvy
- príloha č. 3 Zoznam subdodávateľov
- príloha č. 4 Zápis o zmene prílohy
- príloha č. 5 Evidencia servisných zásahov
- príloha č. 6 Sprostredkovateľská zmluva
- príloha č. 7 Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

12.6 Ak by sa niektoré ustanovenia tejto zmluvy stali celkom alebo sčasti neúčinnými, nemá to vplyv na platnosť zmluvy. Zmluvné strany sa zaväzujú neúčinné ustanovenia preformulovať, doplniť alebo nahradiť tak, aby sa dosiahol účel zmluvy.

12.7 Zmluva je vyhotovená v štyroch rovnopisoch, z ktorých každý má platnosť originálu. Každá zmluvná strana dostane po dva rovnopisy tejto zmluvy.

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

V Bratislave dňa

V Bratislave dňa

Za poskytovateľa:

Za objednávateľa:

Ing. Pavel Struhárik
konateľ
Eviden Slovakia s.r.o.

Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

ŠPECIFIKÁCIA PREDMETU ZMLUVY

Predmetom zmluvy je technická podpora pre aplikačné programové vybavenie (APV) pre Centrálny dochádzkový systém (CDS), zapracovanie zmenových požiadaviek v prípade požiadavky do centrálného dochádzkového systému, zabezpečiť prípadný upgrade, dodávku, resp. výmenu hardware (HW) komponentov dochádzkového systému vrátane plnej integrácie do existujúceho systému v rozsahu:

- 1 podpora softvéru po dobu 36 mesiacov odo dňa nadobudnutia účinnosti zmluvy,
- 2 technická podpora komponentov pre dochádzkový a prístupový systém po dobu 36 mesiacov odo dňa nadobudnutia účinnosti zmluvy,
- 3 hardvérové rozšírenie prístupového systému (na základe požiadavky objednávateľa),
- 4 implementácia spracovania cestovných príkazov ako integrálnej súčasti systému CDS (na základe požiadavky objednávateľa),
- 5 úpravy aplikácie iCard (na základe požiadavky objednávateľa).

Popis súčasného stavu:

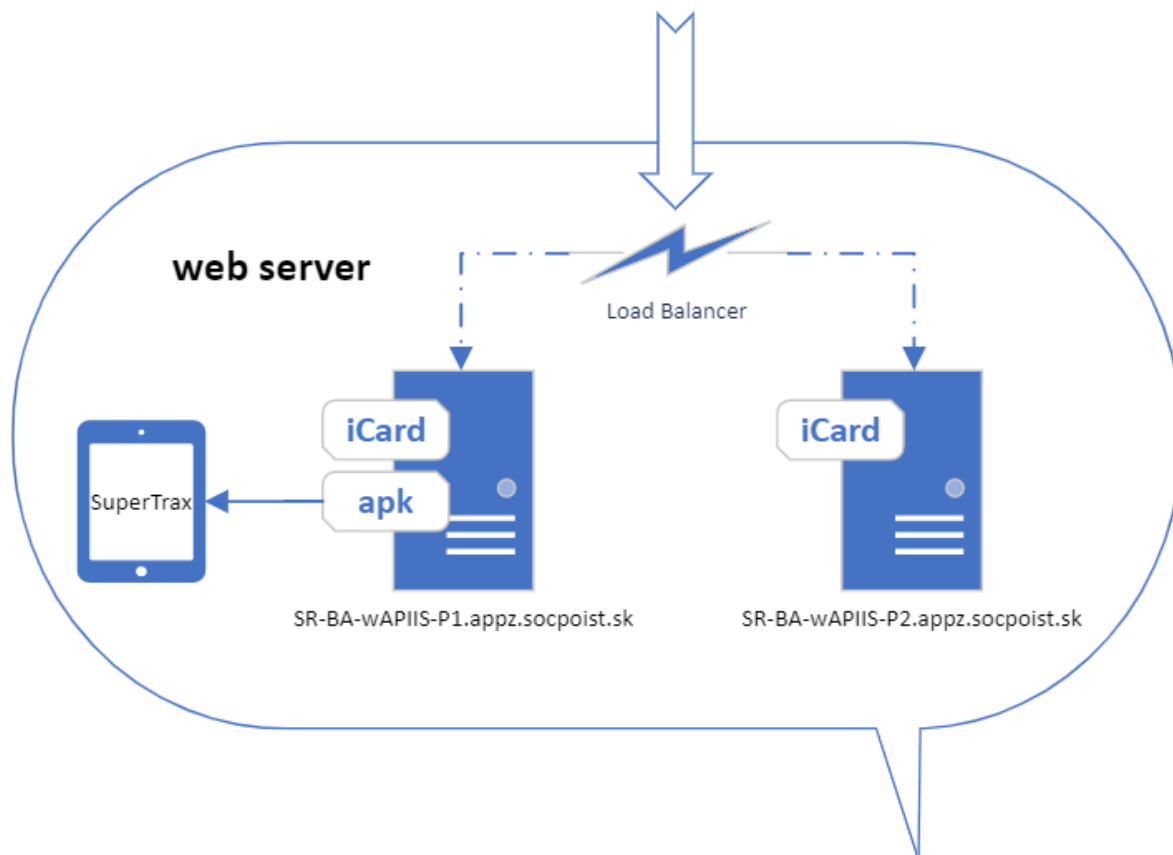
➤ Aktuálna štruktúra servera:

- Použitá technológia servera je OS Windows Server 2008 R2, SQL server MS SQL Server 2008 R2 a ASP.NET

Web server ktorého súčasťou sú dva oddelené servery:

- SR-BA-wAPIIS-P1.appz.socpoist.sk
- SR-BA-wAPIIS-P2.appz.socpoist.sk

- Load Balancer rozdeľuje komunikáciu na jeden alebo druhý server, IS iCard je nainštalovaný na oboch serveroch, na serveri SR-BA-wAPIIS-P1.appz.socpoist.sk je inštalovaná web služba pre komunikáciu so snímačmi SuperTrax.



Databázový / Aplikačný Cluster:

- cluster je tvorený z troch rovnocenných Node-ov:

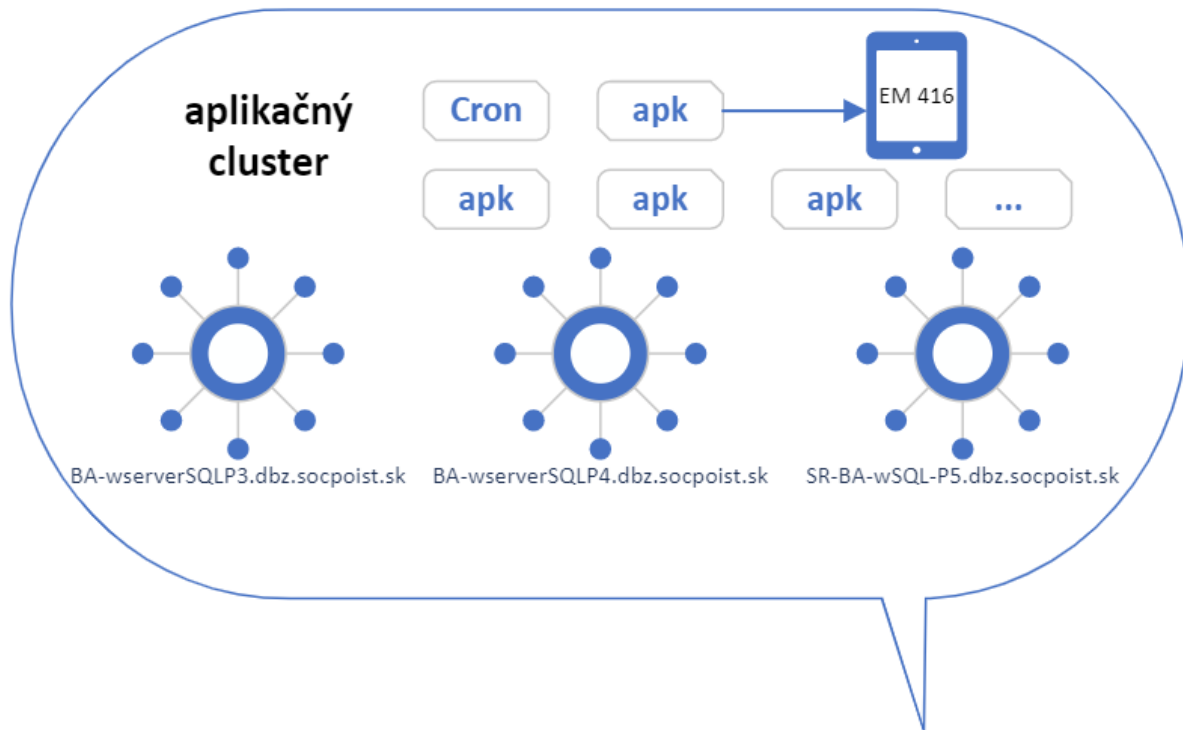
BA-wserverSQLP3.dbz.socpoist.sk

BA-wserverSQLP4.dbz.socpoist.sk

SR-BA-wSQL-P5.dbz.socpoist.sk

Obsahuje nasledovné inštalácie:

- aplikácie pre komunikáciu pôvodných snímačov typu EM 316
- integrácia IS iCard so SAP
- aplikácia pre posielanie výročných emailov
- pravidelné spracovanie dochádzky
- služba Cron



- integrácia so SAP je momentálne spustená cez JavaConnector. Počas migrácie je potrebné v spolupráci technikov IS iCard a SAP obnoviť komunikáciu na novom serveri, alt. využiť komunikáciu cez web služby.

Opis predmetu zákazky

1 Podpora softvéru

Podpora Softwaru vrátane implementácie legislatívnych zmien, ktoré súvisia s HR (Ľudské zdroje) politikou, ako aj zabezpečenie bezporuchovej prevádzky APV, vrátane podpory pri prevádzke žiadanej cez Service desk, vrátane riešenia denných hlásení, poskytovania konzultácií, opravy chýb, drobných úprav a nasadenia zmien funkcionalít APV do testovania a prevádzky, kontrola/zmeny parametrických nastavení systému, obnovenie prevádzky po vyriešení havarijnej situácie), poskytovanej podľa potreby aj formou prítomnosti zamestnanca/ zamestnancov poskytovateľa na pracovisku objednávateľa (v rozsahu max. 6 Ľlovekodní (ČD) ročne), za stanovenú paušálnu sumu.

Cez Service desk objednávateľ komunikuje so všetkými externými dodávateľmi prostredníctvom automatizovaného komunikačného nástroja Service desk, prostredníctvom ktorého predloží poskytovateľovi požiadavku (ticket), ktorá bude obsahovať:

- špecifikáciu požadovanej služby/tovaru,
- rozsah/počet požadovaných služieb/tovaru,
- navrhovaný termín poskytnutia/dodania služby/tovaru.

Ticket (požiadavka) sa dá prirovnať k [počítačovému súboru](#), ktorý v sebe zahŕňa všetky informácie o zásahoch oddelenia technickej podpory s cieľom vyriešiť problém nahlásený koncovým užívateľom.

2 Technická podpora komponentov pre dochádzkový a prístupový systém

Technická podpora komponentov pre prístupový systém v režime on-site, t. j. odstránenie výpadku do 48 hodín pre vstup osôb do chránených priestorov.

Rozsah plnenia - služby zabezpečujúce technickú podporu pre APV a CDS, najmä riešenie denných hlásení, poskytovanie konzultácií, oprava chýb, drobné úpravy, zapracovanie zmenových požiadaviek v prípade požiadavky do centrálného dochádzkového systému, zabezpečiť prípadný upgrade, dodávku, resp. výmenu HW komponentov dochádzkového systému vrátane plnej integrácie do existujúceho systému.

Úroveň poskytovanej služby pre predmet zmluvy podľa bodu 1 a 2:

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

- kritická priorita - vada systému, ktorá znemožňuje prácu so systémom ako celkom, alebo znemožňuje používanie systému, alebo celoplošný problém, alebo tiež nedostupnosť kritických funkcionalít; alebo výrazné obmedzenie prevádzkyschopnosti systému alebo jeho častí ohrozujúce dodržanie významného míľnika, pričom vplyv vady nie je možné dočasne eliminovať náhradným postupom,
- vysoká priorita - vada systému, ktorá znemožňuje prácu so systémom ako celkom; alebo znemožňuje používanie systému; alebo celoplošný problém, alebo tiež nedostupnosť kritických funkcionalít; alebo výrazné obmedzenie prevádzkyschopnosti systému alebo jeho častí, pričom vplyv vady je možné dočasne eliminovať náhradným postupom,
- normálna priorita - vady systému, ktoré postihujú menej dôležité funkcionality a nemajú kritický dopad na prácu používateľov.

Maximálne hodnoty časových limitov pre odstraňovanie problémov:

Tabuľka č. 1

Priorita	Doba potvrdenia previatia hlásenia	Reakčná doba	Servisná doba
Kritická	2 hodiny	4 hodiny	24 hodín
Vysoká	2 hodiny	4 hodiny	48 hodín
Normálna	2 hodiny	48 hodín	96 hodín

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

Riešenie incidentov nahlásených centrálnym dispečingom zahŕňa riešenie incidentov súvisiacich s prevádzkou podporovaného APV v súlade s definovanými SLA.

Rozpis činností súvisiacich s riešením incidentov:

- simulácia chybových stavov vo vývojovom prostredí poskytovateľa v prípade nahlásenia vady,
- identifikácia príčiny,
- zabezpečenie realizácie riešenia.

Riešenie incidentov nepokrýva hardvér, sieťovú infraštruktúru a operačný systém. Riešenie incidentov je poskytované telefonicky alebo vzdialeným prístupom typu Remote Desktop Protocol (RDP) z pracoviska poskytovateľa alebo v mieste sídla objednávateľa.

Poskytovanie konzultácií:

- osobné alebo telefonické poskytnutie odbornej konzultácie pre kľúčových používateľov ohľadom spôsobu realizácie nových biznis požiadaviek v priestoroch určených objednávateľom. Termín a čas konzultácie bude vzájomne dohodnutý projektovými manažérmi.

Riešenie servisných požiadaviek:

- plnenie servisných požiadaviek na vyžiadanie,
- mimoaplikačné výbery, opravy dát v databáze na vyžiadanie,
- testovanie APV na prechod SW tretích strán (napr. OS, DB, aplikačný server, integračné rozhrania) na vyššiu verziu alebo inú technológiu,
- realizácia drobných úprav aplikácie, ako napr. úprava reportov, prípadne zmena nastavenia systému, v celkovom rozsahu maximálne 6 človekodní za rok.

Súčinnosť pri riešení problémov súvisiacich s podporovaným APV:

- súčinnosť pri riešení problémov podporovaných aplikácií, ktoré boli spôsobené treťou osobou alebo problémami technickej infraštruktúry IT. Poskytovateľ vykoná súčinnosť poskytovaním pomoci pri analýze problémov, predkladaním návrhov a doporučení pre možné riešenia,
- súčinnosť poskytovateľa pri riešení problémov súvisiacich s APV je poskytovaná telefonicky z pracoviska poskytovateľa, v mieste sídla objednávateľa.

Odstraňovanie vád (chyb) APV:

- objednávatel' hlási poskytovateľovi vzniknuté vady (chyby) APV písomnou špecifikáciou prostredníctvom Helpdeskového nástroja na dohodnutú mailovú adresu alebo telefonicky na dohodnutom tel. čísle s tým, že telefonické hlásenie bude dodatočne potvrdené i písomným hlásením,
- objednávatel' pri hlásení vady (chyby) v písomnej špecifikácii uvedie čo najpresnejší užívateľský popis práce pred výskytom vady (chyby), prioritu v bode **Úroveň poskytovanej služby**, aktuálnu verziu APV, a v prípade systémových a aplikačných výpisov zašle aj znenie týchto výpisov prostredníctvom printscreenu obrazoviek. Pri opakujúcom sa výskyte rovnakej vady (chyby) bude objednávatel' odosielať aj výpis z eventlogov na základe požiadavky poskytovateľa,
- po doručení hlásenia má poskytovateľ služby povinnosť odoslať objednávatel'ovi potvrdenie o prevzatí hlásenia na mailovú adresu objednávatel'a,
- po doručení hlásenia má poskytovateľ právo otestovať alebo vykonať kontrolu funkčnosti počítačových programov priamo u objednávatel'a,
- zásah zo strany poskytovateľa služby sa uskutoční podľa stanovenej priority v bode **Úroveň poskytovanej služby**
- reakčná doba je považovaná za ukončenú zo strany objednávatel'a zaslaním informácie o stave riešenia alebo o ďalšom postupe riešenia poskytovateľom písomnou formou na mailovú adresu objednávatel'a,
- servisná doba je považovaná za ukončenú zo strany objednávatel'a zaslaním informácie o odstránení vady (chyby) vrátane popisu riešenia zo strany poskytovateľa písomnou formou na mailovú adresu objednávatel'a,
- v prípade straty dát vplyvom vady (chyby) HW alebo SW konfigurácie je obnova dát mimo rozsahu služieb a nezapočítava sa do garantovaného času na odstránenie vady (chyby). Obnova dát je vykonávaná administrátorom objednávatel'a. Zálohovanie dát je povinnosťou objednávatel'a,
- pred odstránením vady (chyby), ktorá sa nedá odstrániť do servisnej doby uvedenej v tabuľke č. 1, bude dohodnutý rozsah prác potrebných na odstránenie vady (chyby) s termínom realizácie novej verzie (release) APV v zmluvne dohodnutej forme. Predpokladom odstránenia vád je objednávatel'om zabezpečená podpora SW komponentov tretích osôb, na ktorých je APV prevádzkované,
- odstránenie každej vady (chyby) sa bude realizovať ako súčasť konkrétnej verzie (release) APV. O odstránení vady (chyby) bude urobený písomný záznam.

Profylaktika:

- Profylaktika zahŕňa jedenkrát ročne prezretie nastavení a konfigurácie prostredia jednotlivých APV, na ktoré sa vzťahuje podpora.
- Termín plánovanej kontroly poskytovateľ vždy dohodne telefonicky alebo písomne s objednávatel'om. Pravidelná profylaktika pozostáva z nasledujúcich krokov:

- a) revízia systémových log-súborov na serveroch,
- b) kontrola zaplnenosti úložiska systému,
- c) odstránenie problémov zistených počas preventívnej prehliadky, ktoré umožní systém riešiť v priebehu vykonávanej kontroly.

Poskytovateľ vyhodnotí závery z profylaktiky a vytvorí plán na odstránenie zistených problémov.

3 HW rozšírenie prístupového systému,

prípadne výmena za nové, výrobcom podporované terminály, ktoré budú kompatibilné so systémom iCard. Zariadenia musia komunikovať v on-line režime, s okamžitým obojsmerným prenosom dát do riadiacich jednotiek aj do databázy. V prípade ponuky iných ako iCard podporovaných zariadení je nevyhnutá náhrada všetkých zariadení, ktoré sú nekompatibilné s existujúcim systémom iCard, tak aby neobmedzil každodennú prevádzku na pobočkách SP (zoznam komponentov).

4 Implementácia spracovania cestovných príkazov ako integrálnej súčasti systému CDS

Zpracovanie nového modulu: „Cestovne príkazy“ **najneskôr do 6 mesiacov** po odsúhlasení začiatku implementácie zo strany Objednávateľa:

Objednávateľ zadáva požiadavku vytvoriť ručne skupinu pre schvaľovateľa. Administrátor systému objednávateľa bude mať právo tieto skupiny podľa potreby vytvoriť.

- Pri vrátení CP (cestovného príkazu) spracovateľom, bude možnosť vložiť krátky text, kde sa uvedie dôvod vrátenia CP.
- Zamestnanec (ZC) bude mať možnosť pri zadávaní CP vložiť sumu predpokladaných nákladov.
- Náklady (predpokladané, žiadané a uznané) doplniť do základnej tabuľky pre hromadné schvaľovanie CP pre oprávneného ZC alebo rozpočtára.
- Systém pošle zamestnancovi hlásenie, že má po ceste dať na likvidáciu CP do 10 pracovných dní. Spúšťač pre posielanie notifikácie by mohol byť dátum, ktorý je uvedený na CP ako koniec SC (služobnej cesty). Ďalšia notifikácia príde na piaty deň po konci SC. Ak do 10 pracovných dní nevyúčtuje CP, tak mu vybehne notifikácia, že nesplnil 10 pracovných dní a musí napísať dôvod omeškania. Niekde bude možnosť vložiť text s dôvodom oneskoreného odovzdania CP (prosím naceniť každú notifikáciu zvlášť).
- Ak je cesta kratšia ako 5 h. bude mať schvaľovateľ možnosť dopísať sumu náhrady stravného do vyúčtovania.
- Pri vyúčtovaní, musí ZC podať správu o služobnej ceste. Systém ponúkne možnosť zakliknúť akou formou podá správu – buď ústne alebo písomne.
- Keď ZC musí odovzdať písomnú správu. Bude aktívne tlačidlo, vlož prílohu o správe. Ak ju nevloží, tlačidlo odoslať na schválenie nebude aktívne.

- Je potrebné odoslať exportnú dávku do SAP/HR, v ktorej sa odošlú potrebné informácie o vyrovnaní CP, u ktorých bolo v predošlom mesiaci vykonané schválenie vyúčtovania CP. Informácie, ktoré je potrebné odoslať, sú podobné ako v prípade stravného pre ZC. Informácie: osobné_číslo_ZC dátum mzdová_dávka suma uznaná. Dátum by bol zhodný s dátumom odsúhlaseného vyúčtovania likvidátorom. Mzdová dávka by bola pri preplatku 8735 alebo doplatku 5905.
- CP iCard_A_vzor doplniť nasledovné v časti cestovný príkaz č.:
 - „Dátum a podpis zodpovedného zamestnanca“ plus veta „Súhlasím s vyslaním na pracovnú cestu a vo finančnej operácii je možné pokračovať.“
 - „Dátum a podpis zamestnanca, ktorý elektronicky schválil pracovnú cestu“ doplniť o vetu „Vo finančnej operácii je možné pokračovať“ v prípade ak oprávnený ZC neschváli SC vetu: „Vo finančnej operácii nie je možné pokračovať“
 - „Podpis pokladníka“ nahradiť „Dátum a podpis rozpočtára“ plus vety „Vo finančnej operácii je možné pokračovať“ a „Finančné prostriedky sú zabezpečené v rozpočte na položke 631001.51210000 Fond: **číslo** Fin. stred. **číslo**“. **Číslo** je údaj, ktorý zadá rola – rozpočtár v procese schvaľovania a sem sa to číslo dotiahne. Ak rozpočtár neodsúhlasí CP tak sa vypíše veta „Vo finančnej operácii nie je možné pokračovať“.
- CP iCard_A_vzor doplniť nasledovne v časti vyúčtovanie služobnej cesty:
 - K vete „Vyhlasujem, že som všetky údaje uviedol(a) úplne a správne.“ Doplniť vetu „V prípade nedoplatku/preplatku súhlasím so zúčtovaním so mzdou.“ „Vo finančnej operácii je možné pokračovať“
 - „So spôsobom vykonania a vyúčtovania súhlasím“ a „Vo finančnej operácii je možné pokračovať“ plus „Dátum a podpis oprávneného zamestnanca“
 - Vetu „Vyrovnanie vyúčtovania bolo vykonané“ nahradiť vetou: „Dátum, meno, priezvisko a podpis zamestnanca, ktorý upravil vyúčtovanie“ a k tomu vetu „Vo finančnej operácii je možné pokračovať“
 - „Dátum, meno, priezvisko a podpis zamestnanca, ktorý schválil úpravu vyúčtovania“ a k tomu vetu „Vo finančnej operácii je možné pokračovať“
- Vytvoriť štatistiku pre kroky v IS kto a kedy sa prihlásil a aké kroky vykonal. Potrebujeme zoznam krokov o ktoré sa jedná. V systéme sú logované zmeny, ktoré sú v dokumente vykonané.
- Zpracovať priamo do procesu legislatívu schvaľovania, konkrétne – zákon č. 357/2015 o finančnej kontrole a audite a zákon č. 431/2002 o účtovníctve. (je možné zameniť tlačidlo „odsúhlasiť“ za vetu „Vo finančnej operácii je možné pokračovať.“ Pri tlačidle „vrátiť“ a „zamietnuť“ použiť formuláciu „Vo finančnej operácii nie je možné pokračovať“, „Poslať na schválenie“ z Rozpisu CP použiť formuláciu „Súhlasím s vyslaním na pracovnú cestu. Vo finančnej operácii je možné pokračovať.“ Pri tlačidle „Poslať na kontrolu“ z Vyúčtovania „Vyhlasujem, že som všetky údaje uviedol úplne a správne. V prípade nedoplatku/preplatku súhlasím so zúčtovaním so mzdou. Vo finančnej operácii je možné pokračovať.“)

- V prípade preddavku, si zamestnanec iba vypíše sumu, ktorá mu bola vyplatená, aby sa dalo urobiť vyúčtovanie. (Schvaľovanie preddavku podľa kompetenčného poriadku spadá pod iného zamestnanca ako schvaľovanie CP.)
- Zabezpečiť ukladanie CP a príloh na náš server. Vytvorenie úložiska pre CP a prílohy. Pre 17 000 CP ročne, 5 príloh ku každému CP, veľkosť súboru 4MB, s potrebou archivovať 10 rokov je potrebných 3,5 TB úložiska iba pre prílohy. Samotné CP sú uložené ako záznamy v databáze a neukladajú sa vo forme tlačových výstupov.
- Umožniť pre ľudí, ktorí sú na cestách často, vyrobiť CP pre viac ciest súčasne.
- Do procesu okrem role: vyslaný ZC, oprávnený ZC schvaľovať služobnú cestu zahrnúť aj role rozpočtár, likvidátor, schvaľovateľ-likvidátor a ku procesu upraviť stavy. (k tomuto nižšie návrh na stavy a ich definovanie)
- Pri roli „Rozpočtár“ je potrebná veta: „Potvrdzujem, že finančné prostriedky sú zabezpečené v rozpočte na položke 631001.51210000 Fond: číslo Fin. stred. číslo,„. Číslo bude dopísané rozpočtárom a bude sa doťahovať do CP na tlač.
- Pri roli „Likvidátor“ je potrebná veta: „Kópia súhlasí s originálom pri týchto účtovných záznamov:“ a bude tam priestor, kde likvidátor doplní zoznam účtovných záznamov. Je potrebné definovať o aké záznamy sa jedná.
- Pri vyplňaní nového CP: nech je pole typ predvyplnené – tuzemský CP, potrebuje údaj doprav. prostriedkov s možnosťou výberu (O – osobný vlak, R – rýchlik, A – autobus, L – lietadlo, P – pešo, AUS – auto služobné, AUV – auto vlastné, MHD – mestská hromadná doprava)
- Pri vyplňaní – detail rozpisu cesty: predvyplniť čas od 7.00, do 15.00
- Pri vyplňaní – doklad: pole „spôsob platby“ nebude aktívne, lebo SP nepoužíva firemnú kartu.

Systém iCard spracováva cestovné príkazy tak, že po zamietnutí CP na ktorejkoľvek úrovni kontroly sa CP vráti vždy na prepracovanie žiadateľovi. Následne sa celý proces schvaľovania opakuje.

- Rozpracovaný: zamestnanec zadá nový CP, systém vygeneruje číslo CP, stav je ukončený odoslaním na oprávneného zamestnanca s vyjadrením „Súhlasím s vyslaním na pracovnú cestu. Vo finančnej operácii je možné pokračovať.“
- Schvaľovaný: CP čaká na kontrolu a schválenie oprávneného zamestnanca, stav je ukončený odoslaním na rozpočtára s vyjadrením „Vo finančnej operácii je možné pokračovať“ /ak neschválené, tak: „Vo finančnej operácii nie je možné pokračovať“
- Schvaľovaný rozpočtárom: CP čaká na schválenie rozpočtárom, stav je ukončený odoslaním na zamestnanca s vyjadrením „Vo finančnej operácii je možné pokračovať“ / ak neschválené, tak: „Vo finančnej operácii nie je možné pokračovať“
- Schválený CP: zamestnanec môže odísť na služobnú cestu. Po ukončení služobnej cesty spraví vyúčtovanie CP. Stav je ukončený odoslaním na oprávneného zamestnanca s vyjadrením „Vyhlasujem, že som všetky údaje uviedol úplne a správne. V prípade

nedoplatku/preplatku súhlasím so zúčtovaním so mzdou. Vo finančnej operácii je možné pokračovať.“

- **Kontrolovaný:** CP čaká na kontrolu a schválenie vyúčtovania oprávneného zamestnanca, stav je ukončený odoslaním na likvidátora s vyjadrením „Vo finančnej operácii je možné pokračovať“ / ak neschválené, tak: „Vo finančnej operácii nie je možné pokračovať“ vráti zamestnancovi na prepracovanie, resp. úpravu, doplnenie
- **Kontrolovaný likvidátorom:** CP čaká na kontrolu vyúčtovania likvidátorom, stav je ukončený odoslaním na schvaľovateľ likvidátor s vyjadrením „Vo finančnej operácii je možné pokračovať“ / ak neschválené, tak: „Vo finančnej operácii nie je možné pokračovať“ vráti oprávnenému zamestnancovi na prepracovanie, resp. úpravu, doplnenie a ten vracia zamestnancovi.
- **Schvaľovaný likvidátorom:** CP čaká na kontrolu vyúčtovania od schvaľovateľa likvidátora, stav je ukončený odoslaním na rozpočtára s vyjadrením „Vo finančnej operácii je možné pokračovať“ / ak neschválené, tak: „Vo finančnej operácii nie je možné pokračovať“ vráti likvidátorovi
- **Kontrolovaný rozpočtárom:** CP čaká na kontrolu vyúčtovania od rozpočtára, stav je ukončený odsúhlasením vyúčtovania rozpočtárom s vyjadrením „Vo finančnej operácii je možné pokračovať“ / ak neschválené, tak: „Vo finančnej operácii nie je možné pokračovať“ vráti likvidátorovi schvaľovateľovi a ten likvidátorovi.
- **Vyrovňovaný:** systém vygeneruje vetu pre SAP-HR, stav je ukončený odoslaním do SAP-HR
- **Uzavretý:** pre nulové vyrovnanie nie je potrebné generovať vety pre SAP-HR, preto zo stavu kontrolovaný rozpočtárom prejde rovno do stavu uzavretý.

5 Úpravy aplikácie iCard na základe požiadavky objednávateľa

V rozsahu kumulatívne 400 človekodní počas trvania zmluvy = 3 roky/36 mesiacov. Počet človekodní je stanovený len ako predpokladaný, pričom objednávateľ nie je povinný počas platnosti a účinnosti zmluvy vyčerpať, resp. objednať celý predpokladaný počet človekodní, ale len počet, ktorý bude zodpovedať aktuálnej potrebe objednávateľa. Objedávateľ si vyhradzuje právo nevyčerpať celkovú cenu za predmet zmluvy a poskytovateľ sa zaväzuje uvedené právo objednávateľa akceptovať.

Kvantitatívna špecifikácia predmetu zmluvy:

P.č.	Technická podpora pre Centrálny dochádzkový systém	Jednotka	Počet
1	Podpora SW: vrátane implementácie legislatívnych zmien, ktoré súvisia s HR politikou ako aj zabezpečenie bezporuchovej prevádzky APV, vrátane podpory pri prevádzke žiadanej cez Service desk, vrátane riešenia denných hlásení, poskytovania konzultácií, opravy chýb, drobných úprav a nasadenia zmien funkcionalít APV do testovania a prevádzky, kontrola/zmeny parametrických nastavení systému, obnovenie prevádzky po vyriešení havarijnej situácie), poskytované podľa potreby aj formou prítomnosti	1 mesiac	36

	zamestnanca/zamestnancov poskytovateľa na pracovisku objednávateľa (v rozsahu max. 6 ČD ročne), za stanovenú paušálnu sumu. Poskytovateľ bude túto položku fakturovať mesačne najneskôr do 5 pracovných dní od začiatku nasledujúceho mesiaca poskytovania služby.		
2	Technická podpora komponentov pre dochádzkový a prístupový systém v režime on-site, t. j. odstránenie výpadku do 48 hodín pre vstup osôb do chránených priestorov. Poskytovateľ bude túto položku fakturovať mesačne najneskôr do 5 pracovných dní od začiatku nasledujúceho mesiaca poskytovania služby.	1 mesiac	36
3	HW rozšírenie prístupového systému, prípadne výmena za nové, výrobcom podporované terminály, ktoré budú kompatibilné so systémom iCard. Zariadenia musia komunikovať v on-line režime, s okamžitým obojsmerným prenosom dát do riadiacich jednotiek aj do databázy. V prípade ponuky iných ako iCard podporovaných zariadení je nevyhnutná náhrada všetkých zariadení, ktoré sú nekompatibilné s existujúcim systémom iCard, tak aby neobmedzil každodennú prevádzku na pobočkách SP (zoznam komponentov).		
3a	Prístupový snímač Mifare kariet (Multi RFID/5) Výrobca: Axess TMC; Označenie výroku: RFID/5	ks	50
3b	Riadiaca jednotka RJPS2-LAN, s pamäťou na 10 000 kariet a 30 000 udalostí Výrobca: Eltis, Označenie výrobku: RJPS2L	ks	28
	Riadiaca jednotka RJPS2 bez LAN, s pamäťou na 10 000 kariet a 30 000 udalostí Výrobca: Eltis, Označenie výrobku: RJPS2L	ks	7
	Prevodníkova riadiaca jednotka RJPS2-PREV Výrobca: Eltis, Označenie výrobku: RJPS2P	ks	2
3c	Zámok elektromagnetický štandardný, nízkooodberový 12V 150 mA, bez signalizácie otvorenia dverí	ks	2
	Zámok elektromagnetický reverzný protipožiarny zámok 12V, bez certifikácie, bez signalizácie otvorenia dverí	ks	8
	Zámok elektromagnetický štandardný, nízkooodberový 12V 150 mA, so signalizáciou otvorenia dverí	ks	5
	Zámok elektromagnetický reverzný protipožiarny zámok 12V, bez certifikácie, so signalizáciou otvorenia dverí	ks	10
	Zámok elektromagnetický štandardný ÚZKY 66 x 16 x 28 mm, 12V/200mA <u>Použitie pre tenké zárubne a skryté montáže.</u> Bez lišty.	ks	5
	Zámok elektromagnetický reverzný ÚZKY 66 x 16 x 28 mm, 12V / 200 mA <u>Použitie pre tenké zárubne a skryté montáže.</u> Bez lišty.	ks	5
	Lišta 250 x 25 x 3 mm, obojstranná	ks	1
	Lišta uhlová, L, Zn pre úzke zámky	ks	1
	Chránička na kabeláž zámku - dvojkrídlové dvere resp.	ks	1
	Elektromagnetický zámok so signalizáciou, LED, zabezpeč. sila 280 kg, povrchová montáž	ks	1
	Elektromagnetický zámok so signalizáciou, LED, zabezpeč. sila 2x280 kg, povrchová	ks	1

	montáž		
	Elektromagnetický zámok so signalizáciou, LED, zabezpeč. sila 500 kg, povrchová montáž	ks	1
	Dverová lišta EMZ krátka so signalizáciou - dverová lišta 40 cm s madlom s plastovým úchytom a elektromagnetom so signalizáciou stavu dverí, povrchová montáž na existujúce dvere, zabezpečovacia sila 300 kg, rozmery (d x š x h) 400 x 105 x 63 mm, teplotný rozsah: -20°C do +70°C, saténový anodizovaný hliník, spotreba 550 mA na 12 VDC	ks	3
	Sada troch konzol pre povrchové elektromagnetické zámky 300 kg	ks	2
	Sada troch konzol pre povrchové elektromagnetické zámky 600 kg	ks	1
3d	Záložný zdroj pre prístupové snímače 12V/1A 1,3Ah	ks	1
	Záložný zdroj pre prístupové snímače 13,8V/4A + akumulátor 7Ah, UPS režim 3,3A, 55W, IP20, plechová skrinka 260x210x75 mm, biela	ks	20
	Záložný zdroj pre prístupové snímače 13,8V/10A + akumulátor 18Ah, UPS režim 8A, 140W, IP20, plechová skrinka 300x285x80 mm, biela	ks	13
	AC/DC napájací zdroj 12V/4,5A pre montáž na DIN lištu, pre prístupový systém bez zálohovania prevádzky akumulátorom	ks	1
	Náhradný akumulátor 12V/7Ah	ks	5
	Náhradný akumulátor 12V/18Ah	ks	3
3e	Skrinka 400x300x200 (VxŠxH) mm pre uloženie komponentov PS, uzamykateľná kľúčom	ks	17
	Skrinka 500x400x200 (VxŠxH) mm pre uloženie komponentov PS, uzamykateľná kľúčom	ks	10
	Inštalčná krabica na stenu, 150x110x70, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1
	Inštalčná krabica na stenu, 190x140x70, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1
	Inštalčná krabica na stenu, 240x190x90, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1
	Inštalčná krabica na stenu, 300x220x120, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	2
	Inštalčná krabica na stenu, 380x300x120, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	2
	Inštalčná krabica na stenu, 452x380x130, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1
3f	Zelené (panic) núdzové výstupné tlačidlo resetovateľné, priehľadný plastový kryt pre núdzové tlačidlo	ks	10
3g	Diaľkové ovládanie pre otváranie elektromagnetického zámku z recepcie (prijímač 2 kanály, 433MHz + diaľkový ovládač 4 kanálový (umožňuje ovládať 2 prijímače))	ks	3
3h	Siréna audiovizuálna 6-14VDC; rozmery D=110mm, H=47mm; 122dB; IP65; kábel	ks	2

3i	Elektroinštalačný a montážny materiál (kabeláž + lišty + spojovací materiál)		
	Lišta káblová biela 15x10x2000mm	ks	10
	Lišta káblová biela 25x25x2000mm	ks	10
	Štruktúrovaná kabeláž FTP Cat 5E krabica 305m	ks	10
3j	Karty - bezkontaktná čipová karta, pracovná frekvencia 13,56 MHz,• biela,• s možnosťou farebnej obojstrannej potlače karty – retransferová metóda tlače,• rozmery 85,6mm x 53,98mm x 0,76mm. Obal na kartu z priehľadného pružného plastu, s klipom štipca.	ks	5000
3k	Inštalčné, konfiguračné a ostatné práce súvisiace s implementáciou HW	ČD	100
4	Implementácia spracovania cestovných príkazov ako integrálnej súčasti systému CDS		
4a	Implementácia modulu spracovania CP a zaškolenie kľúčových používateľov	ČD	50
5	Úpravy aplikácie iCard na základe požiadavky objednávateľa	ČD	400

Zoznam SW funkcionalít existujúceho CDS

Oblasť	Kategória	Voľba (konkrétna funkcia systému)
Dochádzka	Číselníky	Číselník hodinových vyhodnotení
Dochádzka	Číselníky	Číselník mzdových druhov
Dochádzka	Číselníky	Číselník nehodinových vyhodnotení
Dochádzka	Číselníky	Číselník prerušení
Dochádzka	Číselníky	Číselník spôsobov zaokrúhlenia
Dochádzka	Číselníky	Číselník výpočtových vzorcov
Dochádzka	Číselníky	Prepojenie dochádzky a miezd
Dochádzka	Hromadné operácie	Generovanie plánu nároku na stravné
Dochádzka	Hromadné operácie	Hromadné rušenie spracovania
Dochádzka	Hromadné operácie	Hromadné spracovanie
Dochádzka	Hromadné operácie	Hromadný dopočet
Dochádzka	Hromadné operácie	Hromadný prepočet
Dochádzka	Hromadné operácie	Nastavenie uzávierky
Dochádzka	Hromadné operácie	Prenos z pracovného kalendára
Dochádzka	Nastavenia	Definícia ročného hodinového výkazu
Dochádzka	Nastavenia	Definícia ročného nehodinového výkazu
Dochádzka	Nastavenia	Definícia voliteľnej zostavy
Dochádzka	Nastavenia	Nastavenia dochádzky
Dochádzka	Nastavenia	Nastavenia reportov
Dochádzka	Nastavenia	Nastavenie chybových stavov
Dochádzka	Práca nad skupinou osôb	Denné vyhodnotenie
Dochádzka	Práca nad skupinou osôb	Mesačné signo
Dochádzka	Práca nad skupinou osôb	Okamžitý stav
Dochádzka	Práca nad skupinou osôb	Osobné kalendáre
Dochádzka	Práca nad skupinou osôb	Prehľad dennej evidencie
Dochádzka	Práca nad skupinou osôb	Prehľad pracovných zmien
Dochádzka	Práca nad skupinou osôb	Prehľad vyhodnotení
Dochádzka	Práca nad skupinou osôb	Zmena hodinových výkazov
Dochádzka	Práca nad skupinou osôb	Zmena nehodinových výkazov

Dochádzka	Práca s jednotlivcom	Mesačná evidencia
Dochádzka	Práca s jednotlivcom	Mesačné vyhodnotenie
Dochádzka	Práca s jednotlivcom	Mesačný prehľad snímaní
Dochádzka	Práca s jednotlivcom	Ročná evidencia
Dochádzka	Práca s jednotlivcom	Ročný výkaz hodinový
Dochádzka	Práca s jednotlivcom	Ročný výkaz nehodinový
Dochádzka	Práca s jednotlivcom	Ročný výkaz po mesiacoch
Dochádzka	Práca s jednotlivcom	WEB snímač
Dochádzka	Prehľady	Denný opis snímaní
Dochádzka	Prehľady	Kontrola poradia snímania
Dochádzka	Prehľady	Opis snímaní
Dochádzka	Prehľady	Prehľad dochádzky
Dochádzka	Prehľady	Prítomnosť na pracovisku
Dochádzka	Prehľady	Rozpis zmien
Dochádzka	Prehľady	Zoznam chybových stavov
Dochádzka	Prehľady	Zoznam opravených chýb
Dochádzka	Procesy	Hromadné schvaľovanie
Dochádzka	Procesy	Prehľad žiadaniek
Dochádzka	Procesy	Schvaľovacie reťazce
Dochádzka	Procesy	Schvaľovanie žiadaniek
Dochádzka	Procesy	Zastupovanie
Dochádzka	Procesy	Žiadanky
Dochádzka	Report/Export	Dochádzkový list
Dochádzka	Report/Export	Mesačný výkaz
Dochádzka	Report/Export	Okamžitý stav
Dochádzka	Report/Export	Počet osôb na pracovných zmenách
Dochádzka	Report/Export	Predbežná ME s aktuálnym snímaním
Dochádzka	Report/Export	Predbežná mesačná evidencia
Dochádzka	Report/Export	Štatistika vyhodnotenia dochádzky
Dochádzka	Report/Export	Týždenný výkaz
Dochádzka	Report/Export	Voliteľné zostavy

Dochádzka	Report/Export	Záverečná mesačná evidencia
Menu používateľa	Prítomnosť na pracovisku	Export do PDF
Prístup	Číselníky a nastavenia	Časové zóny
Prístup	Číselníky a nastavenia	Formát návštevného lístka
Prístup	Číselníky a nastavenia	Nastavenie prístupu
Prístup	Číselníky a nastavenia	Preukazy
Prístup	Číselníky a nastavenia	Pridelovanie práv
Prístup	Číselníky a nastavenia	Pridelovanie práv s ľuďmi
Prístup	Číselníky a nastavenia	Priestorové zóny
Prístup	Číselníky a nastavenia	Typy automobilov
Prístup	Návštevy	Číselník členenia návštev
Prístup	Návštevy	Číselník dôvodov návštev
Prístup	Návštevy	Číselník návštevníkov
Prístup	Návštevy	Evidencia návštev a ich práv
Prístup	Prehľady	Prehľad Molekula
Prístup	Prehľady	Prehľad prístupové skupiny
Prístup	Prehľady	Prehľad Skupina-Snimač-Osoba
Prístup	Prehľady	Prechod osôb
Prístup	Prehľady	Prechod Zóna
Prístup	Prehľady	Prechod Zóna - Sumár
Spoločné	Aplikačné práva	Číselník používateľov
Spoločné	Aplikačné práva	Číselník vlastníkov
Spoločné	Aplikačné práva	Prehľad osôb a ich spracovateľov
Spoločné	Aplikačné práva	Prístupové profily
Spoločné	Číselníky a nastavenia	Číselník gratulačných notifikácií
Spoločné	Číselníky a nastavenia	Číselník štátov
Spoločné	Číselníky a nastavenia	Skupinové členenie
Spoločné	Číselníky a nastavenia	Skupinové členenie s ľuďmi
Spoločné	Číselníky a nastavenia	Sviatky
Spoločné	Číselníky a nastavenia	Tituly pred menom
Spoločné	Číselníky a nastavenia	Tituly za menom

Spoločné	Kalendár	Kalendár
Spoločné	Kalendár	Kombinácie dní
Spoločné	Kalendár	Náhradné zmeny
Spoločné	Kalendár	Pracovná zmena
Spoločné	Kalendár	Príplatky
Spoločné	Kalendár	Šablóna
Spoločné	Kalendár	Typy pracovných zmien
Spoločné	Konfigurácia	Definícia exportných dát
Spoločné	Konfigurácia	Licencie
Spoločné	Konfigurácia	Nastavenie aplikácie
Spoločné	Konfigurácia	Nastavenie importu
Spoločné	Konfigurácia	Nastavenie jazykov
Spoločné	Konfigurácia	Nastavenie overovania
Spoločné	Konfigurácia	Nastavenie upozornenia
Spoločné	Konfigurácia	Ovládač
Spoločné	Konfigurácia	Rozmiestnenie tlačidiel
Spoločné	Konfigurácia	Snímač
Spoločné	Konfigurácia	Systémové číselníky
Spoločné	Monitoring systému	História prihlásení
Spoločné	Monitoring systému	Mazanie starých údajov
Spoločné	Monitoring systému	Monitoring HW - aktuálny
Spoločné	Monitoring systému	Monitoring HW - prehľad
Spoločné	Monitoring systému	Prehľad logov
Spoločné	Monitoring systému	Prehľad nezariadených snímaní
Spoločné	Monitoring systému	Správa EPS a Synchronizácia
Spoločné	Monitoring systému	Zoznam prihlásených osôb
Spoločné	Personálna identifikácia	Hromadná tlač kariet
Spoločné	Personálna identifikácia	Hromadná zmena údajov
Spoločné	Personálna identifikácia	Nastavenie mailovej notifikácie
Spoločné	Personálna identifikácia	Osobná karta
Spoločné	Personálna identifikácia	Prehľad časových údajov

Spoločné	Personálna identifikácia	Rýchla zmena údajov
Spoločné	Personálna identifikácia	Výberové kritériá
Spoločné	Personálna identifikácia	Zmena hesla
Spoločné	Personálna identifikácia	Zmena skupinového zaradenia
Spoločné	Personálna identifikácia	Zoznam zamestnancov
Spoločné	Report/Export	Externé SQL
Spoločné	Report/Export	Tvorba exportnej dávky
Stravovanie	Číselníky	Cena
Stravovanie	Číselníky	Druhy jedál
Stravovanie	Číselníky	Generovanie kalendára
Stravovanie	Číselníky	Jedálne
Stravovanie	Číselníky	Nastavenia stravy
Stravovanie	Číselníky	Pridelenie limitu skupine
Stravovanie	Číselníky	Strava
Stravovanie	Číselníky	Typy jedál
Stravovanie	Číselníky	Úprava kalendára
Stravovanie	Číselníky	Výdajne
Stravovanie	Číselníky	Vytvorenie limitu
Stravovanie	Číselníky	Zoznam jedál
Stravovanie	Jedáleň	Generovanie jedálneho lístka
Stravovanie	Jedáleň	Hromadný prepočet stravy
Stravovanie	Jedáleň	Objednanie stravy
Stravovanie	Jedáleň	Tlač jedálneho lístka
Stravovanie	Jedáleň	Tvorba jedálneho lístka
Stravovanie	Nákupy	Nákupy v bufete podľa stravníka
Stravovanie	Nákupy	Nákupy v jedálni
Stravovanie	Nákupy	Sortiment
Stravovanie	Prehľady/Export	Finančný prehľad za skupinu
Stravovanie	Prehľady/Export	Finančný prehľad za stravníka
Stravovanie	Prehľady/Export	Prehľad podľa stravníkov
Stravovanie	Prehľady/Export	Prehľad za skupinu

Rozmiestnenie existujúcich zariadení po jednotlivých pracoviskách Sociálnej poisťovne vrátane uvedenia jednotlivých typov

Bratislava

Kód	Umiestnenie	Názov	Ovládač	Typ snímača
0; 1	BA - 29/10 Turniket ľavá strana vstup	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
0; 2	BA - 29/10 Turniket ľavá strana výstup	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
0; 3	BA - 29/8 Chodba 1 poschodie - červený kútik	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8 1NP	RJ16Driver	RJ12 RFID5
0; 4	BA - Cukrová rampa	RJ16; 10.3.101.39; Cukrova rampa	RJ16Driver	RJ12 RFID5
0; 5 in	BA - Cukrová bránička vstup	RJ16; 10.3.101.38; Cukrova bránička	RJ16Driver	RJ12 RFID5
0; 5 out	BA - Cukrová bránička výstup	RJ16; 10.3.101.38; Cukrova bránička	RJ16Driver	RJ12 RFID5
0in; 8	BA - 29/8 Turniket ľavá strana vstup	RJ16; 10.3.80.38; Ústredie SP 29 augusta 8 turnik	RJ16Driver	RJ12 RFID5
0out; 8	BA - 29/8 Turniket ľavá strana výstup	RJ16; 10.3.80.38; Ústredie SP 29 augusta 8 turnik	RJ16Driver	RJ12 RFID5
1; 1	BA - 29/10 Turniket pravá strana vstup	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
1; 2	BA - 29/10 Turniket pravá strana výstup	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
10; 2	BA - 29/8 Dvere "chodba VS / m.c.H7" Serverovňa	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
11; 2	BA - 29/8 Dvere "chodba VS / m.c.H6" Serverovňa	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
12; 2	BA - 29/8 Dvere chodba VS / m.c.H5" Sala IBM	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
14in; 2	BA - 29/8 Dvere "chodba/m.c.432B" Jukebox z vonku	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
14out; 2	BA - 29/8 Dvere "chodba/m.c.432B" Jukebox z vnútra	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
16in; 2	BA - 29/8 Dvere "chodba/m.c.432C" Jukebox z vonku	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
16out; 2	BA - 29/8 Dvere "chodba/m.c.432C" Jukebox z vnútra	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
18; 2	BA - 29/8 Dvere "chodba / m.c.432A" priestor	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5

	OAS			
1in; 8	BA - 29/8 Turniket pravá strana vstup	RJ16; 10.3.80.38; Ústredie SP 29 augusta 8 turnik	RJ16Driver	RJ12 RFID5
1out; 8	BA - 29/8 Turniket pravá strana výstup	RJ16; 10.3.80.38; Ústredie SP 29 augusta 8 turnik	RJ16Driver	RJ12 RFID5
2; 1	BA - 29/10 Prechod z nádvoria	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
13; 2	BA - 29/8 Dvere "chodba VS/chodba VS" pri nakl. výťahu	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
2; 2	BA - 29/10 Prechod do nádvoria	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
30in; 2	BA - 29/8 Parkovisko vstup dvere c.1204	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
30out; 2	BA - 29/8 Parkovisko výstup dvere c.1204	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
4; 1	BA - 29/10 Vrátnica cukrová ulica vstup	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
4; 2	BA - 29/10 Vrátnica cukrová ulica výstup	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
7; 2	BA - 29/8 Dvere "vestibul / chodba VS"	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
8; 2	BA - 29/8 Dvere "chodba VS / m.c.H8" Serverovňa	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
9; 2	BA - 29/8 Dvere "chodba VS / m.c.15" Sala IBM	RJ16; 10.3.80.39; Ústredie SP ul. 29 augusta 8	RJ16Driver	RJ12 RFID5
BA Hag 01	BA Hagarova Vstup in	RJ16; 10.4.30.39; BA Hagarova	RJ16Driver	RJ12 RFID5
BA Hag 02	BA Hagarova Vstup out	RJ16; 10.4.30.39; BA Hagarova	RJ16Driver	RJ12 RFID5
BA Hag 03	BA Hagarová Mreža in	RJ16; 10.4.30.39; BA Hagarova	RJ16Driver	RJ12 RFID5
BA Hag 04	BA Hagarova Mreža out	RJ16; 10.4.30.39; BA Hagarova	RJ16Driver	RJ12 RFID5
BA Nev 11	BA Nevädzova miest. 116 vstup	RJ16; 10.4.19.31; Nevädzova 1	RJ16Driver	RJ12 RFID5
BA Nev 12	BA Nevädzova miest. 116 výstup	RJ16; 10.4.19.31; Nevädzova 1	RJ16Driver	RJ12 RFID5
BA Nev 21	BA Nevädzova miest. 112 vstup	RJ16; 10.4.19.32; Nevädzova 2	RJ16Driver	RJ12 RFID5
BA Nev 22	BA Nevädzova miest. 112 výstup	RJ16; 10.4.19.32; Nevädzova 2	RJ16Driver	RJ12 RFID5
BA Nev 31	BA Nevädzova miest. 104 vstup - bránička	RJ16; 10.4.19.33; Nevädzova 3	RJ16Driver	RJ12 RFID5

BA Nev 32	BA Nevädzova miest. 104 výstup - bránička	RJ16; 10.4.19.33; Nevädzova 3	RJ16Driver	RJ12 RFID5
BA Nev 41	BA Nevädzova hlavný vchod vstup	RJ16; 10.4.19.34; Nevädzova 4	RJ16Driver	RJ12 RFID5
BA Nev 42	BA Nevädzova hlavný vchod výstup	RJ16; 10.4.19.34; Nevädzova 4	RJ16Driver	RJ12 RFID5
BA Nev 51	BA Nevädzova bránička recepcia vstup	RJ16; 10.4.19.35; Nevädzova 5	RJ16Driver	RJ12 RFID5
BA Nev 52	BA Nevädzova bránička recepcia výstup	RJ16; 10.4.19.35; Nevädzova 5	RJ16Driver	RJ12 RFID5
BA Nev 61	BA Nevädzova miest. 137 vstup	RJ16; 10.4.19.36; Nevädzova 6	RJ16Driver	RJ12 RFID5
BA Nev 62	BA Nevädzova miest. 137 výstup	RJ16; 10.4.19.36; Nevädzova 6	RJ16Driver	RJ12 RFID5
3; 1	BA - 29/10 Chodba gen. riaditeľa	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
5; 1	Chodba na prízemí za vrátnicou 29/10	RJ16; 10.3.100.39; Ústredie SP ul. 29 augusta 10	RJ16Driver	RJ12 RFID5
01	Bratislava Ústredie, Cukrová	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava
07	Nevädzová 7	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava
08	Nevädzová 8	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava
02	Vrátnica 8	SuperTrax	termSeverSuperTrax	EM 316
03	Vrátnica 8	SuperTrax	termSeverSuperTrax	EM 316
04	Ul.29 augusta 10	SuperTrax	termSeverSuperTrax	EM 316
05	Ul.29 augusta 10	SuperTrax	termSeverSuperTrax	EM 316
06	dvorný objekt	SuperTrax	termSeverSuperTrax	EM 316
0A	Petržalka	SuperTrax	termSeverSuperTrax	EM 316
0C	Hagarová 9	SuperTrax	termSeverSuperTrax	EM 316
0E	DaRZ Staré Hory	SuperTrax	termSeverSuperTrax	EM 316
0G	Ústredie SP, Nevädzova BA	SuperTrax	termSeverSuperTrax	EM 316
0I	Ústredie SP, pridaný 21.6.2013	SuperTrax	termSeverSuperTrax	EM 316
13	Bratislava, Záhradnícka 153	SuperTrax	termSeverSuperTrax	EM 316
14	Bratislava, Záhradnícka 153	SuperTrax	termSeverSuperTrax	EM 316
15	Bratislava, Záhradnícka 31	SuperTrax	termSeverSuperTrax	EM 316
16	Bratislava, Záhradnícka	SuperTrax	termSeverSuperTrax	EM 316

	31			
09	ESO - KAMO BA	SuperTrax	termSeverSuperTrax	EM 316 dochádzka
0B	Karlova Ves	SuperTrax	termSeverSuperTrax	EM 316 dochádzka

Svidník

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7T	Svidník - Sovietskych hrdinov 121	SuperTrax	termSeverSuperTrax	EM 316	admin
7U	Svidník - Sovietskych hrdinov 121	SuperTrax	termSeverSuperTrax	EM 316	admin

Michalovce

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
8A	Michalovce - Nám. osloboditeľov 1	SuperTrax	termSeverSuperTrax	EM 316	admin

Piešťany

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
25	Sládkovičova 10, Piešťany	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Hlohovec

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
26	Jarmočná 3, Hlohovec	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Senica

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2A	Hollého 1219, 905 01 Senica	SuperTrax	termSeverSuperTrax	EM 316	admin
2B	Hollého 1219, 905 01 Senica	SuperTrax	termSeverSuperTrax	EM 316	admin
2C	Sotinská 1577/1A, 90501 Senica	SuperTrax	termSeverSuperTrax	EM 316	admin
2D	Sotinská 1577/1A, 90501 Senica	SuperTrax	termSeverSuperTrax	EM 316	admin

Holíč

Kód	Umiestnenie	Názov	Ovládač	Typ	Správca
-----	-------------	-------	---------	-----	---------

				snímača	
2E	ul. SNP 32, 908 51 Holíč	SuperTrax	termSeverSuperTrax	EM 316	admin

Myjava

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2F	nám. M. R. Štefánika 561, 907 01Myjava	SuperTrax	termSeverSuperTrax	EM 316	admin

Šaľa

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2H	Šaľa	SuperTrax	termSeverSuperTrax	EM 316	admin

Galanta

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2I	Z. Kodálya 1629/48, Galanta	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
2G	Mierové námestie (povodne - Hlavná 987) Galanta	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
1; 21	Galanta Posuvné dvere	RJ16 10.5.16.39; Galanta	RJ16Driver	RJ12 RFID5	admin

Dunajská
Streda

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2K	Galantská cesta 693/5, Dunajská Streda	SuperTrax	termSeverSuperTrax	EM 316	admin
2L	Galantská cesta 693/5, Dunajská Streda	SuperTrax	termSeverSuperTrax	EM 316	admin

Malacky

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2N	Malacky,	SuperTrax	termSeverSuperTrax	EM 316	admin

	Bernoláková 1/A			dochádzka	
--	-----------------	--	--	-----------	--

Pezinok

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2O	Pezinok, Radničné nám.	SuperTrax	termSeverSuperTrax	EM 316 dochádzka	admin

Trenčín

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
31	Jilemnického 3760, Trenčín	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
32	Jilemnického 3760, Trenčín	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
33	Jilemnického 3760, Trenčín	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Nové Mesto nad Váhom

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
34	Jánošíkova, Nové mesto n. Váhom	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
35	Jánošíkova, Nové mesto n. Váhom	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Prievidza

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
3A	Matrice slovenskej 10, 97101 Prievidza	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Považská Bystrica

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
3H	Kukučínova 208/23, Považská Bystrica 017 53	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Dubnica n/Váhom

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
3J	Bratislavská 4051, Dubnica n/Váhom 018 41	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Púchov

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
3L	Royova 1048, Púchov 020 01	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Nitra

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
41	Slančíkovej 3, 950 43 Nitra	SuperTrax	termSeverSuperTrax	EM 316	admin
42	Slančíkovej 3, 950 43 Nitra	SuperTrax	termSeverSuperTrax	EM 316	admin
1; 18	NR - 1. Poschodie	RJ16 10.5.32.39; Nitra	RJ16Driver	RJ12 RFID5	Nitra

Zlaté Moravce

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
43	Sládkovičova 3, 953 01 Zlaté Moravce	SuperTrax	termSeverSuperTrax	EM 316	admin

Topoľčany

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
4A	M.R.Štefánika 2269/18, 955 01 Topoľčany	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
4B	M.R.Štefánika 2269/18, 955 01 Topoľčany	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
4C	M.R.Štefánika 2269/18, 955 01 Topoľčany	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Partizánske

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
4F	Jesenského fir. Wolker Partizánske	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Bánovce nad Bebravou

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
4G	SOU odevné A.Hlinku 21 Bánovce n./Bebr.	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Kysucké Nove Mesto

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
57	KNM, Belanského	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Bytča

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
-----	-------------	-------	---------	-------------	---------

55	M.Rázusa 5, Bytča	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
----	----------------------	-----------	--------------------	--------------------------	-------

Čadca

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
58	F. Kráľa 1504, Čadca	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
56	Štúrova 2078, Čadca	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
1; 5	Čadca Posuvné dvere	RJ16 10.6.16.39; Čadca	RJ16Driver	RJ12 RFID5	Čadca

Dolný Kubín

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
5A	Aleja Slobody 1878, Dolný Kubín,02601	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
5C	Aleja Slobody 2203, Dolný Kubín,02601	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Námestovo

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
5E	Ubytovňa, Bernoláková 390/14,Námestovo,02901	SuperTrax	termSeverSuperTrax	EM 316	admin
5F	Územná poliklinika, ČK 62/30, Námestovo, 02901	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Tvrdošín

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
5H	Zdravotné stredisko, Medvedzie 132, Tvrdošín, 02744	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Liptovský Mikuláš

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
5J	Liptovský Mikuláš, Štúrova 34	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Ružomberok

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
5L	Ružomberok, Podhora 9	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Komárno

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
1; 12	KN - Serverovňa	RJ16 10.5.48.39; Komárno	RJ16Driver	RJ12 RFID5	Komárno
2; 12	KN - Prezentačná miestnosť	RJ16 10.5.48.39; Komárno	RJ16Driver	RJ12 RFID5	Komárno
4L	Petőfiho 7, 945 79 Komárno 5	SuperTrax	termSeverSuperTrax	EM 316	admin
4M	Petőfiho 7, 945 79 Komárno 5	SuperTrax	termSeverSuperTrax	EM 316	admin

Martin

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
5O	Námestie SNP č.4, Martin	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
5P	Námestie SNP č.4	SuperTrax	termSeverSuperTrax	EM 316	admin

Nové Zámky

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca	
6; 15	NZ - Zvláštne úlohy	RJ16; 10.5.56.39; Nové Zámky 10	RJ16Driver	RJ12 RFID5	Nové Zámky	
3; 15	NZ - prízemie vchod	RJ16; 10.5.56.39; Nové Zámky 10	RJ16Driver	RJ12 RFID5	Nové Zámky	
4; 15	NZ - Serverovňa	RJ16; 10.5.56.39; Nové Zámky 10	RJ16Driver	RJ12 RFID5	Nové Zámky	
1; 13	NZ - Vstup	RJ16; 10.5.57.39; Nové Zámky 11	RJ16Driver	RJ12 RFID5	Nové Zámky	1. 2. 2012
1; 15	NZ - Pivnica	RJ16; 10.5.56.39; Nové Zámky 10	RJ16Driver	RJ12 RFID5	Nové Zámky	
2; 15	NZ - vestibul - vchod na poschodie	RJ16; 10.5.56.39; Nové Zámky 10	RJ16Driver	RJ12 RFID5	Nové Zámky	
5; 15	NZ - VT	RJ16;	RJ16Driver	RJ12	Nové	

		10.5.56.39; Nové Zámky 10		RFID5	Zámky	
44	Nám. Gy. Széchényiho 10, Nové Zámky	SuperTrax	termSeverSuperTrax	EM 316	admin	
45	Nám. Gy. Széchényiho 10, Nové Zámky	SuperTrax	termSeverSuperTrax	EM 316	admin	
46	Nám. Gy. Széchényiho 10, Nové Zámky	SuperTrax	termSeverSuperTrax	EM 316	admin	

Brezno

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
68	Boženy Nemcovej 2, 977 01 Brezno	SuperTra x	termSeverSuperTra x	SuperTrax Doch+Strava	admin
69	Boženy Nemcovej 2, 977 01 Brezno	SuperTra x	termSeverSuperTra x	EM 316	admin

Zvolen

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
6A	Moyzesova 52, Zvolen	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
6C	SNP 35, Zvolen	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Detva

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
6E	Záhradná ul. č. 11/13, Detva	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Krupina

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
6F	ČSA 2190/3, Krupina	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Lučenec

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
6I	Ul. Dr. Vodu č. 6, 984 01 Lučenec	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Veľký Krtíš

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
6M	ul. SNP 28, 990 01 Veľký Krtíš	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
6N	ul. SNP 28, 990 01 Veľký Krtíš	SuperTrax	termSeverSuperTrax	EM 316	admin

Šahy

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
6O	Šahy, Hlavné námestie 1	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Bardejov

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
77	Bardejov, Hurbanova 6	SuperTrax	termSeverSuperTrax	EM 316	admin

Humenné

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7A	Námestie slobody 58, 066 57 Humenné	SuperTrax	termSeverSuperTrax	EM 316	admin
7B	Námestie slobody 58, 066 57 Humenné	SuperTrax	termSeverSuperTrax	EM 316	admin
6; 9	HE - Sekretariát riaditeľa 3. poschodie	RJ16 10.7.88.39; Humenné	RJ16Driver	RJ12 RFID5	Humenné
5; 9	HE - Ekonomika 3. poschodie	RJ16 10.7.88.39; Humenné	RJ16Driver	RJ12 RFID5	Humenné
4; 9	HE - Vstup z garáže	RJ16 10.7.88.39; Humenné	RJ16Driver	RJ12 RFID5	Humenné
3; 9	HE - Vstup pre externistov	RJ16 10.7.88.39; Humenné	RJ16Driver	RJ12 RFID5	Humenné
2; 9	HE - Bočná chodba prízemie	RJ16 10.7.88.39; Humenné	RJ16Driver	RJ12 RFID5	Humenné
1; 9	HE - Vestibul prízemie	RJ16 10.7.88.39; Humenné	RJ16Driver	RJ12 RFID5	Humenné

Snina

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7F	Partizánska 1057, 069 01	SuperTrax	termSeverSuperTrax	EM 316	admin

	Snina				
--	-------	--	--	--	--

Kežmarok

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7K	Kežmarok, Mučeníkov 4	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Kráľovský Chlmec

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7N	Hlavná 171, Kráľovský Chlmec	SuperTrax	termSeverSuperTrax	EM 316	admin

Poprad

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7I	Poprad, ul. 1. mája č. 4053/24	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
7J	Poprad, ul. 1. mája č. 4053/24	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Prešov

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
71	Masarykova 1, 08001 Prešov	SuperTrax	termSeverSuperTrax	EM 316	admin
72	Masarykova 1, 08001 Prešov	SuperTrax	termSeverSuperTrax	EM 316	admin
74	Masarykova 1, 08001 Prešov	SuperTrax	termSeverSuperTrax	EM 316	admin
76	Sabinov - detaš. pracovisko SP Prešov	SuperTrax	termSeverSuperTrax	EM 316	admin

Vranov n/T

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7O	Vranov n/T	SuperTrax	termSeverSuperTrax	EM 316	admin
7P	Vranov n/T	SuperTrax	termSeverSuperTrax	EM 316	admin

Stará Ľubovňa

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7Q	Budovateľská 42, 064 01 Stará Ľubovňa	SuperTrax	termSeverSuperTrax	EM 316	admin
7R	Budovateľská 42, 064 01 Stará Ľubovňa	SuperTrax	termSeverSuperTrax	EM 316	admin

7S	Budovateľská 42, 064 01 Stará Ľubovňa	SuperTrax	termSeverSuperTrax	EM 316	admin
----	---------------------------------------	-----------	--------------------	--------	-------

Giraltovce

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7V	Hviezdoslavova 3, Giraltovce	SuperTrax	termSeverSuperTrax	EM 316	admin

Stropkov

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
7W	Hlavná 26, Stropkov	SuperTrax	termSeverSuperTrax	EM 316	admin

Žilina

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
1; 11	ZA - 3. Poschodie vľavo	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
10; 11	ZA - Bočný vchod odchod	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
11; 11	ZA - Rampa príchod	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
12; 11	ZA - Rampa odchod	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
2; 11	ZA - 3. Poschodie vpravo	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
3; 11	ZA - 2. Poschodie vľavo	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
4; 11	ZA - 2. Poschodie vpravo	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
6; 11	ZA - 1. Poschodie vpravo	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
7; 11	ZA - Prízemie	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
8; 11	ZA - Vchod z parkoviska	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
9; 11	ZA - Bočný vchod príchod	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
5; 11	ZA - 1. Poschodie vľavo	RJ16; 10.6.8.39; Žilina	RJ16Driver	RJ12 RFID5	Žilina
51	A. Bernoláka 53, Žilina	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
52	A. Bernoláka 53, Žilina	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

53	A. Bernoláka 53, Žilina	SuperTrax	termSeverSuperTra x	SuperTrax Doch+Strava	admin
54	A. Bernoláka 53, Žilina	SuperTrax	termSeverSuperTra x	SuperTrax Doch+Strava	admin

Žiar nad Hronom

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
ZH 01	ZH Prechodové dvere	RJ16; 10.6.24.39; ZH	RJ16Driver	RJ12 RFID5	Admin
ZH 021	ZH Bočný vchod vstup	RJ16; 10.6.24.39; ZH	RJ16Driver	RJ12 RFID5	Admin
ZH 022	ZH Bočný vchod výstup	RJ16; 10.6.24.39; ZH	RJ16Driver	RJ12 RFID5	Admin
ZH 03	ZH Serverovňa + IT	RJ16; 10.6.24.38; ZH	RJ16Driver	RJ12 RFID5	Admin
6G	Sládkovičova 17	SuperTrax	termSeverSuperTra x	EM 316	admin
6H	Sládkovičova 17	SuperTrax	termSeverSuperTra x	EM 316	admin

Trnava

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
TT00	Trnava Rampa	RJ16 10.5.8.39; Trnava	RJ16Driver	RJ12 RFID5	Trnava
TT01	Trnava Dvere	RJ16; 10.5.9.28; Trnava	RJ16Driver	RJ12 RFID5	Trnava
21	V. Clementisa 24/A, Trnava	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin
22	V. Clementisa 24/A, Trnava	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Rožňava

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
RV 1	RV - 3. Mreža	RJ16 10.7.8.35; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 10	RV - Sut. - PR OLPČ	RJ16 10.7.8.33; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 11	RV - Sut. - Registratúrne stredisko	RJ16 10.7.8.33; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 2	RV - 3. Serverovňa	RJ16 10.7.8.35; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 3	RV - 3. Dvere pri	RJ16 10.7.8.34; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava

	riaditeľni				
RV 4	RV - 3. Dvere pri OVPO	RJ16 10.7.8.36; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 5	RV - 3. Dvere pri schodisku	RJ16 10.7.8.36; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 6	RV - Sut. - PR OP, OEaP	RJ16 10.7.8.33; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 7	RV - Sut. - Sklad VT, sklad 300	RJ16 10.7.8.33; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 8	RV - Sut. - Sklad 100, 200	RJ16 10.7.8.33; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
RV 9	RV - Sut. - PR ODP, ONP, OPvN	RJ16 10.7.8.33; Rožňava	RJ16Driver	RJ12 RFID5	Rožňava
8E	Štítnická 12, 048 13 Rožňava	SuperTrax	termSeverSuperTra x	EM 316	admin
8F	Štítnická 12, 048 13 Rožňava	SuperTrax	termSeverSuperTra x	EM 316	admin

Rimavská Sobota

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
RS01	Suterén	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS02	Prízemie - schodište	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS03	Zadný vchod	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS04	1. Poschodie	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS05	2. Poschodie	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS06	3. Poschodie	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS07	Serverovňa	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
RS08	4. Poschodie	RJ16 10.6.88.39; Rimavská Sobota	RJ16Driver	RJ12 RFID5	Rimavská Sobota
6K	Rimavská	SuperTrax	termSeverSuperTrax	SuperTrax	admin

	Sobota			Doch+Strava	
6L	Rimavská Sobota	SuperTrax	termSeverSuperTrax	SuperTrax Doch+Strava	admin

Levice

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
L01	Serverovňa - vstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L02	2. Poschodie - výstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L03	2. Poschodie - vstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L04	1. Poschodie - výstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L05	1. Poschodie - vstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L06	Prízemie výťah - výstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L07	Prízemie výťah - vstup	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L08	Klientske centrum - ľavý	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
L09	Klientske centrum - pravý	RJ16 10.5.81.41; Levice	RJ16Driver	RJ12 RFID5	Levice
4H	Sv. Michala 4, Levice	SuperTrax	termSeverSuperTrax	EM 316	admin
4I	Sv. Michala 4, Levice	SuperTrax	termSeverSuperTrax	EM 316	admin
4J	Sv. Michala 4, Levice	SuperTrax	termSeverSuperTrax	EM 316	admin

Sereď

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
90	Sereď	SuperTrax	termSeverSuperTra x	SuperTrax Doch+Strava	admin

Senec

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
2M	Senec, Brezova	SuperTrax	termSeverSuperTra x	EM 316 dochádzka	admin

Banská Bystrica

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
9; 16	BB - Tretie poschodie zo schodišťa	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
7; 16	BB - Druhé poschodie zo schodišťa	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
6; 16	BB - Prvé poschodie zo schodišťa	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
5; 16	BB - Prízemie zadný vchod	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
3; 16	BB - Suterén chodba vľavo	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
2; 16	BB - Suterén archív	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
10; 16	BB - Serverovňa	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
1; 16	BB - Suterén chodba vpravo	RJ16 10.6.40.39; Banská Bystrica	RJ16Driver	RJ12 RFID5	Banská Bystrica
61	Kapitulská 27, 97426 Banská Bystrica	SuperTrax	termSeverSuperTra x	SuperTrax Doch+Strava	admin
62	Kapitulská 27, 97426 Banská Bystrica	SuperTrax	termSeverSuperTra x	SuperTrax Doch+Strava	admin
67	Trieda SNP 75, 5p. Banská Bystrica	SuperTrax	termSeverSuperTra x	SuperTrax Doch+Strava	admin

Gelnica

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
8M	Banické nám. 99, Gelnica	SuperTrax	termSeverSuperTrax	EM 316	admin

Levoča

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
8L	Levoča	SuperTrax	termSeverSuperTrax	EM 316	admin

Krompachy

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
8K	Krompachy - novo pridaná pobočka	SuperTrax	termSeverSuperTrax	EM 316	admin

Spišská Nová Ves

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
8J	SN, Elektrárenská 10	SuperTrax	termSeverSuperTrax	EM 316	admin
1; 20	SN - Park. rampa - vstup	RJ16 10.7.16.39; Spišská Nová Ves	RJ16Driver	RJ12 RFID5	Spišská Nová Ves
2; 20	SN - Park. rampa - výstup	RJ16 10.7.16.39; Spišská Nová Ves	RJ16Driver	RJ12 RFID5	Spišská Nová Ves

Revúca

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
8I	Komenského 40, 050 01 Revúca	SuperTrax	termSeverSuperTrax	EM 316	admin

Moldava nad Bodvou

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
89	Hviezdoslavova 32, Moldava nad Bodvou	SuperTrax	termSeverSuperTrax	EM 316	admin

Košice

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
81	Festivalové námestie 1, 041 84 Košice	SuperTrax	termSeverSuperTrax	EM 316	admin
82	Festivalové námestie 1, 041 84 Košice	SuperTrax	termSeverSuperTrax	EM 316	admin
6; 14	KE - Prízemie - vstup k výťahom	RJ16 10.7.48.39; Košice	RJ16Driver	RJ12 RFID5	Košice
5; 14	KE - Prízemie - vstup na poschodie	RJ16 10.7.48.39; Košice	RJ16Driver	RJ12 RFID5	Košice
2; 14	KE - Telef. ústredňa - prízemie	RJ16 10.7.48.39; Košice	RJ16Driver	RJ12 RFID5	Košice

Trebišov

Kód	Umiestnenie	Názov	Ovládač	Typ snímača	Správca
4; 17	TV - 4. Poschodie	RJ16 10.7.80.39; Trebišov	RJ16Driver	RJ12 RFID5	Trebišov
3; 17	TV - 3. Poschodie	RJ16 10.7.80.39; Trebišov	RJ16Driver	RJ12 RFID5	Trebišov

1; 17	TV - 1. Poschodie	RJ16 10.7.80.39; Trebišov	RJ16Driver	RJ12 RFID5	Trebišov
2; 17	TV - 2. Poschodie	RJ16 10.7.80.39; Trebišov	RJ16Driver	RJ12 RFID5	Trebišov
7L	Trebišov - M.R.Štefánika 178	SuperTrax	termSeverSuperTrax	EM 316	admin

PODROBNÁ CENOVÁ KALKULÁCIA PREDMETU ZMLUVY

P.č.	Názov	Merná jednotka	Počet	Jednotková cena v EUR bez DPH	Jednotková cena v EUR s DPH	Cena spolu v EUR bez DPH	Cena spolu v EUR s DPH
1	Podpora SW: vrátane implementácia legislatívnych zmien, ktoré súvisia s HR politikou ako aj zabezpečenie bezporuchovej prevádzky APV, vrátane podpory pri prevádzke žiadanej cez Service desk, vrátane riešenia denných hlásení, poskytovania konzultácií, opravy chýb, drobných úprav a nasadenia zmien funkcionalít APV do testovania a prevádzky, kontrola/zmeny parametrických nastavení systému, obnovenie prevádzky po vyriešení havarijnej situácie), poskytované podľa potreby aj formou prítomnosti zamestnanca/zamestnancov poskytovateľa na pracovisku objednávateľa (v rozsahu max. 6 ČD ročne), za stanovenú paušálnu sumu. Poskytovateľ bude túto položku fakturovať mesačne najneskôr do 5 pracovných dní od začiatku nasledujúceho mesiaca poskytovania služby.	mesiac	36	8600	10320	309600	371520
2	Technická podpora komponentov pre dochádzkový a prístupový systém v režime on-site, t. j. odstránenie výpadku do 48 hodín pre vstup osôb do chránených priestorov. Poskytovateľ bude túto položku fakturovať mesačne najneskôr do 5 pracovných dní od začiatku nasledujúceho mesiaca poskytovania služby.	mesiac	36	1000	1200	36000	43200
3	HW rozšírenie prístupového systému, prípadne výmena za nové, výrobcom podporované terminály, ktoré budú kompatibilné so systémom iCard. Zariadenia musia komunikovať v on-line režime, s okamžitým obojsmerným prenosom dát do riadiacich jednotiek aj do databázy. V prípade ponuky iných ako iCard podporovaných zariadení je nevyhnutá náhrada všetkých zariadení, ktoré sú nekompatibilné s existujúcim systémom iCard, tak aby neobmedzil každodennú prevádzku na pobočkách SP (zoznam komponentov).						
3a	Prístupový snímač Mifare kariet (Multi RFID/5) Výrobca: Axess TMC; Označenie výroku: RFID/5	ks	50	276.00	331.2	13800	16560
3b	Riadiaca jednotka RJPS2-LAN, s pamäťou na 10 000 kariet a 30 000 udalostí Výrobca: Eltis, Označenie výrobku: RJPS2L	ks	28	372.00	446.4	10416	12499.2
	Riadiaca jednotka RJPS2 bez LAN, s pamäťou na 10 000 kariet a 30 000 udalostí Výrobca: Eltis, Označenie výrobku: RJPS2L	ks	7	282.00	338.4	1974	2368.8

	Prevodníková riadiaca jednotka RJPS2-PREV Výrobca: Eltis, Označenie výrobku: RJPS2P	ks	2	330.00	396	660	792
3c	Zámok elektromagnetický štandardný, nízkoodberový 12V 150 mA, bez signalizácie otvorenia dverí	ks	2	58.00	69.6	116	139.2
	Zámok elektromagnetický reverzný protipožiarny zámok 12V, bez certifikácie, bez signalizácie otvorenia dverí	ks	8	66.00	79.2	528	633.6
	Zámok elektromagnetický štandardný, nízkoodberový 12V 150 mA, so signalizáciou otvorenia dverí	ks	5	82.00	98.4	410	492
	Zámok elektromagnetický reverzný protipožiarny zámok 12V, bez certifikácie, so signalizáciou otvorenia dverí	ks	10	91.00	109.2	910	1092
	Zámok elektromagnetický štandardný ÚZKY 66 x 16 x 28 mm, 12V/200mA, Použitie pre tenké zárubne a skryté montáže. Bez lišty.	ks	5	94.00	112.8	470	564
	Zámok elektromagnetický reverzný ÚZKY 66 x 16 x 28 mm, 12V / 200 mA. Použitie pre tenké zárubne a skryté montáže. Bez lišty.	ks	5	102.00	122.4	510	612
	Lišta 250 x 25 x 3 mm, obojstranná	ks	1	8.00	9.6	8	9.6
	Lišta uhlová, L, Zn pre úzke zámky	ks	1	10.00	12	10	12
	Chránička na kabeláž zámku - dvojkrídlové dvere resp.	ks	1	12.00	14.4	12	14.4
	Elektromagnetický zámok so signalizáciou, LED, zabezpeč. sila 280 kg, povrchová montáž	ks	1	215.00	258	215	258
	Elektromagnetický zámok so signalizáciou, LED, zabezpeč. sila 2x280 kg, povrchová montáž	ks	1	421.00	505.2	421	505.2
	Elektromagnetický zámok so signalizáciou, LED, zabezpeč. sila 500 kg, povrchová montáž	ks	1	294.00	352.8	294	352.8
	Dverová lišta EMZ krátka so signalizáciou - dverová lišta 40 cm s madlom s plastovým úchytom a elektromagnetom so signalizáciou stavu dverí, povrchová montáž na existujúce dvere, zabezpečovacia sila 300 kg, rozmery (d x š x h) 400 x 105 x 63 mm, teplotný rozsah: -20°C do +70°C, saténový anodizovaný hliník, spotreba 550 mA na 12 VDC	ks	3	211.00	253.2	633	759.6
	Sada troch konzol pre povrchové elektromagnetické zámky 300 kg	ks	2	62.00	74.4	124	148.8
	Sada troch konzol pre povrchové elektromagnetické zámky 600 kg	ks	1	75.00	90	75	90

3d	Záložný zdroj pre prístupové snímače 12V/1A 1,3Ah	ks	1	59.00	70.8	59	70.8
	Záložný zdroj pre prístupové snímače 13,8V/4A + akumulátor 7Ah, UPS režim 3,3A, 55W, IP20, plechová skrinka 260x210x75 mm, biela	ks	20	122.00	146.4	2440	2928
	Záložný zdroj pre prístupové snímače 13,8V/10A + akumulátor 18Ah, UPS režim 8A, 140W, IP20, plechová skrinka 300x285x80 mm, biela	ks	13	162.00	194.4	2106	2527.2
	AC/DC napájací zdroj 12V/4,5A pre montáž na DIN lištu, pre prístupový systém bez zálohovania prevádzky akumulátorom	ks	1	30.00	36	30	36
	Náhradný akumulátor 12V/7Ah	ks	5	32.00	38.4	160	192
	Náhradný akumulátor 12V/18Ah	ks	3	61.00	73.2	183	219.6
3e	Skrinka 400x300x200 (VxŠxH) mm pre uloženie komponentov PS, uzamykateľná kľúčom	ks	17	140.00	168	2380	2856
	Skrinka 500x400x200 (VxŠxH) mm pre uloženie komponentov PS, uzamykateľná kľúčom	ks	10	168.00	201.6	1680	2016
	Inštalačná krabica na stenu, 150x110x70, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1	18.00	21.6	18	21.6
	Inštalačná krabica na stenu, 190x140x70, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1	24.00	28.8	24	28.8
	Inštalačná krabica na stenu, 240x190x90, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1	32.00	38.4	32	38.4
	Inštalačná krabica na stenu, 300x220x120, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	2	41.00	49.2	82	98.4
	Inštalačná krabica na stenu, 380x300x120, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	2	50.00	60	100	120
	Inštalačná krabica na stenu, 452x380x130, stupeň krytia IP56, trieda ochrany II (s izoláciou), prevádzková teplota -20°C ~ +60°C Mechanická odolnosť IK04/IK08	ks	1	64.00	76.8	64	76.8
3f	Zelené (panic) núdzové výstupné tlačidlo resetovateľné, priehľadný plastový kryt pre núdzové	ks	10	85.00	102	850	1020

	tlačidlo						
3g	Diaľkové ovládanie pre otváranie elektromagnetického zámku z recepcie (prijímač 2 kanály, 433MHz + diaľkový ovládač 4 kanálový (umožňuje ovládať 2 prijímače))	ks	3	42.00	50.4	126	151.2
3h	Síreňa audiovizuálna 6-14VDC; rozmery D=110mm, H=47mm; 122dB; IP65; kábel	ks	2	42.00	50.4	84	100.8
3i	Elektroinštalačný a montážny materiál (kabeláž + lišty + spojovací materiál)						
	Lišta káblová biela 15x10x2000mm	ks	10	1.25	1.5	12.5	15
	Lišta káblová biela 25x25x2000mm	ks	10	2.20	2.64	22	26.4
	Štruktúrovaná kabeláž FTP Cat 5E krabica 305m	ks	10	92.00	110.4	920	1104
3j	Karty - bezkontaktná čipová karta, pracovná frekvencia 13,56 MHz, biela s možnosťou farebnej obojstrannej potlače karty – retransferová metóda tlače, rozmery 85,6mm x 53,98mm x 0,76mm.Obal na kartu z priehľadného pružného plastu, s klipom štipca.	ks	5000	2.60	3.12	13000	15600
3k	Inštalačné, konfiguračné a ostatné práce súvisiace s implementáciou HW	ČD	100	500	600	50000	60000
4	Implementácia spracovania cestovných príkazov ako integrálnej súčasti systému DS						
4a	Implementácia modulu spracovania CP a zaškolenie kľúčových používateľov	ČD	50	500.00	600	25000	30000
5	Úpravy aplikácie iCard na základe požiadavky objednávateľa	ČD	400	500.00	600	200000	240000
	Celková cena za predmet zákazky					676558.5	811870.2

V Bratislave dňa

V Bratislave dňa

.....
Ing. Pavel Struhárik, konateľ
Eviden Slovakia s.r.o.

ZOZNAM SUBDODÁVATEĽOV

Eviden Slovakia s.r.o.

Pribinova 19/7828

811 09 Bratislava

IČO: 45 650 276

Na poskytovanie plnenia Zmluvy o poskytovaní technickej podpory pre Centrálny dochádzkový systém č.-/2023-BA

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

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 Bratislave dňa

.....
Ing. Pavel Struhárik, konateľ
Eviden Slovakia s.r.o.

ZÁPIS

O ZMENE PRÍLOHY

k Zmluve o poskytovaní technickej podpory pre Centrálny dochádzkový systém č.-/2023-BA uzavretej podľa § 269 ods. 2 Obchodného zákonníka (ďalej len „zmluva“) medzi:

poskytovateľom,
IČO: (ďalej len „poskytovateľ“)

a

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

V súlade s článkom XI bodom 11.5 zmluvy, v ktorom sa zmluvné strany dohodli o spôsobe zmeny prílohy č. 3 k zmluve „ZOZNAM SUBDODÁVATEĽOV“, zmluvné strany v zastúpení ich oprávnenými zástupcami podpisujú tento zápis, ktorým sa mení príloha č. 3 k zmluve „ZOZNAM SUBDODÁVATEĽOV“, ktorá tvorí prílohu k tomuto zápisu.

Dôvod potreby uskutočnenia zmeny prílohy č. 3 k zmluve „ZOZNAM SUBDODÁVATEĽOV“:

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

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. 3 k zmluve „ZOZNAM SUBDODÁVATEĽOV“.

Za poskytovateľa:

..... dňa

.....

oprávnená osoba

Príloha:

Príloha č. 3 k zmluve „ZOZNAM SUBDODÁVATEĽOV“

Za objednávateľa:

Bratislava, dňa

.....

riaditeľ sekcie informatiky

EVIDENCIA SERVISNÝCH ZÁSAHOV

Evidencia servisných zásahov							
Dátum	Čas od	Čas do	Titul	Meno	Priezvisko	Príslušnosť k spoločnosti	Stručný popis zásahu

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 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Tariška generálny riaditeľ Sociálnej poisťovne
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA
IČO:	308 07 484
DIČ:	2020592332

(ďalej len „prevádzkovateľ“)

a

Sprostredkovateľ

Obchodné meno:	Eviden Slovakia s.r.o.
Sídlo:	Pribinova 19/7828, 811 09 Bratislava
Štatutárny orgán:	Ing. Pavel Struhárik, konateľ
Bankové spojenie:	XXXXXX
IBAN:	XXXXXX
IČO:	45 650 276
DIČ:	2023110661
IČ DPH:	SK2023110661

Zapísaný v Obchodnom registri Mestského súdu Bratislava III., oddiel Sro, vložka č. 66638/B.

(ďalej len „sprostredkovateľ“)

(spolu ďalej ako „zmluvné strany“)

Preambula

Zmluvné strany spolu uzatvárajú „Zmluvu č.“ o poskytovaní technickej podpory pre Centrálny dochádzkový systém, podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, predmetom ktorej je predovšetkým poskytovať služby technickej podpory pre Centrálny dochádzkový systém (ďalej len „zmluva o poskytovaní služieb“).

Sprostredkovateľ vystupuje v tejto zmluve ako poskytovateľ týchto služieb, pričom nie je vylúčené, že v rámci plnenia predmetu zmluvy sa dostane priamo k spracovaniu osobných údajov zamestnancov prevádzkovateľa, aj keď takéto spracovanie nie je predmetom zmluvy. Vzhľadom na vyššie uvedenú možnosť spracovania osobných údajov prevádzkovateľa sprostredkovateľom, zmluvné strany uzatvárajú podľa čl. 28 ods. 3 nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane osobných údajov) (ďalej len „GDPR“) a podľa § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „ZOOU“) túto sprostredkovateľskú zmluvu (ďalej len „zmluva“).

Článok I.

Vymedzenie pojmov

Dotknutá osoba je identifikovaná, alebo identifikovateľná fyzická osoba, ktorej sa spracúvané osobné údaje týkajú:

- a) osoby, ktorých údaje sa spracúvajú na základe zákona č. 461/2003 Z. z. o sociálnom poistení a 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.

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 poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Čl. II

Predmet zmluvy

1. Predmetom tejto zmluvy je poverenie sprostredkovateľa na spracovanie osobných údajov dotknutých osôb v mene prevádzkovateľa a podľa pokynov prevádzkovateľa v rozsahu osobných údajov, spracúvanie ktorých je potrebné pre plnenie účelu zmluvy o poskytovaní služieb.
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje po splnení povinností uvedených v tejto zmluve.
3. Účel spracúvania osobných údajov je vymedzený v zákone č. 461/2003 Z. z. o sociálnom poistení, v Nariadení (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, v Nariadení (ES) Európskeho parlamentu a Rady č. 987/2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, podľa ktorých je prevádzkovateľ oprávnený spracúvať osobné údaje dotknutých osôb za účelom výkonu sociálneho poistenia.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje výhradne pre poskytovanie služieb prevádzkovateľovi, a to na základe pokynov prevádzkovateľa podľa podmienok stanovených v tejto zmluve v súlade so všeobecne záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov. Za pokyny prevádzkovateľa sa považujú pokyny uvedené v tejto zmluve, v servisnej zmluve, prípadne iné písomne zdokumentované pokyny alebo požiadavky prevádzkovateľa na poskytnutie služby v zmysle servisnej zmluvy.
5. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou zmluvy o poskytovaní služieb a to na účel:
 - Účelom spracúvania osobných údajov poskytovateľom je poskytovanie služieb technickej podpory pre Centrálny dochádzkový systém.
6. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu zmluvy o poskytovaní služieb je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom 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 predmetu ktorej je sprostredkovateľ poverený spracúvať osobné údaje klientov prevádzkovateľa:
Zmluva o poskytovaní technickej podpory pre Centrálny dochádzkový systém uzatvorená podľa § 269 ods. 2 Obchodného zákonníka (ev. č. zmluvy-/2023-BA).
2. Zoznam osobných údajov, ktoré môžu byť realizácii predmetu zmluvy o poskytovaní služieb predmetom spracúvania:

Sprostredkovateľ je oprávnený spracúvať osobné údaje v rozsahu najmä meno, priezvisko, titul, telefón a emailová adresa dotknutých osôb a iné údaje spracované v informačných systémoch prevádzkovateľa v rozsahu, aký je nevyhnutný na plnenie predmetu zmluvy č. ...-.../2023-BA o poskytovaní služieb,

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

Čl. IV

Spôsob výkonu a oprávnenia sprostredkovateľa

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

Čl. V

Vyhlásenie prevádzkovateľa

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

- c) osobné údaje, ktoré sprostredkovateľ spracúva na základe tejto zmluvy sú aktuálne, úplné a primerané vzhľadom na účel spracúvania.

Čl. VI

Vyhlasenie sprostredkovateľa

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

Čl. VII

Povinnosti sprostredkovateľa

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

- h) ak všeobecne záväzné právne predpisy upravujúce problematiku archívov a registratúr neustanovujú inak, bezodkladne odovzdávať prevádzkovateľovi všetky získané materiály obsahujúce osobné údaje, ktoré už pre realizáciu zmluvy nepotrebuje, resp. všetky osobné údaje, ktoré bude spracúvať v súvislosti s plnením zmluvy o poskytovaní služieb, bezodkladne po tom, čo pominie dôvod na ich spracúvanie podľa zmluvy, zmazať zo všetkých elektronických, hmotných alebo iných nosičov informácií (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 zaviazat' týmito povinnosťami aj osoby, ktoré by dojednal na činnosti na plnenie podľa tejto zmluvy (zamestnancov či iných pracovníkov),
 - l) plniť predmet zmluvy len prostredníctvom riadne a preukázateľne poučených alebo vyškolených oprávnených osôb pre účel plnenia predmetu zmluvy a z nej vyplývajúceho rozsahu a podmienok spracúvania osobných údajov,
 - m) spracúvať osobné údaje oprávnenými osobami konajúcimi za sprostredkovateľa len v rozsahu pokynov prevádzkovateľa v zmysle čl. 32 GDPR vrátane prípadnej pseudonymizácie a šifrovania s ohľadom na okolnosti konkrétneho prípadu a v rozsahu nevyhnutnom na dosiahnutie účelu spracúvania osobných údajov, ako je uvedené v čl. II tejto zmluvy a pokynu prevádzkovateľa udeleného osobou oprávnenou konať v danom rozsahu za prevádzkovateľa, alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
 - n) v prípade sťažností alebo sporu týkajúceho sa spracúvania osobných údajov pri plnení predmetu zmluvy, bezodkladne informovať prevádzkovateľa o tejto skutočnosti a spolupracovať pri riešení sťažnosti alebo sporu s prevádzkovateľom,
 - o) nepoužiť spracúvané osobné údaje v mene prevádzkovateľa pre vlastnú potrebu, pokiaľ všeobecne záväzné platné právne predpisy neustanovujú inak,
 - p) zabrániť neoprávneným osobám v prístupe k osobným údajom a k prostriedkom na ich spracovanie, zabrániť neoprávnenému čítaniu, vytváraniu, kopírovaniu, prenosu, úprave či vymazaniu záznamov obsahujúcich osobné údaje a zabezpečiť opatrenia, ktoré umožnia určiť a overiť, komu/kým a akým spôsobom boli osobné údaje odovzdané, resp. kým boli prevzaté a spracúvané.
2. Sprostredkovateľ je pri spracúvaní osobných údajov podľa tejto zmluvy ďalej povinný bezodkladne informovať prevádzkovateľa o
- a) poskytnutí a sprístupnení osobných údajov tretej strane spolu s odôvodnením a určením všeobecne záväzného právneho predpisu, ktorý sprostredkovateľovi ukladá povinnosť

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

- b) skutočnostiach zabráňujúcich 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 zaistovaní plnenia jeho povinností pri prevencii rizík a ďalších povinností Prevádzkovateľa podľa ustanovení čl. 32 – 36 GDPR. K vyžiadaniu Prevádzkovateľa je mu nápomocný technickými a organizačnými prostriedkami pri plnení povinností Prevádzkovateľa reagovať na žiadosti o výkon práv

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

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

Čl. VIII

Podmienky spracúvania osobných údajov

1. Sprostredkovateľ vyhlasuje, že spracúvanie osobných údajov bude vykonávať sám, a zároveň prostredníctvom iných osôb (ďalej len „subdodávateľ“), ktorými sú spoločnosti Prevádzkovateľ so spracúvaním osobných údajov uvedenými subdodávateľmi súhlasí. Subdodávatelia budú spracúvať osobné údaje na zodpovednosť sprostredkovateľa v rozsahu a za podmienok stanovených v tejto zmluve. Sprostredkovateľ nezapojí do spracovania žiadneho ďalšieho sprostredkovateľa bez predchádzajúceho konkrétneho písomného súhlasu prevádzkovateľa. Náležitosti žiadosti o poskytnutie súhlasu sú uvedené v bode 3 tohto článku zmluvy.
2. 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.
3. 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.
4. 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 dní od jej vyžiadania prevádzkovateľovi.
 5. 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 povinností subdodávateľom. Sprostredkovateľ sa nemôže zbaviť zodpovednosti za porušenie povinností 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.
 6. 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 povinností sprostredkovateľa vo vzťahu k tomuto subdodávateľovi.

Čl. IX

Ostatné dohodnuté podmienky

1. Sprostredkovateľ postupuje pri spracúvaní osobných údajov podľa GDPR a podľa ZOOU.
2. Sprostredkovateľ sa zaväzuje nahradiť prevádzkovateľovi v plnom rozsahu všetky škody, ktoré mu vzniknú v súvislosti s nedodržaním tejto zmluvy zo strany sprostredkovateľa a ktorá prevádzkovateľovi vznikne porušením alebo nesplnením povinností subdodávateľa sprostredkovateľa pri spracúvaní a ochrane osobných údajov vyplývajúcich z ustanovení zmluvy a všeobecne záväzných právnych predpisov.
3. Ochrana osobných údajov podľa zmluvy trvá aj po ukončení zmluvného vzťahu založeného touto zmluvou a zaväzuje aj právnych nástupcov zmluvných strán. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá prevádzkovateľovi vznikla porušením povinností sprostredkovateľa.
4. Sprostredkovateľ je poverený spracúvať osobné údaje po dobu platnosti tejto zmluvy. Okamihom skončenia jej platnosti už sprostredkovateľ nesmie disponovať žiadnymi

osobnými údajmi. Sprostredkovateľ je povinný vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje, v prípade že ich spracovával, po ukončení poskytovania služieb týkajúcich sa plnenia zmluvy o poskytovaní služieb a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov, o čom vyhotoví písomné vyhlásenie, ktoré je povinný doručiť prevádzkovateľovi najneskôr do dvoch pracovných dní od skončenia platnosti zmluvy.

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

Čl. X

Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Sprostredkovateľ berie na vedomie povinnosť prevádzkovateľa zverejniť túto zmluvu a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy v plnom rozsahu.
2. Táto zmluva nadobúda platnosť podpisom oprávnených zástupcov zmluvných strán a účinnosť dňom nasledujúcim deň po dni zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Táto zmluva sa uzatvára na dobu určitú, po dobu platnosti a účinnosti zmluvy o poskytovaní služieb.
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 uzatvorená po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave, dňa

V Bratislave dňa

Za prevádzkovateľa:

Za sprostredkovateľa:

Ing. Michal Tariška
generálny riaditeľ Sociálnej poisťovne

Ing. Pavel Struhárik
konateľ
Eviden Slovakia s.r.o.

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 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Tariška, generálny riaditeľ Sociálnej poisťovne
IČO:	308 07 484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA

(ďalej len „prevádzkovateľ“)

a

Obchodné meno:

Sídlo:	Eviden Slovakia s.r.o. Pribinova 19/7828, 811 09 Bratislava
Štatutárny orgán:	Ing. Pavel Struhárik, konateľ
Zápis v registri:	Obchodný register Mestského súdu Bratislava III., oddiel Sro, vložka č. 66638/B.
IČO:	45 650 276
DIČ:	2023110661
IČ DPH:	SK2023110661
Bankové spojenie:	XXXXXX
IBAN:	XXXXXX

(ďalej len „dodávateľ“)

(spolu ďalej ako „zmluvné strany“)

Čl. II

Preambula

1. Prevádzkovateľ je podľa § 3 písm. l) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“) prevádzkovateľom základnej služby podľa § 3 písm. k) body 2 a 3 zákona o kybernetickej bezpečnosti. Dodávateľ je podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom, ktorý na základe zmluvy na výkon činností poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa, ako prevádzkovateľa základnej služby.
2. Zmluvné strany spolu uzatvárajú Zmluvu č. o poskytovaní technickej podpory pre Centrálny dochádzkový systém, podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, predmetom ktorej je predovšetkým poskytovať služby technickej podpory pre Centrálny dochádzkový systém (ďalej len „zmluva na výkon činností“).
3. Zmluvné strany uzatvárajú za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a podľa § 8 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška“) túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „zmluva“).

Čl. III Predmet zmluvy

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

Čl. IV Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné politiky prevádzkovateľa, ktoré tvoria prílohu č. 1 k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami prevádzkovateľa.
2. Dodávateľ súhlasí s tým, že bezpečnostné politiky prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov prevádzkovateľa.
3. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú súčasťou bezpečnostnej politiky prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu

uvedenom v tejto zmluve a bezpečnostných politikách prevádzkovateľa. Dodávateľ vyhlasuje, že s bezpečnostnými opatreniami súhlasí.

4. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti.
5. Dodávateľ je povinný chrániť všetky informácie ku ktorým má prístup na základe zmluvy na výkon činností alebo tejto zmluvy, alebo ktoré mu boli poskytnuté zo strany prevádzkovateľa s tým, že všetci dotknutí zamestnanci dodávateľa jeho subdodávateľa a/alebo iné tretie osoby, prostredníctvom ktorých dodávateľ poskytuje služby podľa zmluvy na výkon činností (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 odborom bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa podpísala vyhlásenie o mlčanlivosti a zúčastnila sa na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností. Po podpísaní vyhlásenia o mlčanlivosti budú týmto osobám sprístupnené bezpečnostné politiky prevádzkovateľa.
9. Dodávateľ je povinný písomne informovať prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom na účely plnenia tejto zmluvy.
10. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Čl. V

Okolnosti plnenia zmluvy

1. Pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.
2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie

v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.

3. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa podľa zmluvy na výkon činností. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania zmluvy na výkon činností.
4. Odplata za plnenie povinností dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom dodávateľovi podľa zmluvy na výkon činností a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Čl. VI

Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

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

- a. zabezpečiť vlastnú kybernetickú bezpečnosť, aby pri poskytovaní elektronických komunikačných služieb a sietí cez siete a informačné systémy dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa,
- b. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy na výkon činností a tejto zmluvy alebo budú mať prístup k informáciám prevádzkovateľa,
- c. sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
- d. sledovať hrozby týkajúce sa dodávateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
- e. predchádzať hrozbe vzniku kybernetických incidentov,
- f. v prípade vzniku kybernetických incidentov, systematicky získavať (monitorovať a detegovať), sústredovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
- g. prijímať od prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
- h. zasielať prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a
- i. spolupracovať s prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa.

Čl. VII

Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident prevádzkovateľovi, ktorý by mohol mať vplyv na bezpečnosť dát prevádzkovateľa spôsobom určeným prevádzkovateľom, ktorý je uvedený v bode 3.1.5 bezpečnostnej politiky prevádzkovateľa, ktorá tvorí prílohu č. 1 k tejto zmluve, 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, ohraňovaním 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 Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“), 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, záväzkov 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 nezavahuje 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 MIRRI, 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, dôverynosť, 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 povinností podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu, v celom rozsahu. Prevádzkovateľ má nárok na preukázanie náhradu škody, pokuty alebo iné náklady, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov dodávateľa.
8. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.
9. Po ukončení tejto zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

Čl. XI

Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom UPVS, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti je: riaditeľ odboru bezpečnosti informačných systémov.
3. Kontaktná osoba dodávateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je:
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: bis@socpoist.sk
5. Kontakt na zástupcu dodávateľa na úseku kybernetickej bezpečnosti je:@.....
6. Kontaktné osoby podľa bodov 2. a 3. tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme na adresu zmluvnej strany uvedenú v záhlaví tejto zmluvy alebo elektronicky prostredníctvom UPVS.

Čl. XII

Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií) a v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
2. Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády SR.
3. Táto zmluva sa uzatvára na dobu určitú po dobu platnosti a účinnosti zmluvy na výkon činnosti definovanej v článku II - Zmluva č. o poskytovaní technickej podpory pre Centrálny dochádzkový systém, podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, predmetom ktorej je predovšetkým poskytovať služby technickej podpory pre zálohovanie prevádzkovaných systémov.
4. Počas platnosti a účinnosti zmluvy na výkon činností je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane. Skončenie tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do skončenia tejto zmluvy.
5. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

6. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.
7. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve.
8. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akejkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek nezákonného, neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.
9. Neoddeliteľnou súčasťou tejto zmluvy je:
Príloha č. 1 – Bezpečnostné politiky,
Príloha č. 2 – Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni.
10. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.
11. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorená po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave, dňa

V Bratislave dňa

Za prevádzkovateľa:

Za dodávateľa:

.....
Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

.....
Ing. Pavel Struhárik
konateľ
Eviden Slovakia s.r.o.

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 riaditeľom sekcie informatiky prevádzkovateľa a po doručení záznamu o vykonaní kontroly fyzickej bezpečnosti na mieste výkonu práce, zrealizuje požiadavku príslušný administrátor.

2.3 Klasifikácia informácií

- (1) Pre potrebu ochrany informácií platí ich nasledovná klasifikačná schéma
 - a) citlivé,
 - b) interné,
 - c) verejné.
- (2) Citlivé - sú chránené informácie, a to
 - a) osobné údaje poistencov,
 - b) osobné údaje zamestnancov,
 - c) osobné údaje tretích strán,
 - d) mzdové náležitosti zamestnancov,
 - e) vymeriavacie základy poistencov,
 - f) informácie dôležité pre ochranu osobných údajov v rozsahu: analýza rizík, posúdenie vplyvu na ochranu údajov, bezpečnostný incident, bezpečnostný monitoring, bezpečnostný audit,
 - g) údaje zhromaždené v IS prevádzkovateľa (ďalej len „IS SP“).
- (3) Interné - sú chránené informácie, kam patria všetky informácie, ktoré nie sú klasifikované ako citlivé alebo verejné, a ktoré
 - a) vznikajú v súvislosti s plnením pracovných činností zamestnancov a nie sú určené pre zverejnenie,
 - b) boli poskytnuté externým subjektom a nie sú určené pre zverejnenie.
- (4) Verejné - nie sú chránené informácie. Patria sem informácie už zverejnené alebo určené na zverejnenie v zmysle platných právnych predpisov a vnútorných predpisov.

2.4 Zaobchádzanie s aktívami

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

2.5 Zmluvy o dôvernosti alebo utajení

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

2.6 Ochrana testovacích údajov

Ak je na účely testovania dodávateľom nevyhnutné použiť prevádzkové údaje, môže byť použitá iba ich pseudonymizovaná kópia na základe súhlasu riaditeľa odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa. Kópia prevádzkových údajov musí byť bezpečne vymazaná ihneď po skončení testovania. Dozor vykonáva zodpovedná osoba prevádzkovateľa.

3. Riadenie vzťahov s dodávateľom

3.1 Informačná bezpečnosť vo vzťahoch s dodávateľom

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

3.1.1 Politika informačnej bezpečnosti na vzťahy s dodávateľom

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

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

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

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

3.1.2 Ošetrenie bezpečnosti v zmluvách s dodávateľom

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

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

(3) K bezpečnostným formuláciám v návrhu zmluvy na výkon činností s dodávateľom

zaujme stanovisko riaditeľ odboru bezpečnosti informačných systémov, ktorý posúdi dostatočnosť bezpečnostných opatrení a notifikačných povinností, ktoré musia platiť počas celej doby platnosti zmluvy na výkon činností pre zaistenie kybernetickej bezpečnosti.

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

3.1.3 Monitorovanie a preskúvanie 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 centrálnemu 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 slabínach 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 centrálnemu 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 poisťovňami, 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 poisťovní 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, tokeny, prvkov PKI),
- d) prístup neoprávnenej (cudzí osoba, nevyškolená obsluha a pod.) osoby do IS SP,
- e) vírusová infiltrácia do IS SP, zasielanie nežiadúceho obsahu, škodlivý kód,
- f) prienik do IS alebo pokus o prienik,
- g) kybernetický bezpečnostný incident,
- h) inštalácie neschváleného hardvéru a softvéru na komponentoch IS SP,
- i) neoprávnené premiestnenie technických komponentov IS SP,
- j) používateľom vykonané zmeny hardvérovej konfigurácie počítača, servera, siete, komunikačných prvkov a pod.,
- k) nevykonávanie záloh na serveroch zaradených do systému centralizovaných záloh alebo serverov s inak definovanou zálohovacou stratégiou,
- l) zničenie alebo odcudzenie médií, na ktorých sú bezpečnostné zálohy serverov,

- m) prepisovanie auditných záznamov,
- n) krádež hardvéru alebo softwaru, ktorá ovplyvňuje prevádzky schopnosť IS SP,
- o) krádež a deštrukcia dát IS SP,
- p) zámerné zneužitie prístupu k zariadeniam IS SP,
- q) neplánovaný výpadok elektrického prúdu,
- r) poskytnutie, sprístupnenie, alebo zverejnenie osobných údajov konaním osoby alebo technickou poruchou IS v rozpore s pravidlami platných vnútorných predpisov prevádzkovateľa,
- s) neoprávnené použitie vstupno-výstupných zariadení nepatriacich do vlastníctva prevádzkovateľa, spôsobujúce hrozbu nebezpečnej infiltrácie,
- t) spracúvanie osobných údajov inou ako oprávnenou osobou,
- u) porušenie bezpečnostných vnútorných predpisov prevádzkovateľa majúce za následok nedostupnosť služieb pre klientov alebo partnerov prevádzkovateľa,
- v) porušenie vnútorných predpisov prevádzkovateľa s kontrolovateľným až katastrofálnym dopadom pre prevádzkovateľa.

3.1.7 Poučenie a záväzok mlčanlivosti

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

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

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 materiáloch, ktoré spracujú zadávatelia projektov spolu s IT analytikmi, IT architektami, PM a internými či externými dodávateľmi a následne ich predložia odboru BIS na validáciu.

Obmedzenia

Dokument sa v tejto verzii nezaobrá 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).

Štandardy implementácie

Bezpečnosť životného cyklu

Pri vývoji riešenia je potrebné myslieť na bezpečnosť už od začiatku a prispôbiť 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 commitu.
- 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 špecifikácii 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 prístupit' 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 adresu, cieľovú IP adresu, 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 centrálné 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.

1 Konfigurácia webového servera

System

- 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 právidiel 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 inštalácii 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 inštalácii 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 funkcionality 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 údaje 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 renegotiation 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 správčovské 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 prispôbenie 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 separátном 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, obsahujúcim 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 zobrazit' 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 prístupná 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 iníciaľných 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 sol' (angl. salt).

- 18) Aplikácia musí implementovať funkcionality 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 funkcionality 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 ošetrovania 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 ošetrovania.
- 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 zamietat' neznáme relačné identifikátory zo strany klienta.
- 15) Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú expiráciu 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.

2 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 centrálné spravované a centrálné 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.

3 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 Protocol 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 použitie 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 šestickej časovej pečiatky, 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-F1) 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 šesticte časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 (šesť) mesiacov.

4 Prenos elektronickej pošty

4.1 Prenos elektronickej pošty

- 1) Štandardom prenosu elektronickej pošty je
 - a) používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronickej poštovej správ,
 - b) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group na zabezpečenie prenosu elektronickej poštovej správ.
- 2) SMTP banner by nemal obsahovať informácie o použítom 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 existencii 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 blokovat' 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.

4.2 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.

5 Štandardy prístupu k elektronickým službám

5.1 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.

5.2 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.

6 Štandardy webovej služby

6.1 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.

7 Štandardy integrácie dát

7.1 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.

7.2 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.

8 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).

9 Dátové štandardy

9.1 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 Centrálného 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 odpoveďami, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti) certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.

10 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.

11 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.

12 Firewall

- 1) Všetky prepoje medzi segmentami a externými sieťami musia byť chránené firewallom a všetky spojenia (IN aj OUT) musia byť povolené 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 sietí 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 funkcionálnosť 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 posilať 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).

13 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.

14 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 ošetrovania,
 - 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
- Zákon č. **215/2004** Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
- Trestný zákon č. **300/2005** Z. z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí)
- Zákon č. **45/2011** Z. z. o Kritickej infraštruktúre
- Zákon č. **305/2013** Z. z. o elektronickej podobe výkonu pôsobnosti OVM a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)
- Zákon č. **272/2016** Z. z. o dôverných službách (elektronický podpis) pre elektronické transakcie na vnútornom trhu (eIDAS) a o zmene a doplnení niektorých zákonov
- Zákon č. **18/2018** Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a odporúčacích opatrení (zákon o ochrane osobných údajov)
- Nariadenie GDPR – Nariadenie 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)
- Zákon č. **69/2018** Z. z., o Kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov
- Zákon č. **95/2019** Z. z., o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov
- Zákon č. **452/2021** Z. z. o elektronických komunikáciách (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu

č. **179/2020** Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,

- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **78/2020** Z. z. o štandardoch pre informačné technológie verejnej správy
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **85/2018** Z. z., ktorou sa ustanovujú podrobnosti o spôsobe vyhotovenia a náležitostiach listinného rovnopisu elektronického úradného dokumentu
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **331/2018** Z. z. o zaručenej konverzii
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **438/2019** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy VS
- Vyhláška Ministerstva vnútra Slovenskej republiky č. **29/2017** Z. z. o alternatívnom autentifikátore
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **85/2020** Z. z. o riadení projektov v znení neskorších predpisov
- Vyhláška Národného bezpečnostného úradu č. **338/2004** Z. z. o administratívnej bezpečnosti
- Vyhláška Národného bezpečnostného úradu č. **164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby)
- Vyhláška Národného bezpečnostného úradu č. **165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov v aktuálne platnom znení
- Vyhláška Národného bezpečnostného úradu č. **166/2018** Z. z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- Vyhláška Národného bezpečnostného úradu č. **362/2018** Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Výnos MF SR č. **55/2014** Z. z., o štandardoch pre IS VS v aktuálne platnom znení
- 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-inovaci/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 centrálného 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 dôverylosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

Dôvernosť

Z hľadiska dôverylosti 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 privilegií“ 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 neohroží 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.