Zmluva o poskytovaní služieb

uzatvorená podľa § 84 a nasl. zákona č. 452/2021 Z.z. o elektronických komunikáciách v znení neskorších predpisov a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

1. ZMLUVNÉ STRANY

1.1. **Sociálna poisťovňa**
Ul. 29. augusta 8 a 10,13 63 Bratislava
Štatutárny orgán: Ing. Michal Ilko, generálny riaditeľ Sociálnej poisťovne
Štátna pokladnica
IBAN: SK40 8180 0000 0070 0016 4314
SWIFT: SPSRSKBA
IČO:30807484
DIČ: 2020592332
IČ DPH: SK2020592332
(ďalej len ako „**Účastník alebo Verejný obstarávateľ**“)

1.2. **SWAN, a.s.**
Landererova 12, 811 09 Bratislava
IČO: 35 680 202
IČ DPH: SK2020324317
IBAN: [redacted]
Zapísaná v obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka č.: 2958/B.
zastúpenie: Ing. Juraj Ondriš, predseda predstavenstva
Ing. Miroslav Strečanský, podpredseda predstavenstva
(ďalej len ako „**Podnik alebo Poskytovateľ**“)
(Účastník a Podnik, alebo Verejný obstarávateľ a Poskytovateľ ďalej spolu aj ako „zmluvné strany“)

1.3. Účastník a Podnik týmto podľa § 84 a nasl. zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov (ďalej len „**Zákon**“) a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov uzatvárajú túto Zmluvu o poskytovaní služieb (ďalej len „**Zmluva**") ako výsledok verejného obstarávania uskutočneného Účastníkom ako verejným obstarávateľom formou verejnej súťaže vyhlásenej vo Vestníku verejného obstarávania č. 270/2022 dňa 22.12.2022 pod značkou 50879-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 ako „zákon o verejnom obstarávaní“) na predmet zákazky „*Systém poskytovania komplexných komunikačných služieb virtuálnej privátnej siete, časť 1*: *Primárne linky a integračné služby “.*

2. PREDMET ZMLUVY

2.1. Na základe Zmluvy sa:
2.1.1. Podnik zaväzuje zriadiť a začať poskytovať Účastníkovi verejné elektronické komunikačné služby a verejné elektronické komunikačné siete (ďalej spolu len „**Služby**“ alebo v jednotnom čísle „**Služba**“) v lehote 180 kalendárnych dní odo dňa účinnosti tejto zmluvy, ktoré sú všeobecne popísané v Prílohe č. 1 tejto Zmluvy a konkrétne špecifikované v Prílohe č. 2, časť A a B tejto Zmluvy, za cenu, spôsobom a za podmienok ďalej uvedených v Zmluve a
2.1.2. Účastník sa zaväzuje Služby riadne užívať a platiť za ich užívanie Podniku dohodnutú cenu.
2.2. Zmluvné strany sa dohodli, že Podnik bude Služby poskytovať na miestach, ktoré sú uvedené v Prílohe č. 2 tejto Zmluvy (ďalej len „**Prístupové body**“ alebo samostatne ako „**Prístupový bod**“).

2.3. Podnik sa zaväzuje zriadiť Služby v rozsahu podľa Prílohy č. č. 1 a č 2 tejto Zmluvy do 180 kalendárnych dní odo dňa účinnosti tejto zmluvy. Prípadné zmeny rozsahu služieb bude Podnik povinný realizovať na základe riadne vyplnených a podpísaných jednotlivých objednávok Účastníka (ďalej len „**Objednávky**“ alebo samostatne ako „**Objednávka**“) odovzdaných Podniku, ktoré sa po ich podpise oboma zmluvnými stranami stanú súčasťou Zmluvy pevne nespojenou s telom Zmluvy (vzor objednávky v Prílohe č. 3 Zmluvy) v lehotách uvedených v Prílohe č. 1 Zmluvy. Služba sa považuje za zriadenú a funkčnú po protokolárnom prevzatí pripojenia, t. j. po podpise preberacieho protokolu oboma zmluvnými stranami (vzor preberacieho protokolu je uvedený v Prílohe č. 4 Zmluvy). Zmluvné strany sa dohodli, že na účely tejto Zmluvy sa každá Služba, ktorú má Podnik poskytovať Účastníkovi na základe Objednávky považuje za prevzatú Účastníkom aj v tom prípade, ak ju Účastník napriek pripravenosti Podniku a jeho výzve na prevzatie neprevezme z dôvodov na jeho strane, a to ani v dodatočnej desaťdňovej lehote poskytnutej mu Podnikom.

2.4. Podnik sa zaväzuje Služby objednané Účastníkom podľa bodu 2.3 tohto článku zriaďovať v lehotách uvedených v Objednávkach.

2.5. Služby poskytované na základe tejto Zmluvy sú poskytované nepretržite (24 x 7, t. j. 24 hodín denne, 7 dní v týždni, vrátane sviatkov počas celej doby platnosti Zmluvy).

3. PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN

3.1. Podnik sa zaväzuje dodať Účastníkovi koncové zariadenia (ďalej len „**Zariadenie**“), ak to vyžaduje povaha Služieb. Účastník je oprávnený so súhlasom Podniku meniť výrobcom alebo Podnikom predkonfigurované hodnoty a parametre Next Generation Fire Wall (ďalej len „NGFW“) a sieťových prepínačov, pričom všetky zásahy musia byť logované. Zariadenia musia byť trvale zapnuté. Zabezpečenie nepretržitého elektrického napájania je vecou Účastníka. Všetky Zariadenia poskytnuté Účastníkovi v rámci Služieb zostávajú vo vlastníctve Podniku

3.2. Podnik je ďalej povinný:

- 3.2.1. pri uzatvorení Zmluvy získavať a overovať údaje Účastníka a viesť evidenciu týchto údajov v rozsahu podľa § 56 ods. 3 písm. c) Zákona,
- 3.2.2. poskytovať Služby špecifikované a dohodnuté v Zmluve, v Prílohe č. 1 tejto Zmluvy, Prílohe č. 2 tejto Zmluvy a v Objednávkach,
- 3.2.3. dodržiavať zákon č. 452/2021 Z. z. o elektronických komunikáciách v platnom znení,
- 3.2.4. dodržiavať všetky technické normy a parametre poskytovaných Služieb,
- 3.2.5. neznižovať technické parametre a poskytovať Služby v súlade so záujmami Účastníka.

3.3. Podnik má právo:

- 3.3.1. na úhradu ceny za poskytnutú Službu,
- 3.3.2. na náhradu škody spôsobenej na verejnej sieti Podniku a na Zariadeniach,
- 3.3.3. dočasne prerušiť alebo obmedziť poskytovanie Služby z dôvodu:
  - 3.3.3.1. jej zneužívania podľa bodu 3.4. Zmluvy, a to až do odstránenia jej zneužívania alebo vykonania technických opatrení zamedzujúcich jej zneužívanie,
  - 3.3.3.2. nezaplatenia splatnej sumy za Službu v lehote 30 dní odo dňa jej splatnosti, a to až do jej zaplatenia alebo do zániku Zmluvy; dočasne prerušiť poskytovanie Služieb je Podnik oprávnený iba po predchádzajúcom náležitom upozornení a uplynutí primeranej lehoty určenej na zaplatenie,
  - 3.3.3.3. podstatného porušenia iných zmluvných podmienok zo strany Účastníka; dočasne prerušiť poskytovanie Služby je podnik oprávnený iba po predchádzajúcom náležitom upozornení,
  - 3.3.3.4. narušenia bezpečnosti alebo integrity verejnej siete Podniku, alebo v prípade jej ohrozenia alebo poškodenia,
  - 3.3.3.5. merania a riadenia prevádzky zameraného na zamedzenie preťaženia sieťového spojenia a to na nevyhnutne potrebnú dobu. Pri meraní Podnik testuje chybovosť a zaťaženie jednotlivých častí verejnej siete Podniku. Počas prevádzky sa nepretržite monitoruje priepustnosť jednotlivých častí verejnej siete Podniku a trendy rastu zaťaženia verejnej siete Podniku.
- 3.3.4. zaviesť dodatočné spôsoby ochrany verejnej siete Podniku, ak je to potrebné z dôvodu jej ochrany alebo ochrany Účastníka a pokiaľ zavedenie tejto ochrany nevyvolá dodatočné finančné náklady pre Účastníka,
- 3.3.5. na nevyhnutný čas prerušiť poskytovanie Služby bez predošlého upozornenia:

3.3.5.1. z dôvodov závažných organizačných, technických alebo prevádzkových, napr. havárií charakteru živelných pohrôm, z dôvodu výpadku elektrickej energie, krízových situácií, teroristického útoku, epidémií, brannej pohotovosti štátu a podobne, ktoré sú okolnosťami vylučujúcimi zodpovednosť podľa právnych predpisov Slovenskej republiky,

3.3.5.2. v prípade, že k takémuto obmedzeniu alebo prerušeniu bude Podnik povinný pristúpiť podľa rozhodnutia príslušného štátneho orgánu Slovenskej republiky.

3.4. Za zneužívanie Služieb sa považuje najmä, ak

3.4.1. Účastník použije Službu na podporu, vytvorenie možnosti, alebo zapojenie sa do akejkoľvek nezákonnej alebo nevhodnej aktivity, t. j. aktivity v rozpore s dobrými mravmi alebo pravidlami slušnosti, najmä však na prenos urážlivej, obťažujúcej alebo zlomyseľnej komunikácie, alebo na šírenie poplašnej správy alebo výhražných informácií,

3.4.2. Účastník použije Službu na narušenie verejnej siete Podniku, vrátane akéhokoľvek pokusu o získanie neoprávneného prístupu k Službám alebo k verejnej sieti Podniku,

3.4.3. Účastník sa pokúsi o preťaženie verejnej siete Podniku akýmkoľvek spôsobom, alebo uskutoční čo i len pokus namierený proti integrite verejnej siete Podniku,

3.4.4. Účastník zasiela nevyžiadanú elektronickú poštu (podľa Zákona č. 452/2021 Z. z. o elektronických komunikáciách),

3.4.5. Účastník poruší alebo využije Službu na porušenie práva duševného vlastníctva (napr. autorské práva v zmysle zákona č. 185/2015 Z. z. Autorský zákon a pod.) Podniku alebo tretích osôb.

3.5. Pre Prípojné body Účastník určí povereného zamestnanca, ktorý bude kontaktnou osobou pre Podnik. Účastník môže určiť aj viac kontaktných osôb. Kontaktná osoba zabezpečí a umožní Podniku, resp. jeho zamestnancom a subdodávateľom za účelom odstraňovania porúch, vykonávania plánovanej údržby, inštalácie a odstraňovania Zariadení a vykonávania iných potrebných prác a výkonov súvisiacich s poskytovaním Služieb, najmä vstup do objektu Prípojného bodu, prístup k technológii a pod. a to na nevyhnutne potrebný čas.

3.6. Účastník sa zaväzuje oznámiť všetky ďalšie údaje a skutočnosti v rámci svojich vedomostí a svojej moci, ktoré sú potrebné na riadne poskytovanie Služieb.

3.7. Preloženie alebo vybudovanie nových Prípojných bodov a zmeny technických parametrov Služieb pre jednotlivé Prípojné body sú dovolené iba na základe dohody zmluvných strán.

3.8. Účastník je ďalej povinný:

3.8.1. používať Službu v súlade so Zákonom a Zmluvou,

3.8.2. platiť cenu za poskytnutú Službu podľa Zmluvy,

3.8.3. používať iba telekomunikačné zariadenia spĺňajúce požiadavky osobitných predpisov,

3.8.4. oznamovať Podniku bez zbytočného odkladu každú zmenu identifikačných údajov a kontaktných osôb,

3.8.5. používať i dodatočne zavedené spôsoby ochrany verejnej siete Podniku.

3.9. Účastník má právo:

3.9.1. na bezplatné odstránenie porúch v poskytovaní Služieb, ktoré nezavinil,

3.9.2. na vrátenie pomernej časti ceny za čas neposkytovania Služieb zavineného Podnikom; toto právo musí uplatniť v Podniku najneskôr do troch mesiacov po obnovení poskytovania Služieb.

4. CENA A PLATOBNÉ PODMIENKY

4.1. Cena za Služby podľa článku 2. Zmluvy je stanovená dohodou zmluvných strán podľa zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov a je špecifikovaná v Prílohe č. 2, časť A tejto Zmluvy a v Objednávkach. Cena za jednotlivé služby je stanovená vo forme jednorazového poplatku za zriadenie príslušnej služby a mesačného poplatku za prevádzkovanie príslušnej služby podľa Prílohy č. 2, časť A tejto zmluvy. Zmluvná cena za Služby poskytované podľa tejto Zmluvy je 23 884 955,- EUR bez DPH (slovom: dvadsaťtrimiliónovosemstoosemdesiatštyritisícdeväťstopäťdesiatpäť eur nula centov).

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

4.2. Pre cenu je stanovená mena – euro.
4.3. Fakturačným obdobím je 1 (jeden) kalendárny mesiac.
4.4. Podnik je oprávnený vyúčtovať faktúrou mesačný poplatok za Službu k prvému dňu mesiaca, ktorý nasleduje po mesiaci, v ktorom bola Služba poskytnutá.
4.5. Zmluvné strany sa dohodli na 30-dňovej splatnosti faktury odo dňa jej riadneho doručenia Účastníkovi. Každá faktúra vystavená Podnikom musí spĺňať náležitosti daňového dokladu podľa § 74 ods. 1 zákona č. 222/2004 Z.z. o dani z pridanej hodnoty v znení neskorších predpisov, a to najmä názov Účastníka a Podniku, sídlo, IČO, označenie tejto zmluvy, splatnosť faktúry, predmet fakturácie, odtlačok pečiatky a podpis oprávneného zástupcu Podniku.
4.6. Účastník má právo vrátiť faktúru, ak nebude obsahovať dohodnuté náležitosti podľa bodu 4.5 tohto článku. V takomto prípade sa zastaví plynutie lehoty splatnosti faktúry a nová 30-dňová lehota splatnosti začne plynúť dňom opätovného doručenia novej bezvadnej faktúry.
4.7. Fakturovaná suma sa považuje za uhradenú dňom odpísania fakturovanej sumy z účtu Účastníka. Ak nastane omeškanie platby faktúry pre dôvody na strane Štátnej pokladnice, nie je Účastník po túto dobu v omeškaní s úhradou sumy uvedenej vo faktúre.
4.8. Zmluvné strany berú na vedomie, že je možné vystaviť a doručiť faktúru podľa tejto zmluvy aj podľa zákona č. 215/2019 Z. z. o zaručenej elektronickej fakturácii a centrálnom ekonomickom systéme a o doplnení niektorých zákonov (ďalej len „zákona č. 215/2019 Z.z.“). Takto vystavená a doručená faktúra musí mať všetky náležitosti podľa § 2 ods. 2 písm. a) až m) zákona č. 215/2019 Z.z.
4.9. Podnik vyhlasuje, že ku dňu uzavretia tejto Zmluvy nie je závislou osobou voči Účastníkovi 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 Účastníkovi v súvislosti s ustanovením § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov je Poskytovateľ povinný Účastníkovi písomne oznámiť a to do 5 dní odo dňa vzniku zmeny.

5. REKLAMAČNÝ PORIADOK

5.1. Účastník je oprávnený podať reklamáciu:
5.1.1. na správnosť úhrady v prípade, ak existuje dôvodné podozrenie, že Podnik nevystavil faktúru za Službu v súlade so Zmluvou,
5.1.2. týkajúcu sa kvality poskytnutých Služieb.
5.2. Podnik si vyhradzuje právo neuznať reklamáciu v prípade, ak zníženie kvality poskytnutých služieb spôsobili okolnosti uvedené podľa Zákona alebo okolnosti vyššej moci.
5.3. Reklamáciu na správnosť úhrady, alebo kvalitu Služieb, je Účastník oprávnený podať písomne a doručiť Podniku v lehote do 30 dní odo dňa, kedy nastala skutočnosť zakladajúca dôvod reklamácie. Reklamácie, ktoré budú doručené Podniku po uplynutí 30 dňovej lehoty, alebo ktoré nebudú podané písomne, nebudú akceptované.
5.4. V reklamácii je Účastník povinný uviesť svoje identifikačné údaje, ako sú najmä meno a priezvisko alebo obchodné meno, adresu bydliska, resp. sídla spoločnosti, IČO spolu s uvedením evidenčného čísla Zmluvy, ktorej sa reklamácia týka a jasným a zrozumiteľným spôsobom popísať predmet reklamácie.
5.5. Podnik je povinný písomne oznámiť Účastníkovi výsledok prešetrenia jeho reklamácie do 30 dní odo dňa jej doručenia na adresu Podniku, inak sa reklamácia považuje za uznanú. V zložitých prípadoch môže Podnik túto lehotu predĺžiť, najviac však o 30 dní; Podnik je povinný o predĺžení písomne informovať Účastníka pred uplynutím pôvodnej 30 dňovej lehoty s uvedením dôvodov. Lehota je zachovaná, ak Podnik odošle svoje oznámenie Účastníkovi najneskôr v posledný deň lehoty. Oznámenie o výsledku prešetrenia reklamácie bude obsahovať výrok a jeho stručné odôvodnenie. Pokiaľ je to vo vzťahu k predmetu reklamácie účelné, v rozhodnutí uvedie Podnik aj krátke technické stanovisko, z ktorého vychádzal pri rozhodovaní o reklamácii.
5.6. Podanie reklamácie na prešetrenie správnosti výšky úhrady nemá odkladný účinok na zaplatenie úhrady, t. j. nezbavuje Účastníka povinnosti uhradiť faktúru do dňa splatnosti. Ak suma presiahne trojnásobok priemerného rozsahu využívania Služieb za predchádzajúcich šesť mesiacov, je Podnik povinný umožniť Účastníkovi odklad zaplatenia časti sumy presahujúcej sumu za priemerný mesačný rozsah využívania Služieb počas predchádzajúcich šesť mesiacov, a to najneskôr do skončenia prešetrovania telekomunikačného zariadenia alebo umožniť Účastníkovi zaplatenie časti sumy presahujúcej trojnásobok priemerného rozsahu využívania v najmenej troch mesačných

splátkach. Ak je využívanie Služieb kratšie ako šesť mesiacov, ale dlhšie ako jeden mesiac, vypočíta sa priemerný rozsah využívania Služieb za celé obdobie využívania Služieb.

5.7. Ak sa na základe reklamácie zistí vada na Zariadení, ktorá sa mohla prejaviť v neprospech účastníka, ale rozsah poskytnutých Služieb ani cenu za ich poskytnutie nemožno preukázateľne zistiť, Účastník zaplatí cenu zodpovedajúcu cene za priemerný mesačný rozsah využívania Služieb za predchádzajúcich šesť mesiacov. Ak je využívanie Služieb kratšie ako šesť mesiacov, ale dlhšie ako jeden mesiac, vypočíta sa priemerný rozsah využívania Služieb za celé obdobie využívania Služieb.

5.8. V prípade, že bude reklamácia uznaná za opodstatnenú a Účastníkovi vznikne právo na vrátenie pomernej časti ceny, bude táto zúčtovaná najneskôr vo fakturačnom období nasledujúcom po fakturačnom období, v ktorom bola reklamácia uznaná, prípadne Podnik dohodne s Účastníkom iný spôsob odškodnenia.

6. SERVIS A GARANCIE

6.1. Pre všetky poskytované Služby Podnik vykonáva odstraňovanie vzniknutých porúch na Zariadeniach dodaných a inštalovaných Podnikom a Zariadeniach, ktoré má v správe Podnik alebo poskytne primerané funkčné náhradné riešenie do 4 hodín (garantovaná doba opravy) od zistenia poruchy dohľadovým centrom Podniku. V prípade nedodržania garantovanej doby opravy Účastník má právo voči Podniku na zaplatenie zmluvnej pokuty vo výške 100 EUR za každú hodinu od uplynutia garantovanej doby opravy, maximálne však do výšky 30% z ceny mesačného prenájmu nefunkčného Zariadenia. Bližšie sú podmienky servisu upravené v Prílohe č. 5 tejto Zmluvy Poriadok a kvalita poskytovania služby SLA.

6.2. Poruchu ohlasuje Účastník alebo kontaktná osoba Účastníka telefonicky alebo e-mailom do dohľadového centra Podniku. Ohlásenie poruchy musí obsahovať okrem podrobného technického popisu poruchy aj evidenčné číslo Zmluvy kvôli identifikácii Služby, meno a telefónne číslo osoby, ktorá poruchu nahlásila, prípadne ďalšie informácie požadované Podnikom pri ohlásení poruchy, ktoré sú bezprostredne potrebné k začatiu odstraňovania poruchy, ako napr. prístupové meno a pod.

6.3. Porucha sa považuje za odstránenú okamihom obnovenia poskytovania Služby alebo okamihom obnovenia dohodnutej úrovne Služby. Odstránenie poruchy Podnik oznámi Účastníkovi telefonicky alebo e-mailom a Účastník potvrdí obnovenie služieb v danom čase.

6.4. Podnik má právo dočasne prerušiť poskytovanie Služieb z dôvodu odstraňovania porúch, pričom vždy zohľadní záujmy Účastníka a obmedzí prerušenie prevádzky na najkratší nevyhnutný čas.

6.5. Plánovanú údržbu je Podnik povinný po dohode s Účastníkom oznámiť Účastníkovi prostredníctvom e-mailu, alebo faxom najneskôr 1 pracovný deň vopred, zodpovedným osobám, ktoré určí Účastník.

6.6. V prípade, že Účastník neumožní Podniku uskutočniť okamžitý servisný zásah na Zariadeniach umiestnených v jeho priestoroch, nebude táto doba započítaná do celkovej lehoty opravy.

6.7. Miesto ohlasovania porúch (24x7x365 vrátane sviatkov) je Helpdesk Podniku (tel. číslo [redacted] alebo [redacted], mail: [redacted]).

6.8. Servisné pokrytie Služby 24x7, t. j. 24 hodín denne, 7 dní v týždni, vrátane sviatkov počas celej doby platnosti Zmluvy.

7. ROZSAH ZODPOVEDNOSTI ZA ŠKODU A NÁHRADA ŠKODY

7.1. Podnik a Účastník zodpovedajú za škody nimi spôsobené v dôsledku zavineného porušenia povinností uvedených v Zákone a Zmluve. Podnik ako aj Účastník nezodpovedajú za nepriame škody, následné škody a ušlý zisk, ak nie je dohodnuté inak.

7.2. Podnik zodpovedá za škodu spôsobenú Účastníkovi neposkytnutím, chybným poskytnutím Služieb alebo iným spôsobom, a to len do výšky pomernej časti ceny podľa Zmluvy za dobu, počas ktorej neboli Účastníkovi poskytované Služby na základe zavinenia Podniku, alebo boli poskytované chybne.

7.3. Podnik nezodpovedá za škodu, ktorá vznikla v dôsledku neposkytnutia alebo obmedzeného poskytnutia Služieb ako priameho dôsledku Užívateľovi oznámenej plánovanej údržby, reštrukturalizácie a rozšírenia verejnej siete Podniku alebo jej časti, ako aj siete prevádzkovanej iným operátorom alebo jej časti.

7.4. Podnik taktiež nezodpovedá za škodu, ktorá vznikla v súvislosti s neposkytnutím alebo nesprávnym poskytnutím Služieb v dôsledku udalostí, ktoré sú okolnosťami vylučujúcimi zodpovednosť podľa

právnych predpisov Slovenskej republiky; ako napr. havárie charakteru živelných pohrôm, výpadky elektrickej energie, krízové situácie, teroristické útoky, epidémie, branná pohotovosť štátu a pod..

7.5. Podnik nezodpovedá za škodu vzniknutú Účastníkovi, ak bola spôsobená nevhodným nastavením Služieb alebo Zariadenia zo strany Účastníka.

7.6. Podnik nezodpovedá za obsah informácií a údajov prenášaných prostredníctvom Služieb a ani za škodu, ktorú ich obsah môže spôsobiť.

7.7. Podnik a ani jeho licenční partneri nenesú zodpovednosť za porušenie právnych predpisov upravujúcich duševné vlastníctvo, ktoré spôsobí Účastník tretej osobe v súvislosti s využívaním Služieb Účastníkom.

7.8. Účastník zodpovedá za zneužitie prístupových kódov zverených mu v súvislosti s využívaním Služieb.

7.9. Na ostatné prípady zodpovednosti za škodu sa primerane vzťahujú ustanovenia slovenského právneho poriadku.

8. DOBA PLATNOSTI ZMLUVY

8.1. Zmluva sa uzatvára na dobu určitú, a to na deväťdesiatšesť 96 mesiacov odo dňa účinnosti tejto zmluvy.

8.2. Platnosť Zmluvy je možné ukončiť:

8.2.1. dohodou zmluvných strán v písomnej forme,

8.2.2. uplynutím doby podľa bodu 8.1. Zmluvy,

8.2.3. odstúpením od Zmluvy zo strany Účastníka z dôvodov uvedených v bode 8.3. Zmluvy,

8.2.4. odstúpením od Zmluvy zo strany Podniku z dôvodov uvedených v bode 8.5. Zmluvy,

8.2.5. výpoveďou od Zmluvy zo strany Podniku podľa bodu 8.6 Zmluvy a

8.2.6. výpoveďou Zmluvy zo strany Účastníka podľa bodu 8.7 Zmluvy.

8.3. Účastník môže odstúpiť od Zmluvy bez sankcií:

8.3.1. za podmienok v zmysle § 87 ods. 9 Zákona.

8.3.2. ak v čase uzavretia tejto mluvy existoval dôvod na vylúčenie objednávateľa pre nesplnenie podmienky účasti podľa §32 ods. 1 písm. a) zákona č. 343/2015 Z. z.,

8.3.3. ak táto Zmluva nemala byť uzavretá s objednávateľom v súvislosti so závažným porušením povinnosti vyplývajúcej z právne záväzného aktu Európskej únie, o ktorom rozhodol Súdny dvoj Európskej únie v súlade so Zmluvou o fungovaní Európskej únie,

8.3.4. ak Podnik nebol v čase uzavretia Zmluvy zapísaný v registri partnerov verejného sektora podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, alebo ak bol vymazaný z registra partnerov verejného sektora alebo ak bol vymazaný z registra partnerov verejného sektora,

8.3.5. ak sa po uzavretí Zmluvy stala konečným užívateľom výhod Podniku alebo jeho subdodávateľa osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní a to po uplynutí 30 dní odo dňa, keď táto skutočnosť nastala, ak táto skutočnosť stále trvá,

8.3.6. podľa § 19 zákona o verejnom obstarávaní alebo ak mu bol právoplatne uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní.

8.4. Ak sa na základe Zmluvy poskytuje viac Služieb, je Účastník oprávnený odstúpiť od Zmluvy z dôvodov uvedených v bode 8.3. Zmluvy buď vo vzťahu k tomu plneniu alebo časti Služby, ktoré je priamo dotknuté dôvodom odstúpenia alebo ktorého poskytovanie nie je možné technicky oddeliť od Služby, ktorého sa dôvod odstúpenia priamo dotýka alebo od celej zmluvy.

8.5. Podnik môže odstúpiť od Zmluvy za podmienok v zmysle § 87 ods. 5 Zákona.

8.6. Podnik môže vypovedať Zmluvu, ak ďalej nemôže poskytovať Službu v dohodnutom rozsahu alebo v potrebnej kvalite z dôvodov technickej neuskutočniteľnosti ďalšieho poskytovania Služby okrem univerzálnej služby. Ak podnik vypovie Zmluvu z dôvodu modernizácie Služieb, s ktorou je spojené ukončenie poskytovania Služby podľa Zmluvy, je povinný s výpoveďou doručiť Účastníkovi ponuku na poskytovanie inej, technicky a cenovo blízkej Služby s jej zvýhodneným zriadením. Výpovedná lehota je 12 mesiacov a začína plynúť od prvého dňa mesiaca nasledujúceho po doručení písomnej výpovede Účastníkovi.

8.7. Účastník je oprávnený písomne vypovedať túto Zmluvu s výpovednou lehotou 1 mesiac, ktorá začína plynúť od prvého dňa nasledujúceho mesiaca po doručení písomnej výpovede Podniku v prípade neplnenia predmetu tejto zmluvy a porušenia SLA parametrov VPS siete Podnikom aspoň v troch SLA parametroch VPS siete, po nepretržitú dobu viac ako 5 pracovných dní.

8.8. Túto Zmluvu je možné meniť počas jej trvania bez nového verejného obstarávania v súlade s ustanovením § 18 zákona o verejnom obstarávaní a v súlade s európskou legislatívou. Zmena Zmluvy musí byť písomná.

9. MIMOSÚDNE RIEŠENIE SPOROV

9.1. Účastník môže predložiť Úradu pre reguláciu elektronických komunikácií a poštových služieb SR spor s Podnikom, a to až po reklamačnom konaní, ak nesúhlasí s výsledkom reklamácie alebo so spôsobom jej vybavenia.

10. DÔVERNOSŤ INFORMÁCIÍ

10.1. Dôvernými informáciami, ktoré sú predmetom ochrany v zmysle tohto článku Zmluvy, sú akékoľvek informácie poskytnuté za účelom realizácie predmetu Zmluvy, ktoré nie sú verejne prístupné, a ktoré niektorá zmluvná strana označí ako dôverné, alebo s ktorými sa má nakladať vzhľadom na okolnosti známe druhej strane pri poskytnutí informácií, ako s dôvernými (ďalej len „dôverné informácie“).

10.2. Dôvernými informáciami nie sú informácie,

10.2.1. ktoré sú, alebo sa následne stanú verejne dostupnými inak, ako porušením povinností podľa tejto dohody prijímateľom, alebo

10.2.2. ktoré boli pred uzavretím tejto Zmluvy známe prijímateľovi bez akejkoľvek povinnosti dodržiavať ich dôvernosť, alebo

10.2.3. ktoré boli získané od tretej osoby, ktorá je oprávnená šíriť tieto informácie.

10.3. Zmluvné strany sú oprávnené dôverné informácie sprístupniť iba:

10.3.1. ak to požaduje zákon alebo iný právny predpis;

10.3.2. ak boli vyžiadané súdmi, orgánmi prokuratúry alebo iným vecne príslušným správnym orgánom na základe zákona;

10.3.3. v rozsahu výslovne povolenom Zmluvou.

10.4. Každá zo zmluvných strán sa týmto zaväzuje, že:

10.4.1. bude zachovávať mlčanlivosť o všetkých dôverných informáciách poskytnutých jej druhou zmluvnou stranou,

10.4.2. bude chrániť dôverné informácie poskytnuté Poskytovateľom dôverných informácií aspoň v takom rozsahu, ako dôverné informácie vlastné, a za tým účelom bude prijímať potrebné opatrenia na ich ochranu,

10.4.3. bude vyhotovovať kópie dokumentov obsahujúcich dôverné informácie len s písomným súhlasom Poskytovateľa dôverných informácií,

10.4.4. poskytne dôverné informácie tretej osobe len s predchádzajúcim písomným súhlasom Poskytovateľa dôverných informácií,

10.4.5. poskytne dôverné informácie svojim zamestnancom, riaditeľom, poverencom, právnym zástupcom, účtovníkom, konzultantom a iným zástupcom, pokiaľ takéto osoby súhlasili s tým, že budú viazané mlčanlivosťou za podmienok podľa tohto článku Zmluvy, alebo obdobnou dohodou,

10.4.6. bude používať dôverné informácie len v súvislosti s realizáciou predmetu Zmluvy,

10.4.7. vráti Poskytovateľovi dôverných informácií na jeho požiadanie všetky dokumenty obsahujúce dôverné informácie,

10.4.8. oznámi Poskytovateľovi dôverných informácií neoprávnené použitie, poskytnutie alebo zverejnenie dôverných informácií, a to ihneď po tomto zistení a bude spolupracovať pri znovuobnovení ochrany dôverných informácií a zabránení ich ďalšiemu neoprávnenému použitiu.

10.5. Povinnosť zachovávať mlčanlivosť o všetkých dôverných informáciách Poskytovateľa dôverných informácií trvá aj po skončení platnosti Zmluvy.

10.6. Zmluvné strany sa zároveň zaväzujú dodržiavať ustanovenia § 17 a nasl. Obchodného zákonníka v znení neskorších právnych predpisov, ktoré upravujú obchodné tajomstvo.

10.7. Podnik súhlasí so zverejnením tejto Zmluvy, vrátane jej príloh v Centrálnom registri zmlúv vedenom Úradom vlády SR, v súlade so zákonom č. 546/2010 Z. z., ktorým sa mení a dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

11. OSOBITNÉ USTANOVENIA

11.1. Podnik vyhlasuje, že má k dispozícii kvalifikovaných expertov v súlade s požiadavkami Účastníka na preukázanie technickej a odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Podnik sa zaväzuje, že požadované služby bude poskytovať Účastníkovi prostredníctvom osôb, ktorými preukazoval splnenie podmienok účasti technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Zoznam expertov je obsahom Prílohy č. 6 k tejto Zmluve. Nahradenie alebo doplnenie týchto osôb inými osobami je možné len so súhlasom Účastníka. V prípade nahradenia osôb musia osoby, ktoré ich nahradia, spĺňať rovnaké podmienky ako sa požadovali v rámci preukázania splnenia podmienok účasti technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní.

11.2. V prípade zmeny niektorého z expertov, ktorí sú uvedení v Prílohe č. 6 k tejto Zmluve, je Podnik povinný toto písomne oznámiť Účastníkovi najneskôr do 5 pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví Zmluvy, údaje o navrhovanom novom expertovi. Nový expert musí spĺňať podmienky podľa bodu 11.1 tohto článku Zmluvy. Zmena nového experta sa vykoná zápisom o zmene prílohy k Zmluve, ktorá nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch účastníkov dohody a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky (ďalej len „CRZ“); vzor zápisu o zmene prílohy k Zmluve tvorí Prílohu č. 8 k tejto Zmluve; osobami oprávnenými konať vo veciach zmeny Prílohy č. 6 sú:
za Účastníka: riaditeľ sekcie informatiky
za Podnik: vedúci odboru verejnej správy

11.3. Na plnenie predmetu Zmluvy môže Podnik využiť subdodávateľov. Podnik je povinný pri uzatvorení Zmluvy uviesť zoznam subdodávateľov, ktorý obsahuje údaje o všetkých známych subdodávateľoch Podniku 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. 7 k tejto dohode a obsahuje okrem uvedených údajov aj podiel plnenia z dohody v % a stručný opis časti Zmluvy, ktorá bude predmetom subdodávky.

11.4. Podnik je povinný písomne oznámiť Účastníkovi akúkoľvek zmenu údajov o subdodávateľovi, ktorý je uvedený v Prílohe č. 7 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 Podnik povinný najneskôr tri (3) pracovné dni pred zmenou subdodávateľa písomne oznámiť Účastníkovi 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, ak mu táto povinnosť zo zákona vyplýva. Zmena nového subdodávateľa sa vykoná zápisom o zmene Prílohy č. 7 k Zmluve, ktorý nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jeho zverejnenia v CRZ; vzor zápisu o zmene prílohy k Zmluve tvorí Prílohu č. 8 k tejto Zmluve; osobami oprávnenými konať vo veciach zmeny Prílohy č. 7 k dohode sú osoby uvedené v bode 11.2 tejto Zmluvy.

11.6. Využitím subdodávateľov nie je dotknutá zodpovednosť Podniku za plnenie predmetu Zmluvy. Pri plnení Zmluvy treťou osobou (subdodávateľom) má Podnik zodpovednosť akoby plnil predmet dohody sám.

11.7. Podnik (v prípade skupiny dodávateľov každý člen skupiny dodávateľov), jeho subdodávatelia a subdodávatelia podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov (ďalej len „zákon o registri partnerov verejného sektora“), musia byť 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 túto povinnosť ukladá. Účastník neuzatvorí túto zmluvu s Podnikom, ak v čase uzatvorenia zmluvy nebude mať Podnik, jeho subdodávatelia alebo subdodávatelia podľa zákona o registri partnerov verejného sektora splnenú podmienku zápisu v registri partnerov verejného sektora (pokiaľ s ohľadom na § 2 ods. 2 zákona o registri partnerov verejného sektora pôjde o partnera verejného sektora), ak im zákon o registri partnerov verejného sektora túto povinnosť ukladá alebo ak Podniku bude uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní.

11.8. Účastník môže podľa § 19 ods. 3 zákona o verejnom obstarávaní odstúpiť od zmluvy, ak Podnik v čase uzatvorenia zmluvy nebol zapísaný v registri partnerov verejného sektora, ak mu zákon o registri partnerov verejného sektora túto povinnosť ukladá alebo ak bol vymazaný z registra partnerov verejného sektora, alebo ak mu bol právoplatne uložený zákaz účasti podľa § 182 ods. 3 písm. b) zákona o verejnom obstarávaní.

12. SÚČINNOSŤ

12.1. Podnik sa zaväzuje poskytnúť Účastníkovi a novému poskytovateľovi služieb, s ktorým Účastník uzavrie zmluvu na základe výsledku verejného obstarávania s predmetom zákazky rovnakým alebo obdobným ako je predmet tejto Zmluvy všetku potrebnú súčinnosť na plynulé odovzdanie a prevzatie poskytovania služieb Účastníkovi a zabezpečenie plynulého poskytovania služieb Účastníkovi.

13. ZÁVEREČNÉ USTANOVENIA

13.1. Právne vzťahy zmluvných strán založené Zmluvou, sa riadia právnym poriadkom Slovenskej Republiky, a to najmä príslušnými ustanoveniami Zákona, Obchodného zákonníka a ďalších právnych predpisov. Pre prípady právnych sporov medzi zmluvnými stranami, ktoré by sa týkali záväzkových vzťahov vyplývajúcich zo Zmluvy, sa zmluvné strany dohodli, že na prejednanie a rozhodnutie takýchto sporov sú príslušné súdne orgány Slovenskej republiky.

13.2. Ak táto Zmluva neustanovuje inak, tak akékoľvek oznámenie, žiadosť, požiadavka, vzdanie sa práva, súhlas, schválenie alebo akákoľvek iná komunikácia, ktorá sa vyžaduje alebo je povolená podľa tejto Zmluvy (ďalej len "Oznámenie"), bude urobená v písomnej forme v slovenskom jazyku a bude sa považovať za doručenú, ak bude doručená do elektronickej schránky alebo osobne alebo poštovou doporučenou listovou zásielkou s doručenkou a poštovným vopred uhradeným príslušným odosielateľom na adresu danej zmluvnej strany uvedenú v článku 1. tejto Zmluvy alebo na takú inú adresu, ktorá bude v súlade s týmto bodom Zmluvy oznámená zmluvnej strane písomne najmenej 5 (päť) pracovných dní vopred. V prípade neúspešného doručenia Oznámenia doporučenou listovou zásielkou sa 3. (tretí) deň uloženia zásielky na pošte bude považovať za deň riadneho doručenia. Akékoľvek Oznámenie podľa tejto Zmluvy bude považované za riadne doručené aj vtedy, ak adresát odmietne prevziať takéto Oznámenie.

13.3. Akékoľvek zmeny tejto Zmluvy je možné vykonať výlučne na základe písomného dodatku k tejto Zmluve podpísanej obidvomi zmluvnými stranami, s výnimkou zmeny experta, ktorá sa uskutoční podľa čl. 11 bodu 11.2 Zmluvy a zmeny subdodávateľa, ktorá sa uskutoční podľa čl. 11 bodu 11.5 Zmluvy. Rovnako akékoľvek zmeny Objednávok je možné vykonať výlučne na základe písomnej dohody zmluvných strán podpísanej obidvomi zmluvnými stranami alebo uzavretím novej Objednávky

13.4. Každé ustanovenie tejto Zmluvy, pokiaľ je to možné, sa interpretuje tak, aby bolo účinné a platné podľa platných právnych predpisov SR. Pokiaľ by však niektoré ustanovenie tejto Zmluvy bolo podľa platných právnych predpisov SR nevymožiteľné alebo neplatné, nebude tým dotknutá platnosť alebo vymožiteľnosť ostatných ustanovení tejto Zmluvy, ktoré budú i naďalej záväzné a v plnom rozsahu platné a účinné. V prípade takejto nevymožiteľnosti alebo neplatnosti budú zmluvné strany v dobrej viere rokovať, aby sa dohodli na zmenách alebo doplnkoch tejto Zmluvy v súvislosti s príslušnou nevymožiteľnosťou alebo neplatnosťou, ktoré sú potrebné na realizáciu zámerov vyjadrených v tejto Zmluve.

13.5. 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, reklamácie, servis a ďalej ustanovení tejto Zmluvy, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení zmluvy, napr. dôvernosť informácií a mlčanlivosť.

13.6. Zmluva je vyhotovená v 4 rovnopisoch, pričom Účastník obdrží po jej podpise dva rovnopisy a Podnik dva rovnopisy.
Zmluva nadobúda platnosť dňom jej podpísania oboma zmluvnými stranami a účinnosť po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády SR.

13.7. Zmluvné strany svojimi podpismi na Zmluve potvrdzujú, že sa so všetkými ustanoveniami Zmluvy riadne oboznámili, tieto sú im jasné a zrozumiteľné, pričom vyjadrujú ich slobodnú a vážnu vôľu

upraviť vzájomné vzťahy dohodnutým spôsobom zbavenú akýchkoľvek omylov, zmluvná voľnosť zmluvných strán nie je žiadnym spôsobom obmedzená a Zmluva nie je uzavretá v tiesni a ani za nápadne nevýhodných podmienok.

13.8. Neoddeliteľnou súčasťou Zmluvy sú jej prílohy:
Príloha č.1: Špecifikácia Služieb
Príloha č.2: A:Cenová kalkulácia a množstvo predmetu zmluvy a B:Zoznam prípojných bodov a špecifikácia predpokladaného množstva expertných prác v jednotlivých lokalitách
Príloha č.3: Vzory Objednávky služby
Príloha č.4: Vzor preberacieho protokolu
Príloha č.5: Poriadok a kvalita poskytovania služby SLA
Príloha č.6: Zoznam expertov
Príloha č.7: Zoznam subdodávateľov
Príloha č.8: Zápis o zmene Prílohy č. X „Zoznam XXX“
Príloha č.9: Sprostredkovateľská zmluva
Príloha č.10: Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

za Účastníka:

podpis : .....
meno : Ing. Michal Ilko
funkcia : generálny riaditeľ Sociálnej poisťovne
dátum : v Bratislave, dňa .....

za Podnik:

podpis : .....
meno : Ing. Juraj Ondriš
funkcia : predseda predstavenstva SWAN, a.s.
dátum : v Bratislave, dňa .....

podpis : .....
meno : Ing. Miroslav Strečanský
funkcia : popredseda predstavenstva SWAN, a.s.
dátum : v Bratislave, dňa .....

Špecifikácia služieb

1. **Predmetom zákazky/zmluvy je:**
   a) Zriadenie a prevádzkovanie **primárnych** dátových pripojení v jednotlivých lokalitách Účastníka, špecifikovaných v Prílohe, časť B,

   b) zriadenie systému a poskytovanie služieb virtuálnej privátnej siete (ďalej len „**VPS SocPoist**“), založenej na technológii SD-WAN, vrátane dodávky a správy koncových zariadení s podporou QoS pre aplikácie a zdroje poskytované z dátového centra,

   c) doplnkové služby v rámci primárnych lokalít Účastníka:

      i. Poskytovanie služieb expertnej a servisnej technickej podpory nad rámec SLA a prvotných inštalačných a konfiguračných prác ktoré budú objednávané na základe osobitnej objednávky v celkovom maximálnom rozsahu 11 368 človeko hodín v jednotlivých lokalitách Účastníka (typ 1 až typ 6) podľa Prílohy, časť B, z toho:

         a) inštalačné práce v rozsahu 2672 človeko hodín,

         b) servisné práce v celkovom rozsahu 4328 človeko hodín,

         c) konfiguračné práce v celkovom rozsahu 2816 človeko hodín,

         d) bezpečnostné práce v celkovom rozsahu 1552 človeko hodín,

      ii. zriadenie nového primárneho pripojenia v jednotlivých lokalitách Účastníka (typ 1 až typ 6) podľa Prílohy, časť A a B a podľa požiadaviek Účastníka na základe samostatnej objednávky,

      iii. navýšenie rýchlosti primárneho pripojenia v jednotlivých lokalitách Účastníka (typ 1 až typ 6) špecifikovaných prílohe, časť A a B a podľa požiadaviek Účastníka na základe samostatnej objednávky.

Predmetom zákazky/zmluvy je zriadenie komunikačného systému a poskytovanie komplexných služieb virtuálnej privátnej siete k prepojeniu pracovísk a poskytovaniu služieb Virtuálnej Privátnej Siete pre potreby obojsmernej dátovej, multimediálnej a hlasovej komunikácie medzi jednotlivými pracoviskami – lokalitami verejného obstarávateľa (ďalej len VPS SocPoist) založeného na technológií SD-WAN a poskytujúcej služby dátového prepojenia pracovísk verejného obstarávateľa, správy a konfigurácie prvkov a zabezpečenia siete spolu s dodaním súvisiacich HW a SW prvkov siete verejného obstarávateľa a ich správa.

Predmet zákazky/zmluvy sa obstaráva na obdobie 96 mesiacov odo dňa účinnosti zmluvy**.**
Poskytovateľ odovzdá všetky pripojenia s rýchlosťou 1Gbit/s a viac na optickom médiu a pripojenie s rýchlosťou do 1Gbit/s na metalickom médiu ukončené koncovkou RJ45 zároveň bude zodpovedný za vybudovanie a podporu pre VPS/SD-WAN sieť SocPoist, Súčasťou predmetu plnenia je aj dodávka, prvotná konfigurácia, správa a servis aktívnych sieťových prvkov.

Základná charakteristika siete Sociálnej poisťovne – súčasná komunikačná sieť
Sieť Sociálnej poisťovne využíva komplexné systémové riešenia integrovaného informačného systému v oblasti poistného na nemocenské, starobné, invalidné, úrazové, garančné poistenie, poistenie v nezamestnanosti a ďalšie, na báze najefektívnejších otvorených riešení a technológií. Jej cieľom je vytvoriť podmienky pre postupné sprístupnenie elektronických služieb v rezorte a zabezpečenie ich použiteľnosti na právne úkony, ako aj zabezpečenie efektívnej integrácie elektronických služieb Sociálnej poisťovne do prostredia e-Governmentu, t. j. vzájomné, efektívne využívanie a zdieľanie elektronických služieb poskytovaných inými modulmi informačných systémov verejnej správy (ďalej len „IS VS“) a

rezortom MPSVR SR v súlade s Národnou koncepciou informatizácie verejnej správy a ostatnými súvisiacimi relevantnými dokumentmi, ktoré prijala vláda Slovenskej republiky v tejto oblasti.
Sieť Sociálnej poisťovne je bezpečne prepojená do vládnej siete GOVNET, ktorá primárne slúži na prepojenia ústredných a rezortných pracovísk a ich užívateľov k ústrednému portálu VS, vrátane prístupu do Vládneho Cloudu.
WAN sieť realizovaná prostredníctvom služby IP MPLS VPN, ktorá zabezpečuje vysokorýchlostné, zálohované pripojenie s vysokou dostupnosťou pre pracoviská Sociálnej poisťovne s centralizovaným prístupom do internetu. Neoddeliteľnou súčasťou riešenia je následne aj infraštruktúra distribuovaná priamo na vzdialených pracoviskách určená pre zabezpečenie komunikácie a ochranu pred útokmi z internetu.

Umiestnenie dátového centra

Verejný obstarávateľ má svoje dátové centrum v lokalite Bratislava - Ul. 29. augusta č. 8 a 10, a všetky ostatné pobočkové lokality zadávateľa sú pripojené cez WAN infraštruktúru založenú na MPLS VPN s výhľadom na migráciu do SD-WAN technológie.

Aplikácie/služby hosťované v DC

Aplikácie/služby hosťované v dátovom centre, ku ktorým majú prístup všetky pobočkové lokality cez WAN:

1. **Aplikácie**
   - webové aplikácie
   - rôzne typy aplikácií klient-server 3-vrstvovej architektúry

2 **Databázy**
   - Väčšinou k 3-vrstvovým aplikáciám sú umiestnené v centrálnom dátovom centre

3. **Cloud**
   - Kancelársky balík Microsoft Office 365
   - Centrálne pripojenie do internetu cez centrálne dátové centrum

4. **Videokonferenčný most a základná infraštruktúra**
   - MS Teams
   - IP telefónia

5. **Patching riešenie (operačný systém, klientsky softvér atď.)**
   - MS Widows operačné systémy - riešené distribuovane
   - Antivírový systém je riešený centralizovane
   - Ostatné patche sa preberajú z centrály

6. **Centralizovaná internetová brána**
   - Momentálne je pripojenie do internetu, realizované cez centrálne dátové centrum

7. **Bezpečnostné riešenia**
   - sú riešené centralizovane, v dátovom centre

2. Technická špecifikácia predmetu zákazky/zmluvy:

Časť: Primárne dátové pripojenia, SD-WAN sieť a podpora

Typy lokalít

Body VPS SocPoist (jednotlivé pracoviská - lokality) sú rozdelené do 6 typov v závislosti od požadovaných parametrov na výkonnosť a kapacitu prepojenia do VPS .
Body VPS SocPoist a jednotlivé minimálne požadované parametre pripojenia jednotlivých pracovísk sú sumarizované v Prílohe, časť B:

Typ 1 – Centrála / Záložná lokalita
Typ 2 – Pobočka 1. úrovne
Typ 3 – Pobočka 2. úrovne
Typ 4 – Pobočka 3. úrovne
Typ 5 – Pobočka 4. úrovne
Typ 6 – Pobočka 5. úrovne

Spôsob a kapacita pripojenia bodov VPS SocPoist

Primárne pripojenie jednotlivých pracovísk všetkých typov 1 až 6 je možné realizovať výhradne jednou z nasledovných možností:

- Pripojenie prostredníctvom optického prenosového média,
- Pripojenie prostredníctvom metalického prenosového média,
- Rádiové pripojenie v licencovanom pásme typu bod - bod

V prípade že úspešných uchádzač bude dodávať obidve časti verejného obstarávania „Systém poskytovania komplexných komunikačných služieb virtuálnej privátnej siete“ musí realizovať záložné pripojenia nezávislou fyzickou trasou v porovnaní s primárnym pripojením s automatickým prepnutím na záložnú linku.

Každý použitý typ prístupu musí garantovať poskytnutie požadovaných parametrov a nesmie byť obmedzený zdieľaním prenosovej kapacity s inými účastníkmi siete poskytovateľa.

Služba pripojenia a zriadenie SD-WAN siete musí zahŕňať aj dodávku a správu koncových zariadení s podporou QoS pre aplikácie a zdroje poskytované z dátového centra a hardware musí byť dostatočne výkonný odpovedajúci parametrom pripojení v Opise predmetu zákazky. Všetky zariadenia za telekomunikačnou službou operátora, ktoré budú v rámci služby poskytovateľa dodávané a nasadené, musia byť nové, nepoužité a dodané s kompletným príslušenstvom, a s deklarovanou dobou podpory od výrobcu po celý čas trvania zmluvy.

Dodávateľ sa zaväzuje zriadiť VPS SocPoist sieť do 180 kalendárnych dní od dňa účinnosti zmluvy.

Bod Typ 1

Primárne pripojenie bodu Typ 1 na uzol poskytovateľa služby musí byť realizované cez optické prenosové médium (optický kábel). Prístupová kapacita primárneho pripojenia musí
byť symetrická a minimálna požadovaná kapacita je 10000 Mbit/s, pričom jej rozdelenie medzi prístup do VPS SocPoist a pripojenie do siete Internet je uvedené v Prílohe, časť B.

Verejný obstarávateľ požaduje aj L2 prepojenie LAN sieti lokalít s pripojením Typ 1 na úrovni 10Gbit/s. Verejný obstarávateľ požaduje funkcionalitu sieťovej bezpečnosti na pripojení Bod Typ 1 s ochranou voči organizovaným útokom typu DDoS. DDoS ochrana je požadovaná na elimináciu nelegitímneho dátového toku, keď je sieťová prevádzka postihnutá útokom typu DDoS a požadované je presmerovať, alebo inak efektívne a z veľkou účinnosťou odfiltrovať útok (napr. protokolu TCP (TCP sync)) minimálne do úrovne 40Gbps. V rámci DDoS ochrany je požadovaný prístup do monitorovacieho rozhrania, ktorý vyhodnocuje prevádzku a informuje obstarávateľa pri zistení útoku. Požadovaná je aj možnosť zaktivovať ochranu manuálne, alebo automaticky s použitím protokolu BGP. Verejný obstarávateľ požaduje použitie technológie alebo technologických zariadení s podporou rýchlosti pripojenia minimálne 20Gbit/s bez výmeny technológie alebo zariadení. Verejný obstarávateľ požaduje minimálne 64 pevných verejných IPv4 adries.

Verejný obstarávateľ požaduje, aby pripojenie bodov „Typ 1“ bolo realizované v systéme vysokej dostupnosti (high availability - HA), pričom každý nod musí individuálne spĺňať parameter priepustnosti

bez obmedzenia prístupovej rýchlosti = primár + backup. Pripojenie do siete Internet musí byť ukončené na centrálnych firewalloch s funkcionalitou (NGFW) zapojených v systéme HA. Požadovaná je kompletná správa zariadení NGFW operátorom a úplný prístup poverených zamestnancov obstarávateľa. Prístup do siete internet musí byť zabezpečený dvojúrovňovo (IPS a UTM ako samostatné služby). NGFW musia umožňovať vytváranie FW kontextov minimálne v počte 8ks s možnosťou rozšírenia. Verejný obstarávateľ požaduje výkonovú rezervu tak aby bolo možné použiť tento HW aj ako interný firewall s priepustnosťou min. 10Gbit/s pri zapnutých všetkých požadovaných bezpečnostných prvkoch: Threat prevention, Sandbox, URL filtering, DNS security, SSL decryption, L7 politiky. NGFW musí poskytovať min. 16x SFP+ portov osadených 10GB MM GBIC, 6 x 100GE QSFP28 portov.

Core prepínače musia spĺňať požadované parametre: všetky porty 10Gbit/s vrátane 10GB MM GBIC, počet portov podľa Prílohy, časť B, podpora statického smerovania, typ prepojovacích „trunk“ portov 10GE SFP, prepínacia kapacita minimálne 560 Gb/s full duplex s priepustnosťou minimálne 417 Mpps, počet aktívnych VLAN minimálne 1023 a unikastových MAC adries minimálne 16 000, podpora štandardov minimálne: IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS, Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad.

Verejný obstarávateľ zároveň požaduje aj prepojenie LAN siete na lokalite typ 1 s LAN sieťou na:

- Lokalite typ 2 na úrovni 1000Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní.
- Lokalite typ 3 na úrovni 300Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní.
- Lokalite typ 4 na úrovni 200Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní.
- Lokalite typ 5 na úrovni 100Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní.
- lokalite typ 6 na úrovni 50Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní.

Bod Typ 2

Primárne pripojenie bodu Typ 2 na uzol poskytovateľa služby musí byť realizované cez pevné prenosové médium (optický kábel/metalický kábel). Prístupová kapacita primárneho pripojenia musí byť symetrická a minimálna požadovaná kapacita je 1000 Mbit/s. Verejný obstarávateľ požaduje použitie technológie alebo technologických zariadení s podporou rýchlosti pripojenia minimálne 5Gbit/s bez výmeny technológie alebo zariadení. Verejný obstarávateľ požaduje minimálne 2 pevné verejné IPv4 adresy. Verejný obstarávateľ požaduje prepojenie LAN siete na lokalite typ 2 s LAN sieťou na lokalite typ 1 na úrovni 1Gbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní. Pripojenie do LAN siete musí byť ukončené na pobočkových firewalloch s funkcionalitou NGFW zapojených v systéme HA (aktív / pasív). Ponúknuté firewally musia podporovať L3 routing a funkcionalitu DHCP. Minimálny throughput 2,2Gbit/s pri zapnutých všetkých požadovaných bezpečnostných prvkoch: Threat prevention, Sandbox, URL filtering, DNS security, SSL decryption, L7 politiky. Minimálne 2x10Gbit/s s osadenými sfp modulmi a 4xEth 1Gbit/s.

Core prepínače využité v navrhovanom riešení musia mať SFP uplink porty s 10Gbit/s podporou. Prepínač musí spĺňať požadované parametre: počet portov v jednotlivých lokalitách podľa Prílohy, časť B, podpora statického smerovania, podpora PoE+ a PoE banka minimálne 600W na všetkých LAN portoch, typ prepojovacích „trunk“ portov 10GE SFP, prepínacia kapacita minimálne 160 Gb/s full duplex s priepustnosťou minimálne 120 Mpps, počet aktívnych VLAN minimálne 1023 a unikastových MAC adries minimálne 16 000, podpora štandardov minimálne: IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS, Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad.

Bod Typ 3

Primárne pripojenie bodu Typ 3 na uzol poskytovateľa služby musí byť realizované cez pevné prenosové médium (optický kábel/metalický kábel) alebo rádiové pripojenie typu bod - bod v licencovanom pásme.

Prístupová kapacita primárneho pripojenia musí byť symetrická a minimálna požadovaná kapacita je 300 Mbit/s. Verejný obstarávateľ požaduje použitie technológie alebo technologických zariadení s podporou rýchlosti pripojenia minimálne 1Gbit/s bez výmeny technológie alebo zariadení. Verejný obstarávateľ požaduje minimálne 2 pevné verejné IPv4 adresy. Verejný obstarávateľ požaduje prepojenie LAN siete na lokalite typ 3 s LAN sieťou na lokalite typ 1 na úrovni 300Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní. Pripojenie do LAN siete musí byť ukončené na pobočkových firewalloch s funkcionalitou NGFW zapojených v systéme HA (aktív / pasív). Ponúknuté firewally musia podporovať L3 routing a funkcionalitu DHCP. Minimálny throughput 500Mbit/s pri zapnutých všetkých požadovaných bezpečnostných prvkoch: Threat prevention, Sandbox, URL filtering, DNS security, SSL decryption, L7 politiky. Minimálne 2x1Gbit/s s osadenými sfp modulmi a 3xEth 1Gbit/s.
Core prepínače využité v navrhovanom riešení musia mať aj SFP uplink porty s 1Gbit/s podporou a tiež musia mať ethernet porty s 1Gbit/s podporou a musia mať natívnu funkcionalitu stacku. Prepínač musí spĺňať požadované parametre: počet portov v jednotlivých lokalitách podľa Prílohy, časť B, podpora statického smerovania, podpora PoE+ a PoE banka minimálne 600W na všetkých LAN portoch, typ prepojovacích „trunk“ portov 1GE SFP, prepínacia kapacita minimálne 160 Gbps full duplex s priepustnosťou minimálne 120 Mpps, počet aktívnych VLAN minimálne 1023 a unikastových MAC adries minimálne 16 000, podpora štandardov minimálne: IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS, Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad.

Bod Typ 4

Primárne pripojenie bodu Typ 4 na uzol poskytovateľa služby musí byť realizované cez pevné prenosové médium (optický kábel/metalický kábel) alebo rádiové pripojenie typu bod - bod v licencovanom pásme. Prístupová kapacita primárneho pripojenia musí byť symetrická a minimálna požadovaná kapacita je 200 Mbit/s. Verejný obstarávateľ požaduje použitie technológie alebo technologických zariadení s podporou rýchlosti pripojenia minimálne 1Gbit/s bez výmeny technológie alebo zariadení. Verejný obstarávateľ požaduje minimálne 2 pevné verejné IPv4 adresy. Verejný obstarávateľ požaduje prepojenie LAN siete na lokalite typ 4 s LAN sieťou na lokalite typ 1 na úrovni 200Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní. Pripojenie do LAN siete musí byť ukončené na pobočkovom firewalle s funkcionalitou NGFW zapojených v systéme HA (aktív / pasív). Ponúknuté firewally musia podporovať L3 routing a funkcionalitu DHCP. Minimálny throughput 250Mbit/s pri zapnutých všetkých požadovaných bezpečnostných prvkoch: Threat prevention, Sandbox, URL filtering, DNS security, SSL decryption, L7 politiky. Minimálne 2x1Gbit/s s osadenými sfp modulmi a 3xEth 1Gbit/s.

Core prepínače využité v navrhovanom riešení musia mať aj SFP uplink porty s 1Gbit/s podporou a tiež musia mať ethernet porty s 1Gbit/s podporou a musia mať natívnu funkcionalitu stacku. Prepínač musí spĺňať požadované parametre: počet portov v jednotlivých lokalitách podľa Prílohy časť B, podpora statického smerovania, podpora PoE+ a PoE banka minimálne 600W na všetkých LAN portoch, typ prepojovacích „trunk“ portov 1GE SFP, prepínacia kapacita minimálne 160 Gbps full duplex s priepustnosťou minimálne 120 Mpps, počet aktívnych VLAN minimálne 1023 a unikastových MAC adries minimálne 16 000, podpora štandardov minimálne: IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS, Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad.

Bod Typ 5

Primárne pripojenie bodu Typ 5 na uzol poskytovateľa služby musí byť realizované cez pevné prenosové médium (optický kábel/metalický kábel) alebo rádiové pripojenie typu bod - bod v licencovanom pásme. Prístupová kapacita primárneho pripojenia musí byť symetrická a minimálna požadovaná kapacita je 100 Mbit/s. Verejný obstarávateľ požaduje použitie technológie alebo technologických zariadení s podporou rýchlosti pripojenia minimálne 500Mbit/s bez výmeny technológie alebo zariadení. Verejný obstarávateľ požaduje minimálne 2 pevné verejné IPv4 adresy. Verejný obstarávateľ požaduje prepojenie LAN siete na

lokalite typ 5 s LAN sieťou na lokalite typ 1 na úrovni 100 Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní. Pripojenie do LAN siete musí byť ukončené na pobočkovom firewalle s funkcionalitou NGFW. Ponúknuté firewally musia podporovať L3 routing a funkcionalitu DHCP. Minimálny throughput 120Mbit/s pri zapnutých všetkých požadovaných bezpečnostných prvkoch: Threat prevention, Sandbox, URL filtering, DNS security, SSL decryption, L7 politiky. Minimálne 3xEth 1Gbit/s.

Core prepínače využité v navrhovanom riešení musia mať aj SFP uplink porty s 1Gbit/s podporou a tiež musia mať ethernet porty s 1Gbit/s podporou. Prepínač musí spĺňať požadované parametre: počet portov v jednotlivých lokalitách podľa Prílohy, časť B, podpora statického smerovania, podpora PoE+ a PoE banka minimálne 400W na všetkých LAN portoch, typ prepojovacích „trunk“ portov 1GE SFP, prepínacia kapacita minimálne 120 Gbps full duplex s priepustnosťou minimálne 65 Mpps, počet aktívnych VLAN minimálne 1023 a unikastových MAC adries minimálne 16 000, podpora štandardov minimálne: IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS, Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad.

Bod Typ 6

Primárne pripojenie bodu Typ 6 na uzol poskytovateľa služby musí byť realizované cez pevné prenosové médium (optický kábel/metalický kábel) alebo rádiové pripojenie typu bod - bod v licencovanom pásme. Prístupová kapacita primárneho pripojenia musí byť symetrická a minimálna požadovaná kapacita je 50 Mbit/s. Verejný obstarávateľ požaduje použitie technológie alebo technologických zariadení s podporou rýchlosti pripojenia minimálne 250Mbit/s bez výmeny technológie alebo zariadení. Verejný obstarávateľ požaduje minimálne 2 pevné verejné IPv4 adresy. Verejný obstarávateľ požaduje prepojenie LAN siete na lokalite typ 6 s LAN sieťou na lokalite typ 1 na úrovni 50 Mbit/s. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní. Pripojenie do LAN siete musí byť ukončené na pobočkovom firewalle s funkcionalitou NGFW. Ponúknuté firewally musia podporovať L3 routing a funkcionalitu DHCP. Minimálny throughput 80Mbit/s pri zapnutých všetkých požadovaných bezpečnostných prvkoch: Threat prevention, Sandbox, URL filtering, DNS security, SSL decryption, L7 politiky. Minimálne 3xEth 1Gbit/s.

Core prepínače využité v navrhovanom riešení musia mať aj SFP uplink porty s 1Gbit/s podporou a tiež musia mať ethernet porty s 1Gbit/s podporou. Prepínač musí spĺňať požadované parametre: počet portov v jednotlivých lokalitách podľa Prílohy, časť B, podpora statického smerovania, podpora PoE+ a PoE banka minimálne 370W na všetkých LAN portoch, typ prepojovacích „trunk“ portov 1GE SFP, prepínacia kapacita minimálne 120 Gbps full duplex s priepustnosťou minimálne 65 Mbps, počet aktívnych VLAN minimálne 1023 a unikastových MAC adries minimálne 16 000, podpora štandardov minimálne: IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS, Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad.

SLA Parametre VPS SocPoist

Minimálna dostupnosť služby v čase 6:00 - 18:00 hod – 99,70%

Maximálne tolerovaná doba nedostupnosti služby za fakturačné obdobie – maximálne 0,5%

Parametre pre symetrické pripojenie bodu typu 1-4:

- RTT pre rámec 100 B do 10 ms
- Jitter pre rámec 100B do 10 ms
- Packet loss maximálne 0,3%

Parametre pre symetrické pripojenie bodu typu 5-6:

- RTT pre rámec 100 B do 30 ms
- Jitter pre rámec 100B do 15 ms
- Packet loss maximálne 0,3%

Odstránenie výpadku primárneho spojenia:

- Typ 1 – 2 hodiny
- Typ 2 – 4 hodiny
- Typ 3 – 6 hodín
- Typ 4 – 6 hodín
- Typ 5 – 8 hodín
- Typ 6 – 8 hodín

Plánovaná údržba:

- Po odsúhlasení výpadku pripojenia Verejným obstarávateľom neobmedzená.
- Bez súhlasu max. 24 hodín ročne s oznámením 3 pracovné dní dopredu

Prevádzka dohľadového centra 24h/ 365 dní

Odozva operátora ku kontaktnej osobe max. 60 minút

Zákaznícka podpora – priama 24h/ 365 dní

Požiadavky na podporu budú spracúvané automatizovane. Poskytovateľ sa zaväzuje najneskôr k začiatku poskytovania služby pripraviť interný automatický Service desk systém, na ktorý bude prijímať požiadavky na podporu a automatizovane ho prepojiť so Service desk systémom objednávateľa. Technickú špecifikáciu k tomu prepojeniu a postup nastavenia prepojenia Service desk systémov dodá objednávateľ a poskytovateľ je povinný ho dodržať a aplikovať vo svojom prostredí na svoje náklady.

Nástroj Service Desk: IBM Control Desk 7.6 – verejný obstarávateľ požaduje aby sa uchádzač vedel integrovať do uvedeného systému, ktorý využíva verejný obstarávateľ.

Meranie SLA parametrov siete

- Verejný obstarávateľ požaduje vykonávanie pravidelných meraní Dostupnosti služby za Obdobie/Monitoring.
- Verejný obstarávateľ požaduje právo na meranie Dostupnosti služby. V prípade nezhody vo výsledkoch merania vykoná Poskytovateľ a Účastník porovnanie nameraných hodnôt, prešetrí všetky zaznamenané hodnoty (odpočíta nezapočítavané hodnoty uvedené vyššie) a opätovne vykoná výpočet Dostupnosti služby.

Spôsob merania SLA parametrov siete

- Verejný obstarávateľ požaduje meranie oneskorenia, stratovosti, variácie oneskorenia. Meranie sa vykonáva medzi zariadením Prevádzkovateľa umiestneného v lokalite verejného obstarávateľa a referenčným bodom umiestneného v SIXe. Meranie sa vykonáva vždy v prípade, kedy je služba určená výlučne na Meranie. Účastník má taktiež právo na meranie. V prípade nezhody vo výsledku merania sa meranie vykoná opätovne. Doba merania závisí od individuálnej dohody s Verejným obstarávateľom.

Poskytované služby

Verejný obstarávateľ požaduje zabezpečiť poskytovanie nasledujúcich základných komunikačných služieb:

- Uzavretú SD-WAN VPS SocPoist prepájajúcu všetky pracoviská pre bezpečný prenos dát,
- Redundantné prepojenie všetkých pracovísk pre zabezpečenie vysokej spoľahlivosti služby v rozsahu podľa stanovených SLA parametrov,
- Centralizovaný riadený spoločný prestup do verejnej siete internet s vysokým stupňom bezpečnosti v rozsahu podľa stanovených SLA parametrov,
- Správu NGFW - aplikácia definovaných politík (podľa zadania verejného obstarávateľa), content, web filteringu, DDoS a IPS ochrany a elimináciu útokov z internetu v minimálnom rozsahu 40 človekohodín mesačne plus report bezpečnostných incidentov

- Prenos a distribúcia multimediálnych streamov (video / hlas / dáta),

Distribúcia jednotlivých služieb v rámci VPS SocPoist musí byť realizovaná s využitím nastavenia parametrov Quality of Service (QoS) s minimálne 6 kvalitatívnymi triedami (IP hlas, IP multimédia, mission critical data, high business application, low business application a best effort traffic). Súčasťou poskytovaných komunikačných služieb musí byť aj online nástroj na nepretržité monitorovanie VPS (dostupnosť a vyťaženie koncových zariadení, vyťaženie liniek, odozva liniek) požadovaný je aj grafický výstup, SLA parametrov VPS SocPoist.

Služba musí zahŕňať dodávku a správu **Nástroja na manažment a dohľad siete** s nasledovnými parametrami:

Monitorovacia časť

- Prevedenie – HW/ virtuálny appliance.
- Grafické rozhranie na správu.
- Zobrazenie topológie siete.
  Nástroje na monitorovanie, vrátane monitoringu v reálnom čase aj pre existujúcu infraštruktúru, zahrňujúcu komponenty dátovej siete od dodávateľov – CISCO, HP, FORTINET, ALE do množstva 300 ks.

Používané modely zariadení : HP 5130, HP 5120,HP 2530, ALE 6350, ALE 6360, ALE 6850, ALE 6250, ALE 6248, ALE 6224, ALE 6024, FS-1024D, APIC-SERVER-M3, NEXUS N9K-C9336C-FX2, NEXUS N9K-C9332C, NEXUS 93180YC-FX3, NEXUS N9K-C93180YC-FX3

Generovanie reportov bezpečnostných rizík prevádzkovanej infraštruktúry.

- na základe podrobného prehľadu zaťaženia siete umožňujú nástroje efektívne plánovanie rozširovania siete,
- systém umožňuje upozorniť kľúčových zamestnancov, ak nastanú mimoriadne udalosti.

FW časť

- Monitorovanie až na aplikačnú vrstvu OSI modelu s možnosťou výberu protokolov.
- Hlásenia o sieťovej prevádzke, hrozbách, aktivitách a trendoch na sieti.
- Sken logov na detekciu APT / (Advanced Persistent Threat) - pokročilá pretrvávajúca hrozba /
- Real-time zobrazovanie a historické náhľady o aktivite na sieti – súhrn aplikácií, zdrojov, cieľov, webových stránok, bezpečnostných hrozieb, administratívnych zmien a systémových udalostí.
- Možnosť automatického blokovania infikovaných zariadení / častí sietí.
- Možnosť zapnutia indikátorov ohrozenia (Indicators of Compromise), ktoré zobrazujú koncových používateľov s podozrivým využívaním webu. Poskytujú informácie min. v rozsahu: IP adresy koncových používateľov, názov hostiteľa, skupinu, operačný systém, celkovú mieru ohrozenia, mapový náhľad a počet hrozieb. Zobraziť sa dajú aj detaily jednotlivých hrozieb.
- Klasifikácia služby/aplikácie, ktoré používajú užívatelia a to aj v prípade, že sú neštandardné (napr. http, ktorá štandardne používa port 80 bude používať iný port a pod.).
- preddefinované a vlastné grafy, ktoré pomáhajú monitorovať a identifikovať problematické situácie, pokusy o útoky a vykonávať revíziu nastavenia bezpečnostných politík,
- pokročilé vlastnosti min. v rozsahu: korelácia udalostí, forenzná analýza a odhaľovanie zraniteľností tvoria základné nástroje na hĺbkovú ochranu komplexných sietí,
- systém umožňuje upozorniť kľúčových zamestnancov, ak nastanú mimoriadne udalosti,
- systém rozoznáva min. nasledovné typy logov (ako napríklad prevádzka, webový filter a pokusy o útok) pre vykonávanie forenznej analýzy s detailným záznamom sledovanej akcie.
- možnosť definície FW pravidiel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je: min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.
- podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií.

Konfiguračná časť

- Prevedenie – HW/ virtuálny appliance.
- Licencie pre spravovanie prepínačov

- Kompletná správa životného cyklu infraštruktúry (nasadenie, administrácia, monitoring, odstraňovanie problémov).
- Grafické rozhranie na správu.
- Zobrazenie topológie siete.
- Inventarizácia prvkov v sieti, hromadná inštalácia aktualizácií podľa potreby.
- Možnosť zadefinovania PnP template pre automatickú konfiguráciu prepínačov.
- Automatická konfigurácia prepínačov.

Požiadavky na výkon

- Minimálne 200GB logov / deň
- Miera analýzy minimálne 4000 logov / sekunda
- Miera zberu dát minimálne 6000 logov / sekunda

Dátové prepojenie pracovísk

Služba dátového prepojenie pracovísk musí spĺňať všetky nasledujúce požiadavky:

- Umožniť obojsmernú dátovú komunikáciu založenú na protokole IP medzi všetkými bodmi formou topológie každý s každým cez sieťovú štruktúru SD-WAN s možnosťou nastavenia ľubovoľných obmedzení v smerovaní tokov podľa požiadaviek verejného obstarávateľa.
- Transport dát zabezpečiť minimálne v 6 kvalitatívnych triedach (IP hlas, IP multimédia, mission critical data, high business application, low business application a best effort traffic), pričom priradenie jednotlivých zdrojov dát (aplikácií) do týchto tried bude realizované na základe požiadaviek verejného obstarávateľa.
- Všetka prevádzka vzdialenej lokality musí byť pri prenose cez všetky prenosové linky WAN SD-WAN vrstva (overlay) šifrovaná.
- Šifrovanie sa musí vykonať podľa štandardov IPsec pomocou AES s 256-bitovými kľúčmi alebo vyššími v spojení s Internet Key Exchange verzie 2 (IKEv2) alebo vyššej vrátane možnosti použitia certifikátov.
- Používanie šifrovania nemôže znižovať rýchlosť a definované SLA linky, alebo dostupnosť aplikácií na vzdialenom mieste a musí byť pre koncových používateľov transparentné.
- Navrhované riešenie SD-WAN musí mať stavové bezpečnostné funkcie (filtrovanie L3 až L7, zónová ochrana siete, DoS ochrana) na izoláciu siete v CPE spolu s funkciami SD-WAN

Bezpečný centrálny prístup do verejnej siete Internet

Služba bezpečného centrálneho prístupu do verejnej siete Internet musí spĺňať všetky nasledujúce požiadavky:

- Neagregované pripojenie do siete Internet (svetovej aj slovenskej) v uzle Typ 1. musí mať v uzle Typ 1 garantovanú kapacitu minimálne 5000 Mbit/s symetricky.
- V záložnom pripojení pracoviska Typ 1 musí byť pre prístup do siete Internet rezervovaná minimálna kapacita 5000 Mbit/s symetricky.

Verejný obstarávateľ požaduje minimálne 64 pevných verejných IP adries. Poskytovateľ vo svojom návrhu pre NGFW musí zohľadniť kapacitné požiadavky.

Súčasťou ochrany prístupu z Internetu musí byť:

- Systém kontroly pred malvérom využívajúcim zero-day alebo neznámych zraniteľností - sandbox. Systém musí byť dimenzovaný pre minimálne 10000 e-mailových kont, 500000 emailov denne a operačný systém MS Windows 10, 11 – požaduje sa z dôvodu, že verejný obstarávateľ uvedený OS využíva vo svojom systéme.
- Prístup do siete internet musí byť zabezpečený IPS systémom a UTM systémom.

Verejný obstarávateľ požaduje pre poverené osoby úplný prístup na všetky zariadenia použité v LAN sieti Verejného obstarávateľa.
Poskytovateľ vo svojom návrhu pre NGFW musí zohľadniť kapacitné požiadavky pre výkonnosť s zapnutými všetkými požadovanými bezpečnostnými prvkami aspoň 5Gbit/s pre firewall na centrále – Typ 1 a 6, a pre pobočky minimálne 50 MB/s, špecifikované pre každý typ NGFW v popise podľa typu.
Súčasťou Firewall ochrany prístupu z Internetu musí byť schopnosť chrániť prístup do siete Internet prostredníctvom funkcionalít systémov

Ústredie firewall – TYP 1 musí poskytovať nasledovné:

- Threat Prevention, Intrusion Prevention System
- Sanboxing, dynamickú a statickú analýzu súborov
- URL filtering, filtrovanie webového obsahu
- DNS bezpečnosť, kontrolu DNS tokov na hrozby
- SSL decryption, kontrola šifrovaných tokov SSL a TLS
- Rozpoznávanie L7 aplikácii a možnosť vytvárať politiky na ich základe.
- API rozhranie.

Pobočkové Firewally, TYP 2-6, musia poskytovať minimálne nasledovné:

- URL filtering, filtrovanie webového obsahu
- Threat Prevention, Intrusion Prevention System
- SSL decryption, kontrola šifrovaných tokov SSL a TLS
- Rozpoznávanie L7 aplikácii a možnosť vytvárať politiky na ich základe.
- API rozhranie.

Firewall:

Administratívny správca v riešení aplikuje a prevádzkuje aktuálnu bezpečnostnú politiku v zmysle interných bezpečnostných smerníc.
Plnenie poskytovaných služieb

Verejný obstarávateľ požaduje maximálnu dobu plnenia nasledovne:
Zriadenie dátového pripojenia pracovísk SocPoist:

Typ primárneho dátového pripojenia	Maximálna doba zriadenia služby od účinnosti zmluvy v dňoch
Typ 1	max. do 180 dní
Typ 2	max. do 180 dní
Typ 3	max. do 180 dní
Typ 4	max. do 180 dní
Typ 5	max. do 180 dní
Typ 6	max. do 180 dní

Doplnkové služby

Verejný obstarávateľ v nadväznosti na základné horeuvedené komunikačné služby môže požadovať poskytovanie doplnkových služieb, ktoré by boli poskytované ako rozšírenie existujúcich základných služieb SD-WAN siete o nové funkcionality, resp. by boli poskytované formou expertnej technickej podpory. Poskytovateľ musí poskytovať nasledujúci minimálny rozsah doplnkových služieb:

a) Poskytovanie služieb expertnej a servisnej technickej podpory nad rámec SLA a prvotných inštalačných a konfiguračných prác

Poskytovateľ na základe požiadavky verejného obstarávateľa (vystavenej formou objednávky) je povinný poskytovať službu expertnej technickej podpory, ktorá bude realizovaná prostredníctvom expertov poskytnutých podnikom na expertných alebo servisných prácach pri inštalácií alebo konfigurácií zariadení, optimalizácií prevádzky VPS SocPoist, presmerovaní a preložení prístupových okruhov, konfigurácia bezpečnosti a podobne. Zoznam expertov (viď. príloha č. 6 zmluvy Zoznam expertov).

Expertnými prácami sa rozumejú:

- Inštalačné práce – inštalácia software/firmware na aktívne sieťové prvky LAN a WAN siete, inštalácia a montáž aktívnych a pasívnych sieťových prvkov LAN a WAN siete ako router, switch, firewall a pod.
- Konfiguračné práce – konfigurácia aktívnych a pasívnych sieťových prvkov LAN a WAN siete ako router, switch, firewall a pod.
- Servisné práce – údržba a čistenie aktívnych a pasívnych sieťových prvkov LAN a WAN siete, servis a údržba existujúcej štruktúrovanej kabeláže v rámci serverovní a rackov, práce s prepojovacími patchcordami medzi portami a patch panelmi aj rozvody štruktúrovanej kabeláže v rámci budovy (medzi miestnosťami, poschodiami a pod.) a taktiež aj servis a údržba optických prenosových médií a ich súčastí v serverovniach ale aj v rámci budovy
- Bezpečnostné práce - konfigurácia bezpečnostných nastavení na aktívnych a sieťových prvkov LAN a WAN siete ako router, switch, firewall a pod.

Expertné práce sú vykonávané na všetkých pobočkách verejného obstarávateľa podľa Prílohy, časť B kde sú uvedené aj odhadované rozsahy prác za konkrétne lokality.

b) Poskytovateľ na základe požiadavky verejného obstarávateľa (vystavenej formou objednávky) je povinný zriadiť ďalší bod pripojenia do VPS SocPoist na lokalite podľa zadania Verejného obstarávateľa.

- Zriadenie ďalšieho bodu Typ 1, Typ 2, Typ 3, Typ 4, Typ 5 a Typ 6

c) Poskytovateľ na základe požiadavky verejného obstarávateľa (vystavenej formou objednávky) je povinný navýšiť kapacitu pripojenia do VPS SocPoist na lokalite podľa zadania Verejného obstarávateľa.

- Navýšenie kapacity pripojenia pre primárny prístup pre body Typ 1, Typ 2, Typ 3, Typ 4, Typ 5 a Typ 6

- Navýšenie kapacity pripojenia v krokoch nasledovne:

Tabuľka navyšovania kapacity pripojení	
Pripojenie	**Kapacita primárna linka**
Typ 1	1000Mbit/s
Typ 2	100Mbit/s
Typ 3	50Mbit/s
Typ 4	20Mbit/s
Typ 5	10Mbit/s
Typ 6	10Mbit/s

Plnenie poskytovaných služieb

Verejný obstarávateľ požaduje maximálnu dobu plnenia nasledovne:
Zriadenie/navýšenie nových liniek

Typ primárneho pripojenia	Maximálna doba zriadenia služby od doručenia objednávky v mesiacoch
Navýšenie pripojenia typ 1 o 1000Mbit/s	max. do 3 mesiacov
Navýšenie pripojenia typ 2 o 100Mbit/s	max. do 3 mesiacov
Navýšenie pripojenia typ 3 o 50Mbit/s	max. do 3 mesiacov
Navýšenie pripojenia typ 4 o 20Mbit/s	max. do 3 mesiacov
Navýšenie pripojenia typ 5 o 10Mbit/s	max. do 3 mesiacov
Navýšenie pripojenia typ 6 o 10Mbit/s	max. do 3 mesiacov
Zriadenie nového pripojenia typ 1	max. do 3 mesiacov
Zriadenie nového pripojenia typ 2	max. do 3 mesiacov
Zriadenie nového pripojenia typ 3	max. do 3 mesiacov
Zriadenie nového pripojenia typ 4	max. do 3 mesiacov
Zriadenie nového pripojenia typ 5	max. do 3 mesiacov
Zriadenie nového pripojenia typ 6	max. do 3 mesiacov

Časť A: CENOVÁ KALKULÁCIA, MNOŽSTVO PREDMETU ZMLUVY

P.č.	Názov	Počet	Merná jednotka	Cena za mernú jednotku bez DPH	Cena spolu bez DPH
	Stí. č. 1	Stí. č. 2	Stí. č. 3	Stí. č. 4	Stí. č. 5
1.	**ČASŤ 1- Primárne dátové pripojenia**				
1.1	**ČASŤ 1.1 - Vytvorenie primárnych dátových pripojení siete SocPoist**				
1.1.1	**Zriadenie primárnych dátových pripojení siete SocPoist na lokalitách podľa Prílohy č. 1 č. 2 B zmluvy - jednorázový poplatok**	1	**jednorázový polatok**	2 022 800,00	2 022 800,00 €
	Dátové pripojenie pracovísk SocPoist - mesačný poplatok				
1.1.2	- Typ 1	2	ks	3 450,00	662 400,00 €
1.1.3	- Typ 2	3	ks	2 360,00	679 680,00 €
1.1.4	- Typ 3	11	ks	967,00	1 021 152,00 €
1.1.5	- Typ 4	22	ks	655,00	1 383 360,00 €
1.1.6	- Typ 5	13	ks	545,00	680 160,00 €
1.1.7	- Typ 6	44	ks	545,00	2 302 080,00 €
1.1.8	**Zriadenie VPS / SD-WAN siete - jednorázový poplatok**	1	ks	1 498 320,00	1 498 320,00 €
1.1.9	**Prevádzka a správa VPS / SD-WAN siete - mesačný poplatok**	1	ks	135 469,00	13 005 024,00 €
	Spolu za časť 1.1				**23 254 976,00 €**
1.2	**ČASŤ 1.2 - Doplnkové služby**				
	Expertné práce - platené jednorázovo na objednávku				
1.2.1	- Inštalačné práce (inštalácia softw are/firmw are na aktívne sieťové prvky LAN a WAN siete, inštalácia a montáž aktívnych a pasívnych sieťových prvkov LAN a WAN siete ako router, sw itch, firew all a pod.)	2672	človekohodina	50,00	133 600,00 €
1.2.2	- Servisné práce (údržba a čistenie aktívnych a pasívnych sieťových prvkov LAN a WAN siete, servis a údržba existujúcej štruktúrovanej kabeláže v rámci serverovní a rackov)	4328	človekohodina	50,00	216 400,00 €
1.2.3	- Konfiguračné práce (konfigurácia aktívnych a pasívnych sieťových prvkov LAN a WAN siete ako router, sw itch, firew all a pod.)	2816	človekohodina	60,00	168 960,00 €
1.2.4	- Bezpečnostné práce (konfigurácia bezpečnostných nastavení na aktívnych a sieťových prvkov LAN a WAN siete ako router, sw itch, firew all a pod.)	1552	človekohodina	60,00	93 120,00 €
	Spolu za časť 1.2				**612 080,00 €**
	Spolu za časť 1.1 a 1.2				**23 867 056,00 €**
1.3	**Navýšenia/zriadenia nových liniek**				
	Navýšenia rýchosti pripojenia - mesačný poplatok				
1.3.1	- Navýšenie pripojenia typ 1 o 1000Mbit/s	2	ks	2 254,00	4 508,00 €
1.3.2	- Navýšenie pripojenia typ 2 o 100Mbit/s	3	ks	1 054,00	3 162,00 €
1.3.3	- Navýšenie pripojenia typ 3 o 50Mbit/s	3	ks	645,00	1 935,00 €
1.3.4	- Navýšenie pripojenia typ 4 o 20Mbit/s	7	ks	480,00	3 360,00 €
1.3.5	- Navýšenie pripojenia typ 5 o 10Mbit/s	4	ks	350,00	1 400,00 €
1.3.6	- Navýšenie pripojenia typ 6 o 10Mbit/s	1	ks	350,00	350,00 €
	Zriadenie pripojenia - jednorázový poplatok				
1.3.7	- Zriadenie nového pripojenia typ 1	1	ks	199,00	199,00 €
1.3.8	- Zriadenie nového pripojenia typ 2	3	ks	199,00	597,00 €
1.3.9	- Zriadenie nového pripojenia typ 3	3	ks	199,00	597,00 €
1.3.10	- Zriadenie nového pripojenia typ 4	3	ks	199,00	597,00 €
1.3.11	- Zriadenie nového pripojenia typ 5	3	ks	199,00	597,00 €
1.3.12	- Zriadenie nového pripojenia typ 6	3	ks	199,00	597,00 €
	Cena spolu za časť č. 1 predmetu zákazky "Primárne linky a integračné služby"				**23 884 955,00 €**

Časť B: Zoznam prípojných bodov a špecifikácia predpokladaného množstva expertných prác v jednotlivých lokalitách

Lokalita	Minimálna požadovaná rýchlosť v Mbps upload/download	Minimálna požadovaná Backup linka v Mbps upload/download	Počet zariadení (PC, IP phones, ...)	Minimálny počet portov LAN na core prepínači	Minimálny počet portov uplink na core prepínači	SLA	Minimálna úroveň typu pripojenia	Mesto	Adresa	Inštalačné práce (človeko-hodiny)	Servisné práce (človeko hodiny)	Konfiguračné práce (človeko-hodiny)	Bezpečnostné práce (človeko-hodiny)
BA 29. augusta	10000/10000	10000/10000	1700	2x24	2x4	A	Typ-1	Bratislava	ul.29. augusta 8 a 10	64	160	120	160
BA, DC SOCPOIST záloha, BA, Nevädzova 8	10000/10000	10000/10000	-	2x24	2x4	A	Typ-1	Bratislava	Nevädzova 8 (nová serverovňa)	64	120	64	80
BA Nevädzova 8	1000/1000	300/300	400	2x24	2x4	A	Typ-2	Bratislava	Nevädzova 8	64	120	64	80
BA Záhradnícka 31	1000/1000	300/300	400	2x24	2x4	A	Typ-2	Bratislava	Záhradnícka 31	64	120	64	80
BA - Záhradnícka 153	1000/1000	300/300	400	2x24	2x4	A	Typ-2	Bratislava	Záhradnícka 153	64	120	64	80
Košice	300/300	100/100	200	2x24	2x4	A	Typ-3	Košice	Festivalové nám. 1	32	64	40	24
Trnava	300/300	100/100	200	2x24	2x4	A	Typ-3	Trnava	Vladimíra Clementisa 24/A	32	64	40	24
Žilina	300/300	100/100	200	2x24	2x4	A	Typ-3	Žilina	Antona Bernoláka 53	32	64	40	24
Senica	300/300	100/100	200	2x24	2x4	A	Typ-3	Senica	Hollého 1219	32	64	40	24
Banská Bystrica	300/300	100/100	200	2x24	2x4	A	Typ-3	Banská Bystrica	Kapitulská 27	32	64	40	24
Nitra	300/300	100/100	200	2x24	2x4	A	Typ-3	Nitra	Slančíkovej 3	32	64	40	24
Prešov	300/300	100/100	200	2x24	2x4	A	Typ-3	Prešov	Masarykova 1	32	64	40	24
Trenčín	300/300	100/100	200	2x24	2x4	A	Typ-3	Trenčín	Jilemnického 3760	32	64	40	24
Považská Bystrica	300/300	100/100	200	2x24	2x4	A	Typ-3	Považská Bystrica	Kukučínova 208/23	32	64	40	24
Poprad	300/300	100/100	200	2x24	2x4	A	Typ-3	Poprad	Ul. 1. mája 4053/24	32	64	40	24
Topoľčany	300/300	100/100	200	2x24	2x4	A	Typ-3	Topoľčany	Nám. M.R.Štefánika 2269/18	32	64	40	24
Prievidza	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Prievidza	Matice slovenskej 10	32	48	32	16
Galanta	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Galanta	Z. Kodálya 1629/48	32	48	32	16

Spišská Nová Ves	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Spišská Nová Ves	Elektrárenská 10	32	48	32	16
Liptovský Mikuláš	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Liptovský Mikuláš	Štúrova 34	32	48	32	16
Čadca	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Čadca	Štúrova 2	32	48	32	16
Nové Zámky	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Nové Zámky	Gy. Széchényiho 10	32	48	32	16
Humenné	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Humenné	Námestie slobody 5672/58	32	48	32	16
Dolný Kubín	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Dolný Kubín	Aleja Slobody 1878	32	48	32	16
Zvolen	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Zvolen	Š. Moyzesa 1369/ 52	32	48	32	16
Dunajská Streda	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Dunajská Streda	Galantská cesta 693	32	48	32	16
Levice	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Levice	Sv. Michala 4	32	48	32	16
Martin	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Martin	nám. SNP 4	32	48	32	16
Michalovce	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Michalovce	Námestie osloboditeľov 81	32	48	32	16
Komárno	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Komárno	Petöfiho 7	32	48	32	16
Žiar n/Hronom	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Žiar nad Hronom	Sládkovičova 17	32	48	32	16
Rimavská Sobota	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Rimavská Sobota	K.Mikszátha 6	32	48	32	16
Lučenec	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Lučenec	Dr.Vodu 6	32	48	32	16
Bardejov	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Bardejov	Hurbanova 6	32	48	32	16
Vranov nad Topľou	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Vranov nad Topľou	Rázusová 128	32	48	32	16
Stará Ľubovňa	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Stará Ľubovňa	Budovateľská 42/535	32	48	32	16
Trebišov	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Trebišov	M. R. Štefánika 178	32	48	32	16
Rožňava	200/200	50/50	do 150	2x24	2x4	A	Typ-4	Rožňava	Štítnická 12	32	48	32	16
Svidník	100/100	50/5	50	24x	4x	A	Typ-5	Svidník	Sov. Hrdinov 121	32	40	32	8
Senec	100/100	50/5	50	24x	4x	A	Typ-5	Senec	Brezová 2	32	40	32	8
Malacky	100/100	50/5	50	24x	4x	A	Typ-5	Malacky	Bernolákova 1/A	32	40	32	8
Senica VP	100/100	50/5	50	24x	4x	A	Typ-5	Senica	Sotinská 1577	32	40	32	8
Pezinok	100/100	50/5	50	24x	4x	A	Typ-5	Pezinok	Radničné námestie 9	32	40	32	8
Veľký Krtíš	100/100	50/5	50	24x	4x	A	Typ-5	Veľký Krtíš	SNP 28	32	40	32	8
Brezno	100/100	50/5	50	24x	4x	A	Typ-5	Brezno	Ul. Boženy Němcovej 4	32	40	32	8
BA - Hagarova	100/100	50/5	50	24x	4x	A	Typ-5	Bratislava	Jozefa Hagaru 9	32	40	32	8
BA - Kutlíková	100/100	50/5	50	24x	4x	A	Typ-5	Bratislava	Kutlíkova 1755/17	32	40	32	8

BA - Karlovka	100/100	50/5	50	24x	4x	A	Typ-5	Bratislava	Nam. Sv. Frantiska 8/A	32	40	32	8
BA Lazaretská	100/100	50/5	50	24x	4x	A	Typ-5	Bratislava	Lazaretská 25	32	40	32	8
Staré Hory	100/100	50/5	50	24x	4x	A	Typ-5	Staré Hory	Staré Hory 24	32	40	32	8
Pavčina Lehota	100/100	50/5	50	24x	4x	A	Typ-5	Pavčina Lehota	Pavčina Lehota 111	32	40	32	8
Ružomberok	50/50	30/3	20	24x	4x	A	Typ-6	Ružomberok	Podhora 9	20	32	20	8
Námestovo - VP	50/50	30/3	20	24x	4x	A	Typ-6	Námestovo	Hviezdoslavovo nám. č. 213	20	32	20	8
Čadca - VP	50/50	30/3	20	24x	4x	A	Typ-6	Čadca	Ul. Fraňa Kráľa	20	32	20	8
Dolný Kubín - VP	50/50	30/3	20	24x	4x	A	Typ-6	Dolný Kubín	Aleja Slobody 2203	20	32	20	8
Piešťany	50/50	30/3	20	24x	4x	A	Typ-6	Piešťany	Sládkovičova 2069/10A	20	32	20	8
Zvolen - VP	50/50	30/3	20	24x	4x	A	Typ-6	Zvolen	Námestie SNP č. 35/48	20	32	20	8
Zlaté Moravce	50/50	30/3	20	24x	4x	A	Typ-6	Zlaté Moravce	Sládkovičova 3	20	32	20	8
Nové M/V	50/50	30/3	20	24x	4x	A	Typ-6	Nové Mesto nad Váhom	Hviezdoslavova ul. č. 36	20	32	20	8
Dubnica n/V	50/50	30/3	20	24x	4x	A	Typ-6	Dubnica nad Váhom	Bratislavská ulica č. 4051/40	20	32	20	8
Púchov	50/50	30/3	20	24x	4x	A	Typ-6	Púchov	Royova 1048	20	32	20	8
Hlohovec	50/50	30/3	20	24x	4x	A	Typ-6	Hlohovec	Jarmočná 3	20	32	20	8
Tvrdošín	50/50	30/3	20	24x	4x	A	Typ-6	Tvrdošín	Medvedzie 132	20	32	20	8
Kežmarok	50/50	30/3	20	24x	4x	A	Typ-6	Kežmarok	Mučeníkov 4	20	32	20	8
Myjava	50/50	30/3	20	24x	4x	A	Typ-6	Myjava	M. R. Štefánika 561/6	20	32	20	8
Galanta - VP	50/50	30/3	20	24x	4x	A	Typ-6	Galanta	Mierové námestie 940	20	32	20	8
Šaľa	50/50	30/3	20	24x	4x	A	Typ-6	Šaľa	Dolná ulica 524/1	20	32	20	8
Sabinov	50/50	30/3	20	24x	4x	A	Typ-6	Sabinov	Námestie slobody 87	20	32	20	8
Snina	50/50	30/3	20	24x	4x	A	Typ-6	Snina	Partizánska 1057	20	32	20	8
Holíč	50/50	30/3	20	24x	4x	A	Typ-6	Holíč	Námestie sv. Martina 1716/9	20	32	20	8
Gelnica	50/50	30/3	20	24x	4x	A	Typ-6	Gelnica	Hlavná 1	20	32	20	8
Kysucké N.Mesto	50/50	30/3	20	24x	4x	A	Typ-6	Kysucké N. Mesto	Belanského ul. 1345	20	32	20	8
Bytča	50/50	30/3	20	24x	4x	A	Typ-6	Bytča	M. Rázusa 749/5	20	32	20	8
Banská Bystrica - VP	50/50	30/3	20	24x	4x	A	Typ-6	Banská Bystrica	Trieda SNP 75	20	32	20	8
Revúca	50/50	30/3	20	24x	4x	A	Typ-6	Revúca	Komenského 40	20	32	20	8
Sereď	50/50	30/3	20	24x	4x	A	Typ-6	Sereď	Mlynárska 83/17	20	32	20	8
Kráľovský Chlmec	50/50	30/3	20	24x	4x	A	Typ-6	Kráľovský	Hlavná 68	20	32	20	8

								Chlmec					
Levoča	50/50	30/3	20	24x	4x	A	Typ-6	Levoča	nám. Majstra Pavla 59	20	32	20	8
Detva	50/50	30/3	20	24x	4x	A	Typ-6	Detva	Záhradná ulica č. 5	20	32	20	8
Giraltovce	50/50	30/3	20	24x	4x	A	Typ-6	Giraltovce	Hviezdoslavova 3	20	32	20	8
Banská Štiavnica	50/50	30/3	20	24x	4x	A	Typ-6	Banská Štiavnica	Križovatka 4	20	32	20	8
Žarnovica	50/50	30/3	20	24x	4x	A	Typ-6	Žarnovica	Bystrická 53	20	32	20	8
Partizánske	50/50	30/3	20	24x	4x	A	Typ-6	Partizánske	Nám. SNP 151/6	20	32	20	8
Stropkov	50/50	30/3	20	24x	4x	A	Typ-6	Stropkov	Hlavná 26	20	32	20	8
Bánovce n/Bebravou	50/50	30/3	20	24x	4x	A	Typ-6	Bánovce nad Bebravou	Sládkovičova 60/6	20	32	20	8
Krupina	50/50	30/3	20	24x	4x	A	Typ-6	Krupina	Kuzmányho 2191/4	20	32	20	8
Krompachy	50/50	30/3	20	24x	4x	A	Typ-6	Krompachy	Kúpeľná 9	20	32	20	8
Sobrance	50/50	30/3	20	24x	4x	A	Typ-6	Sobrance	Michalovská 2	20	32	20	8
Veľké Kapušany	50/50	30/3	20	24x	4x	A	Typ-6	Veľké Kapušany	L. N. Tolstého 1	20	32	20	8
Medzilaborce	50/50	30/3	20	24x	4x	A	Typ-6	Medzilaborce	Mierová 326/4	20	32	20	8
BA - Tomášikova	50/50	30/3	20	24x	4x	A	Typ-6	Bratislava	Tomášikova 43	20	32	20	8
Šahy	50/50	30/3	20	24x	4x	A	Typ-6	Šahy	Hlavné námestie 1	20	32	20	8
Moldava n/Bodvou	50/50	30/3	20	24x	4x	A	Typ-6	Moldava nad Bodvou	Ul. ČSA 13	20	32	20	8
Štúrovo	50/50	30/3	20	24x	4x	A	Typ-6	Štúrovo	Jesenského 85	20	32	20	8
Šamorín	50/50	30/3	20	24x	4x	A	Typ-6	Šamorín	Bratislavská 82/35	20	32	20	8
Expertné práce spolu										2672	4328	2816	1552
Vysvetlivky: SLA –A(ÁNO), N(NIE)													

Tabuľka rozdelenia hlavnej linky typ 1 na adrese Ul. 29 Augusta, Bratislava

Rozdelenie pripojenia

Pripojenie	**Sieť MPLS**	**Internet**
Primárna linka	5 000 Mbps	5 000 Mbps

Príloha č.3 k zmluve č. 12929-22/2023-BA o poskytovaní služieb

Vzor objednávky služby

Evidenčné číslo Objednávky:	

☐ zriadenie ☐ zrušenie ☐ preloženie ☐ zmena parametrov

Požadovaný dátum realizácie:		**Na min. obdobie:**	☐ trvania rámcovej zmluvy	☐ iné:

ÚČASTNÍK			
Obchodné meno (alebo priezvisko, meno, titul): **Sociálna poisťovňa, ústredie**			
IČO: 30807484	DIČ: 2020592332	IČ DPH: SK2020592332	
Ulica: 29. augusta	Orient. č.: 8/10	Obec (sídlo): Bratislava I.	PSČ: 813 63

Zodpovedná osoba účastníka pre veci zmluvné (priezvisko, meno, titul):			Prac. pozícia:
Telefón:	Fax:	Mobil:	E-mail:
Kontaktná osoba účatníka pre veci technické (priezvisko, meno titul):			Prac. pozícia:
Telefón**:**	Fax:	Mobil:	E-mail:

CENA SPOLU (EUR bez DPH	Jednorazový poplatok:	Mesačný poplatok
Elektronická faktúra:	**Áno**	e-mailová adresa pre zasielanie elektronickej faktúry: faktury@socpoist.sk

Ďalšie údaje o koncovom bode Účastníka			
Miesto pripojenia :		Obec:	
Ulica:	Orientačné číslo:	Súpisné číslo:	PSČ:
Kontakt (meno) :	Kontakt (tel./mob.):	Poschodie:	Miestnosť č.:
Pripojené koncové zariadenia – druh:			

Ak vnútorné vedenie v objekte je vybudované		Účastník zabezpečí súhlas s využitím vnútorného telekomunikačného vedenia u vlastníka, resp. správcu vnútorných rozvodov. V prípade nesúhlasu vlastníka, resp. správcu vnútorných rozvodov sa postupuje, ako keby vedenie nebolo vybudované.
Ak vnútorné vedenie v objekte nie je vybudované	☐	Účastník požaduje vnútorné vedenie v objekte vybudovať ako súčasť zriaďovaného telekomunikačného okruhu a zabezpečí súhlas vlastníka, resp. správcu nehnuteľnosti s inštaláciou v objekte a technickú dokumentáciu existujúcich vnútorných rozvodov.
	☐	Účastník zabezpečí vybudovanie vnútorného vedenia podľa požiadaviek operátora

Dátum:	Dátum:	Dátum:
Meno a priezv..:	Meno a priezv.:	Meno a priezv.:
podpis a pečiatka účastníka	podpis a pečiatka obchodného zástupcu	podpis a pečiatka poskytovateľa

Príloha č.4 k zmluve č. 12929-22/2023-BA o poskytovaní služieb

Vzor preberacieho protokolu

Podnik:

PREBERACÍ PROTOKOL

o prevzatí nainštalovaných zariadení

Účastník (preberajúci):		
Podnik (odovzdávajúci):		
Objednávka č.:		

Preberajúci týmto potvrdzuje prevzatie naištalovaného tovaru:

Zariadenie (typové označenie)	Sériové číslo	Miestnosť

Dátum prevzatia:

Zástupca odovzdávajúceho:	Zástupca preberajúceho:
Meno a priezvisko:	Meno a priezvisko:
Pečiatka, podpis	Pečiatka, podpis

Poznámka:

Príloha č.5 k zmluve č. 12929-22/2023-BA o poskytovaní služieb

Poriadok a kvalita poskytovania služby SLA

Podnik sa zaväzuje poskytovať Účastníkovi elektronickú komunikačnú službu s dodržiavaním hodnôt prevádzkových parametrov SLA. Podnik sa touto prílohou zaväzuje poskytovať dohodnutú úroveň SLA.

Vymedzenie pojmov

a) „**Doba zriadenia**“ je garantovaná doba, od prijatia Objednávky na zriadenie Služby na obchodnom mieste spoločnosti Podniku, po odovzdanie Služby a potvrdenie Odovzdávacieho protokolu Účastníkovi.
b) „**Minimálny čas testovania**“ je minimálna doba na testovanie všetkých technických prostriedkov a prenosového prostredia na riadne poskytovanie Služby z hľadiska technologických a technických parametrov.
c) „**Obdobie**“ je doba, počas ktorej Podnik zodpovedá za dodržiavanie dohodnutých parametrov Služby. Obdobie je vždy jeden kalendárny mesiac.
d) „**Porucha**“ je taký stav Služby, ktorý znemožňuje Účastníkovi riadne používanie Služby v rozsahu a kvalite stanovenej v technických podmienkach, alebo keď jeden prípadne viac technických parametrov nedosahuje úroveň uvedenú v Zmluve, resp. v jej prílohách, alebo úroveň podľa odporúčaní ITU-T.
e) „**Doba odstránenia poruchy – fix time**“ (ďalej len DOP) je doba opravy poruchy vyjadrená v minútach a počíta sa, ako doba medzi nahlásením poruchy Účastníkom operátorovi Helpdesku Podniku a okamihom obnovenia prevádzky, potvrdeným Účastníkom.
f) „**Dostupnosť služby**“ (ďalej len DS) je garantovaná dostupnosť Služby, vyjadrená ako podiel času, počas ktorého môže Účastník využívať Službu v dohodnutom rozsahu, kvalite a Obdobím. Výsledná hodnota DS je vyjadrená v percentách a zaokrúhlená na jedno desatinné miesto smerom nahor.
g) „**Reakčný čas podpory**“ je maximálna doba od telefonického nahlásenia *poruchy* Účastníkom resp. formou SMS z monitorovacieho systému Účastníka, po telefonické potvrdenie odôvodnenosti resp. neodôvodnenosti hlásenia *poruchy* zo strany Podniku. V prípade odôvodnenosti informuje Podnik Účastníka o predpokladanej príčine poruchy, predpokladanom čase jej odstránenia a požiadavkách na prípadné poskytnutie súčinnosti pri lokalizácii a odstraňovaní *poruchy*.
h) „**Operátor Helpdesku** Podniku“ je kontaktná osoba Podniku na nahlasovanie poruchových stavov a poskytovanie informácií o ich riešení.
i) **„Hepldesk“** je súbor služieb a procesov, ktoré zabezpečujú centrálny príjem požiadaviek a porúch, ktoré vznesie Účastník alebo užívatelia služby. Helpdesk súčasne zabezpečuje schvaľovacie procesy, evidencie riešenia jednotlivých prípadov a procesy zabezpečenia riešenia problémov.
j) „**Zaznamenaná hodnota**“ je hodnota, ktorá je nameraná / vypočítaná v informačných systémoch Podniku .
k) „***SLA***“ (Service Level Agreement) je Dohodnutá úroveň poskytovanej služby.
l) „**Chrbticová sieť**“ je Sieť zabezpečujúca prenos IP paketov, pozostávajúca výlučne z vybraných uzlov siete v ktorých Podnik má? nainštalované zariadenia na meranie parametrov siete. Súčasťou chrbticovej siete sú aj prepojenia medzi týmito uzlami.
m) „**Výpadok služby**“ je situácia v ktorej koncový bod siete Podniku umiestnený v lokalite Účastníka nemôže z chrbticovej siete prijímať alebo do nej posielať pakety.
n) „**Oneskorenie**“ je priemerný čas potrebný na prenesenie paketu z jedného koncového bodu siete Podniku umiestneného v lokalite Účastníka do referenčného bodu merania umiestneného v SIXe a späť, meraný počas dohodnutej doby merania a v stave, kedy je služba vymedzená len pre účely merania.
o) „**Stratovosť**“ je priemerný počet paketov (vyjadrený v percentách) poslaných od jedného koncového bodu siete Podniku umiestneného v lokalite Účastníka do referenčného bodu merania umiestneného v SIXe, počas dohodnutej doby merania, ktoré podľa merania neboli úspešne doručené. Počas merania musí byť služba vymedzená len pre účely merania.
p) „**Variácia oneskorenia** (jitter)“ je priemerná variácia oneskorenia medzi koncovým bodom siete Podniku umiestneného v lokalite Účastníka a referenčným bodom umiestneným v SIXe meraná počas dohodnutej doby merania. Počas merania musí byť služba vymedzená len pre účely merania.

Určenie základných parametrov SLA

Výpočet dostupnosti služby (primerane sa vzťahuje aj na ostatné SLA parametre)

a) Dostupnosť služby (DS) je vyjadrená v % a vypočíta sa podľa vzorca:

$$dostupnosť\ služby = \frac{(T_S - T_N)}{(T_S)} \times 100\,\%$$

kde T_S – čas prevádzky služby (okruhu) za fakturačné obdobie

T_N – čas nedostupnosti služby (okruhu) za fakturačné obdobie

b) do T_N sa nezapočítava:
- o výpadok elektrickej energie v mieste prevádzkovania služby
- o živelné pohromy v mieste prevádzkovania služby a iné okolnosti spôsobené vyššou mocou
- o krádež alebo násilné poškodenie techniky Podniku umiestnených v lokalite Účastníka, nevyhnutnej na poskytovanie služby
- o totálne softvérové poškodenie na zariadeniach Podniku umiestnených v lokalite Účastníka, potrebných k poskytovaniu služby, zavinené úmyselne alebo z nedbanlivosti Účastníkom alebo tretími stranami
- o nefunkčnosť sieťovej infraštruktúry za ktorú nenesie zodpovednosť Podnik umiestneným v lokalite Účastníka
- o doba ohlásených plánovaných prác
- o doba ohlásených neplánovaných prác
- o doba merania
- o dočasné prerušenie poskytovania služby na žiadosť Účastníka
- o dočasné prerušenie poskytovania služby z dôvodu zmeny prevádzkových parametrov služby na žiadosť Účastníka (zmena rýchlosti a pod.), z dôvodu prekládky koncového bodu na žiadosť Účastníka a pod.
- o prerušenie spôsobené nevhodným používaním zariadení Podniku zo strany Účastníka alebo ich odpojením
- o neposkytnutie nevyhnutnej súčinnosti Podniku pri odstraňovaní Poruchy, a najmä neumožnenie prístupu servisných pracovníkov Podniku alebo poverených pracovníkov Podniku k zariadeniu/zariadeniam a káblovým trasám inštalovaným u Účastníka, nebude sa čas od príchodu pracovníkov Podniku po umožnenie prístupu k zariadeniu/zariadeniam a káblovým trasám (neobmedzený prístup do priestorov, kde sú umiestnené technické prostriedky Podniku potrebné na poskytovanie služby)
- o zapríčinené nefunkčnosťou (aj opakujúcou sa) koncových zariadení, ktoré sú majetkom Účastníka.

Časy sa počítajú na celé minúty, dostupnosť sa vyjadruje v % zaokrúhlene na jedno desatinné miesto smerom nahor.

Prevádzka a kvalita poskytovanej služby SLA

Služby sú poskytované nepretržite v režime 24x7x365 vrátane prevádzkovej podpory, služieb Helpdesk a vrátane monitoringu služieb s možnosťou okamžitého prehľadu o stave pripojenia. Riešenie poruchových stavov je v zmysle príslušnej SLA a v súčinnosti so zodpovedajúcimi zložkami objednávateľa/účastníka.
Pre zriadenie, alebo zmenu služby poskytuje zhotoviteľ nasledovné minimálne parametre:

Parameter	**Hodnota**
Doba potvrdenia objednávky	do 5 pracovných dní
Doba zriadenia služby	do 30 pracovných dní
Minimálny čas testovania služby	1 hodina

Podpora QoS a CoS
Služba IPT a iné poskytované služby vyžadujúce QoS ku svojej funkcionalite sú uprednostnené pred ostatným dátovým tokom a potrebné aktívne prvky sú prevádzkované s nastaveným QoS.
Podnik umožňuje Účastníkovi pri poskytovaní SD-WAN používanie technológie Quality of Service a technológie Class of Service.

Meranie/Monitoring

a) Meranie/Monitoring Dostupnosti služby
Podnik vykonáva pravidelné merania Dostupnosti služby za Obdobie/Monitoring. Účastník má taktiež právo na meranie Dostupnosti služby. V prípade nezhody vo výsledkoch merania vykoná Podnik a Účastník porovnanie nameraných hodnôt, prešetrí všetky zaznamenané hodnoty (odpočíta nezapočítavané hodnoty uvedené vyššie)) a opätovne vykoná výpočet Dostupnosti služby.

b) Meranie Oneskorenia, Stratovosti, Variácie oneskorenia
Meranie sa vykonáva medzi zariadením Podniku umiestneného v lokalite Účastníka a referenčným bodom umiestneného v SIXe. Meranie sa vykonáva vždy v prípade, kedy je služba určená výlučne na Meranie. Účastník má taktiež právo na meranie. V prípade nezhody vo výsledku merania sa meranie vykoná opätovne. Doba merania závisí od individuálnej dohody s Účastníkom.

Postup Účastníka pre nahlásenie a odhlásenie Poruchy, Výpadku, zmenovej požiadavky

a) Miestom na nepretržité (24 hodín denne, 7 dní v týždni, 52 týždňov v roku) nahlasovanie porúch a zmenových požiadaviek na poskytovaných službách Operátorovi Helpdesku Podniku:
- telefónne číslo [redacted]
- mobil
- e-mail

b) Nahlásenie poruchy, zmenovej požiadavky

Telefonické, písomné/email/ nahlásenie Operátorovi Helpdesku Podniku musí obsahovať:
- meno a funkciu osoby nahlasujúcej poruchu
- kontaktné telefónne číslo
- evidenčné číslo objednávky služby, resp. označenie služby podľa protokolu o odovzdaní
- čas vzniku poruchy/popis zmenovej požiadavky
- podrobný technický popis poruchy/požiadavky

Nahlasovanie poruchy formou SMS z monitorovacieho systému Účastníka na mobilné číslo Operátora Helpdesku musí obsahovať:
- kontaktné telefónne číslo
- evidenčné číslo objednávky služby, resp. označenie služby podľa protokolu o odovzdaní
- čas vzniku poruchy
- podrobný technický popis poruchy

Postup Podniku pri nahlasovaní Poruchy, Výpadku služby

Ohlasovanie poruchy

Pri nahlásení poruchy Operátorovi Helpdesku Podniku je tento Operátor povinný vytvoriť ticket, prideliť poruche evidenčné číslo a informuje o ňom Zodpovedného zástupcu Účastníka alebo Kontaktnú osobu, ktorý poruchu nahlasuje. Toto evidenčné číslo sa bude používať vo všetkých ďalších kontaktoch súvisiacich s danou poruchou a bude použité pri vypracovávaní písomnej správy o poruche.

Odstraňovanie poruchy/výpadku služby/vyriešenie zmenovej požiadavky

Zodpovedný zástupca Účastníka alebo Kontaktná osoba sa môže priebežne informovať o priebehu odstraňovania poruchy, a to formou telefonického rozhovoru s Operátorom Helpdesku Podniku alebo e-mailom Operátorovi Helpdesku Podniku.
Po odstránení poruchy/ zrealizovaní zmenovej požiadavky / Operátor Helpdesku Podniku oznámi telefonicky alebo aj e-mailom odstránenie poruchy/ informáciu ku zmenovej požiadavke zodpovednému zástupcovi Účastníka alebo Kontaktnej osobe Účastníka.
Podniku sa zaväzuje:

- začať činnosti potrebné na odstránenie poruchy/výpadku služby (Reakčný čas podpory) do 30 minút od nahlásenia poruchy
- Počas diagnostikovania poruchy/výpadok služby vynaložiť všetko úsilie na čo najskoršie obmedzenie vplyvu poruchy za účelom zabezpečenia aspoň minimálneho rozsahu služby až do jeho úplného obnovenia.

Reklamácie

Pre potreby reklamačného konania sú platné časy nahlásenia a odhlásenia poruchy Operátorovi Helpdesku Podniku v zmysle predchádzajúcich bodov podľa záznamov v dohľadovom systéme a Ticketing systéme spoločnosti SWAN, a.s.

Postup pre plánované a neplánované práce

a) V prípade plánovaného prerušenia služby/výpadku služby alebo vykonávania činností, ktoré môžu viesť k ich prerušeniu, je Podnik povinný písomne/emailom/faxom, resp. telefonicky oznámiť vykonávanie plánovanej práce Účastníkovi minimálne 3 (tri) pracovné dni vopred.
b) V prípade neplánovaného prerušenia služby/výpadku služby alebo vykonávania činností, ktoré môžu viesť k ich prerušeniu, je Podnik povinný písomne/emailom, resp. telefonicky oznámiť vykonávanie plánovanej práce Účastníkovi minimálne 1 (jeden) pracovný deň vopred.
c) Zákazník je povinný príjem informácie obratom potvrdiť emailom na adresu [redacted], prípadne počas telefonického oznámenia na tel. číslo [redacted] **alebo** [redacted], pričom hovor je zaznamenávaný.
d) Účastník má právo žiadať zmenu času vykonania plánovaného a neplánovaného prerušenia služby/výpadku, ak by zmena zmenšila dopad plánovanej práce na poskytované služby a Podnik sa zaväzuje požiadavke vyhovieť, ak to bude v jeho možnostiach.
e) Podnik sa zaväzuje, že čas a postup plánovanej a neplánovanej práce bude voliť tak, aby v maximálnej miere znížil dopad na poskytované služby.

V prípade akejkoľvek zmeny je Podnik povinný túto zmenu prerokovať s Účastníkom rovnakým postupom, ako novú plánovanú prácu, pričom sa Účastník zaväzuje reagovať obratom, ak si to bude plánovaná práca vyžadovať. Objednávateľ je povinný dodržiavať a poskytnúť zoznam kontaktov jednotlivých uzlov a udržiavať jeho aktuálnosť.

Všeobecné podmienky

Podnik je oprávnený v nevyhnutnom rozsahu na nevyhnutný čas **prerušiť alebo obmedziť poskytovanie Služby** bez toho, aby sa to považovalo za akékoľvek porušenie zmluvy, a to z dôvodov

- poskytovania služieb pre orgány krízového riadenia a pre ostatných účastníkov zaradených do systému prednostného spojenia a prevádzku tiesňových volaní na postihnutom území pri mimoriadnych udalostiach a krízových situáciách
- rozhodnutia príslušného orgánu Slovenskej republiky, závažných organizačných, technických alebo prevádzkových dôvodov
- výkonu prác potrebných pre prevádzku, údržbu a opravu siete Poskytovateľa alebo prác potrebných v snahe vyhnúť sa chybám v tejto sieti.

Na tieto skutočnosti bude Podnik pokiaľ je to možné vopred, akýmkoľvek vhodným spôsobom informovať Účastníka o obmedzeniach, prerušeniach a výpadkoch poskytovania Služby s výnimkou stavu krízovej situácie a mimoriadnej udalosti, počas ktorých je splnenie tohto záväzku zo strany Podniku nemožné. Podnik nemá túto povinnosť v stave krízovej situácie a mimoriadnej udalosti, počas ktorých je splnenie tohto záväzku zo strany Podniku nemožné a v prípade výkonu prác potrebných pre zabezpečenie prevádzky, údržbu, opravu a modernizáciu Podniku , ak sú tieto práce vykonávané v dobe medzi 01:00 hod. až 05:00 hod. a jednotlivé súvislé prerušenie alebo obmedzenie poskytovania Služby neprekročí 15 minút.

Príloha č.6 k zmluve č. 12929-22/2023-BA o poskytovaní služieb

Zoznam expertov

Poradové číslo experta	Meno a priezvisko experta
Expert č. 1 – Expert v oblasti návrhu architektúry, implementácie a nasadenia telekomunikačných sietí a sietí VPN, SD-WAN	[redacted]
Expert č. 2 – Špecialista pre inštaláciu a konfiguráciu sieťových zariadení	[redacted]
Expert č. 3 – Špecialista pre bezpečnosť sieťových zariadení	[redacted]
Expert č. 4 – Špecialista technickej podpory pre sieťové zariadenia	[redacted]
Expert č. 5 – Projektový manažér	[redacted]

Príloha č.7 k zmluve č. 12929-22/2023-BA o poskytovaní služieb

Zoznam subdodávateľov

Obchodné meno uchádzača: SWAN, a.s.
Adresa/sídlo uchádzača: Landererova 12, 811 09 Bratislava
IČO uchádzača: 35 680 202

Na uskutočnení plnenia Zmluvy o poskytovaní služieb č. 12929-22/2023-BA

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

b) sa budú podieľať nasledovní subdodávatelia:*

P. č.	Meno a priezvisko alebo obchodné meno alebo názov subdodávateľa Adresa sídla alebo miesta podnikania	Identifikačné číslo alebo dátum narodenia, ak nebolo pridelené identifikačné číslo	Meno a priezvisko, adresa pobytu a dátum narodenia osoby oprávnenej konať za subdodávateľa	IČO	Podiel plnenia zmluvy v %	Predmet subdodávok
1.	**LYNX, s.r.o.**, Jelačičova 8A, 821 08 Bratislava	00692069	[redacted]	00692069	10%	Práce súvisiace s požiadavkami kladenými na expertov 1 až 5
2.	**Slovanet, a.s.,** Záhradnícka151, 821 08 Bratislava	35954612	[redacted]	35954612	16%	Práce súvisiace s implementáciou časti SD-WAN

3.	**Orange Slovensko**, **a.s**.. Metodova 8, 821 08 Bratislava	35697270	[redacted]	35697270	12%	Práce súvisiace s výstavbou siete WAN a LAN

V Bratislave, dňa .....

.

podpis : .....
meno : Ing. Juraj Ondriš
funkcia : predseda predstavenstva SWAN, a.s.

podpis : .....
meno : Ing. Miroslav Strečanský
funkcia : popredseda predstavenstva SWAN, a.s.

*Nehodiace sa prečiarknite

ZÁPIS
O ZMENE PRÍLOHY Č. X „ZOZNAM XXX“

k Zmluve o poskytovaní služieb č. 12929-22/2023-BA

uzatvorenej podľa § 84 a nasl.zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

(ďalej len „zmluva“) medzi:

podnikom **SWAN, a.s.**, Landererova 12, 811 09 Bratislava
IČO: 35 680 202
(ďalej len „Podnik“) a

účastníkom ***Sociálna poisťovňa**, Ul. 29. augusta 8 a 10, 813 63 Bratislava,*
IČO: 30807484 (ďalej len „Účastník“)

V súlade s čl. 11 bodom 11.X zmluvy, v ktorom sa zmluvné strany dohodli o spôsobe zmeny Prílohy č. X k zmluve „Zoznam XXX“, zmluvné strany v zastúpení ich oprávnenými zástupcami podpisujú tento zápis, ktorým sa mení Príloha č. X k zmluve „Zoznam XXX“, ktorá tvorí prílohu k tomuto zápisu.

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

.....

.....

.....

Tento zápis je neoddeliteľnou súčasťou zmluvy.

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

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

Za Podnik:	Za Účastníka:
....., dňa	Bratislava, dňa
.....	.....
oprávnená osoba	oprávnená osoba

Príloha:

Príloha č. X k zmluve „Zoznam XXX“

Príloha č.9 k zmluve č. 12929-22/2023-BA o poskytovaní služieb

Sprostredkovateľská zmluva č. 12929-24/2023-BA

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

Zmluvné strany

Prevádzkovateľ

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

(ďalej len „**prevádzkovateľ**“)

a

Sprostredkovateľ

Obchodné meno:	**SWAN, a.s.**
Sídlo:	Landererova 12, 811 09 Bratislava
Štatutárny orgán:	Ing. Juraj Ondriš, predseda predstavenstva Ing. Miroslav Strečanský, podpredseda predstavenstva
IČO:	35 680 202
DIČ:	2020324317
IČ DPH:	SK2020324317
Bankové spojenie:	[redacted]
IBAN:	

Zapísaný v Obchodnom registri Mestského súdu Bratislava III, oddiel Sa, vložka č. 2958/B.

(ďalej len „**sprostredkovateľ**“)

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

Preambula

Zmluvné strany spolu uzatvárajú Zmluvu č. 12929-22/2023-BA o poskytovaní služieb podľa § 84 a nasl. zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, predmetom ktorej je predovšetkým poskytovanie komplexných komunikačných služieb virtuálnej privátnej siete, časť 1: Primárne linky a integračné služby (ďalej len „zmluva o poskytovaní služieb“).

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

Článok I.

Vymedzenie pojmov

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

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

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

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

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

Čl. II
Predmet zmluvy

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

Čl. III
Zoznam osobných údajov a okruh dotknutých osôb

1. Zmluva, v rámci plnenia predmetu ktorej je sprostredkovateľ poverený spracúvať osobné údaje dotknutých osôb:

Zmluva č. 12929-22/2023-BA o poskytovaní služieb podľa § 84 a nasl. zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

2. Zoznam osobných údajov, ktoré môžu byť v prípade realizácie predmetu zmluvy o poskytovaní služieb predmetom spracúvania:
   - meno, priezvisko, titul, adresa bydliska, dátum narodenia, rodné číslo, číslo občianskeho preukazu
   - osobné údaje nevyhnutné na výkon úrazového poistenia
   - osobné údaje nevyhnutné na výkon garančného poistenia
   - osobné údaje nevyhnutné na výkon starobného dôchodkového sporenia
   - osobné údaje nevyhnutné na výkon lekárskej posudkovej činnosti
   - adresné, číslo bankového účtu
   - audiozáznam telefonického rozhovoru do IPC (inf. poradenské centrum)
   - mzdové náležitosti, miesto výkonu práce, pracovisko, údaje o odpracovanom čase, tel. číslo, e-mail, číslo bankového účtu FO,
   - identifikačné a kontaktné údaje
   - telefónne číslo, e-mail
3. Spracúvané osobné údaje sú typu:
   adresné, zamestnanecké, ekonomické, sociálne, elektronické,
   Iné osobné údaje v rozsahu bodu 2 tohto článku.

Čl. IV
Spôsob výkonu a oprávnenia sprostredkovateľa

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

Čl. V
Vyhlásenie prevádzkovateľa

1. Prevádzkovateľ vyhlasuje, že pri výbere sprostredkovateľa dbal na odbornú, technickú, organizačnú a personálnu spôsobilosť sprostredkovateľa a jeho schopnosť zaručiť ochranu práv dotknutých osôb.
2. Prevádzkovateľ prehlasuje, že
   a) osobné údaje sa spracúvajú na základe primeraného právneho dôvodu v súlade s GDPR a ZOOU,
   b) osobné údaje sa spracúvajú v súlade s jasne definovaným účelom spracúvania,
   c) osobné údaje, ktoré sprostredkovateľ spracúva na základe tejto zmluvy sú aktuálne, úplné a primerané vzhľadom na účel spracúvania.

Čl. VI
Vyhlásenie sprostredkovateľa

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

Čl. VII
Povinnosti sprostredkovateľa

1. Sprostredkovateľ sa pri spracúvaní osobných údajov podľa tejto zmluvy zaväzuje najmä:
   a) postupovať s náležitou starostlivosťou a v súlade s GDPR, ZOOU a súvisiacimi všeobecne záväznými právnymi predpismi Slovenskej republiky, dodržiavať povinnosti vyplývajúce z tejto zmluvy a pokynov prevádzkovateľa, a dodržiavať zásady ochrany osobných údajov zverejnené Prevádzkovateľom,
   b) akékoľvek spracúvanie osobných údajov vykonávať len za účelom plnenia predmetu tejto zmluvy a servisnej zmluvy a len v rozsahu nevyhnutnom na jej plnenie,
   c) údaje dotknutých osôb nezverejňovať, nešíriť či neodovzdávať ďalším osobám,
   d) zaistiť, aby jeho zamestnanci a ďalšie osoby, ktoré využije na plnenie podľa tejto zmluvy, dodržiavali podmienky stanovené GDPR, vnútroštátnymi predpismi a touto zmluvou a boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti,
   e) ak všeobecne záväzné právne predpisy neustanovujú inak, osobné údaje, s ktorými sa dostal do styku v súvislosti s realizáciou zmluvy o poskytovaní služieb nezverejňovať, neposkytovať a nesprístupňovať tretím stranám,
   f) zachovávať mlčanlivosť a zabezpečiť diskrétnosť pri akomkoľvek spracúvaní osobných údajov,
   g) ak zmluva alebo všeobecne záväzný právny predpis neustanovuje inak, nevyhotovovať kópie akýchkoľvek nosičov obsahujúcich osobné údaje a ani z nich nevyhotovovať výpisy alebo odpisy, ktoré by obsahovali osobné údaje,
   h) ak všeobecne záväzné právne predpisy upravujúce problematiku archívov a registratúr neustanovujú inak, bezodkladne odovzdávať prevádzkovateľovi všetky získané materiály obsahujúce osobné údaje, ktoré už pre realizáciu zmluvy nepotrebuje, resp. všetky osobné údaje, ktoré bude spracúvať v súvislosti s plnením zmluvy o poskytovaní služieb, bezodkladne po tom, čo pominie dôvod na ich spracúvanie podľa zmluvy, zmazať zo všetkých elektronických, hmotných alebo iných nosičov informácii (napr. pevné disky počítačov, USB kľúče, CD, DVD, dokumenty v papierovej podobe) alebo tieto nosiče zlikvidovať tak, aby nedošlo k úniku týchto údajov,
   i) poučiť svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby“), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných údajov, ako aj o iných právach a povinnostiach sprostredkovateľa upravených zmluvou alebo ustanovených všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov, o zodpovednosti za ich porušenie, a to všetko pred uskutočnením prvej operácie s osobnými údajmi,
   j) zachovávať mlčanlivosť o osobných údajoch dotknutých osôb a o bezpečnostných opatreniach prijatých na zabezpečenie ochrany osobných údajov, a to aj po skončení tohto zmluvného vzťahu,
   k) je povinný nakladať s údajmi ako s informáciami dôvernými v zmysle Zákona 513/1991 Zb. (Obchodný zákonník) a jeho následných novelizácií a je povinný zaviazať týmito povinnosťami aj osoby, ktoré by dojednal na činnosti na plnenie podľa tejto zmluvy (zamestnancov či iných pracovníkov),
   l) plniť predmet zmluvy len prostredníctvom riadne a preukázateľne poučených alebo vyškolených oprávnených osôb pre účel plnenia predmetu zmluvy a z nej vyplývajúceho rozsahu a podmienok spracúvania osobných údajov,

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

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

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

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

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

zaisťovaní plnenia jeho povinností pri prevencii rizík a ďalších povinností Prevádzkovateľa podľa ustanovení čl. 32 – 36 GDPR. K vyžiadaniu Prevádzkovateľa je mu nápomocný technickými a organizačnými prostriedkami pri plnení povinností Prevádzkovateľa reagovať na žiadosti o výkon práv Dotknutej osoby stanovených v kapitole III. GDPR (informácie a prístup k osobným údajom, oprava a výmaz, právo na obmedzenie spracovania atď.)

9. Sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na doloženie toho, že boli splnené povinnosti sprostredkovateľa a stanovené ustanoveniami GDPR a umožní audity, vrátane inšpekcií, vykonávané prevádzkovateľom alebo iným audítorom, ktorého prevádzkovateľ poveril. Pri vykonávaní auditov bude spolupracovať s prevádzkovateľom alebo ním určeným audítorom. Prevádzkovateľ je oprávnený vykonať inšpekciu plnenia povinností sprostredkovateľa a audit bez predchádzajúceho upozornenia. Nespolupráca sprostredkovateľa bude považovaná za podstatné porušenie tejto Zmluvy s možnosťou odstúpenia zo strany prevádzkovateľa, resp. vyvodením zodpovednosti za prípadnú škodu.

10. Po ukončení poskytovania služieb spojených so spracovaním sprostredkovateľ v súlade s rozhodnutím prevádzkovateľa všetky osobné údaje buď vymaže, alebo ich vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo členského štátu nepožaduje uloženie daných osobných údajov. Dojednáva sa, že takýto pokyn bude sprostredkovateľovi daný písomne.

11. Ak sprostredkovateľ poruší GDPR a túto zmluvu tým, že bez pokynu prevádzkovateľa sám určí účely a prostriedky spracovania osobných údajov, stane sa vo vzťahu k týmto údajom a ich spracovaniu prevádzkovateľom so všetkými dôsledkami z toho vyplývajúcimi.

Čl. VIII
Podmienky spracúvania osobných údajov

1. Sprostredkovateľ vyhlasuje, že spracúvanie osobných údajov bude vykonávať sám, a zároveň prostredníctvom iných osôb (ďalej len „subdodávateľ“), ktorými sú spoločnosti LYNX, s.r.o., sídlo: Jelačičova 8A, 821 08 Bratislava, IČO: 00 692 069, Slovanet, a.s., sídlo: Záhradnícka 151, 821 08 Bratislava, IČO: 35 954 612, Orange Slovensko, a.s., sídlo: Metodova 8, 821 08 Bratislava, IČO: 35 697 270, Prevádzkovateľ so spracúvaním osobných údajov uvedenými subdodávateľmi súhlasí. Subdodávatelia budú spracúvať osobné údaje na zodpovednosť sprostredkovateľa v rozsahu a za podmienok stanovených v tejto zmluve.

2. Sprostredkovateľ nezapojí do spracovania žiadneho ďalšieho sprostredkovateľa bez predchádzajúceho konkrétneho písomného súhlasu prevádzkovateľa. Náležitosti žiadosti o poskytnutie súhlasu sú uvedené v bode 4 tohto článku zmluvy.

3. Sprostredkovateľ nesmie zveriť spracúvanie osobných údajov subdodávateľovi, ak by tým mohli byť ohrozené práva a právom chránené záujmy dotknutých osôb. Pri zapojení ďalšieho sprostredkovateľa do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa je mu sprostredkovateľ povinný uložiť rovnaké povinnosti týkajúce sa ochrany osobných údajov, ako má on sám.

4. Žiadosť o poskytnutie súhlasu musí obsahovať aspoň nasledovné náležitosti:
   a. označenie subdodávateľa obchodným menom, identifikačnými údajmi a zápisom v obchodnom registri,
   b. odôvodnenie jeho poverenia spracúvaním osobných údajov dotknutých osôb,
   c. vyhlásenie sprostredkovateľa, že subdodávateľ poskytuje dostatočné záruky na vykonanie primeraných technických a organizačných opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov a zmluvy,
   d. vyhlásenie sprostredkovateľa, že subdodávateľ nevykonáva prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii ani iným organizáciám v SR, ktorá nezaručuje primeranú úroveň ochrany osobných údajov,
   e. vyhlásenie sprostredkovateľa, že subdodávateľ poučí svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby“), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných údajov ako aj o iných právach a povinnostiach sprostredkovateľa upravených touto zmluvou alebo ustanovených všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov.
5. Zmluvné strany sa dohodli, že sprostredkovateľ po obdržaní súhlasu na spracúvanie osobných údajov podľa tejto zmluvy prostredníctvom subdodávateľa písomne poverí subdodávateľa spracúvaním osobných údajov podľa zmluvy za podmienok, za akých je oprávnený/povinný ich spracúvať sprostredkovateľ a len v rozsahu

nevyhnutnom pre realizáciu zmluvy v záujme prevádzkovateľa, resp. jeho dotknutých osôb. Sprostredkovateľ je povinný predložiť kópiu zmluvy so subdodávateľom do 5 pracovných dni od jej vyžiadania prevádzkovateľovi.

6. Subdodávateľ spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa. Ak subdodávateľ nesplní svoje povinnosti pri spracúvaní osobných údajov dotknutých osôb, sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný za plnenie týchto povinnosti subdodávateľom. Sprostredkovateľ sa nemôže zbaviť zodpovednosti za porušenie povinnosti subdodávateľom tvrdením, že tieto povinnosti porušil subdodávateľ sprostredkovateľa. Ustanovenia GDPR o sprostredkovateľovi, vrátane ustanovení zmluvy upravujúcich povinnosti a podmienky spracúvania osobných údajov zo strany sprostredkovateľa sa vzťahujú aj na subdodávateľa.
7. Sprostredkovateľ je povinný oznámiť prevádzkovateľovi ukončenie spracúvania osobných údajov dotknutých osôb prostredníctvom subdodávateľa, a to bezodkladne, najneskôr však do piatich pracovných dní od ukončenia takéhoto spracúvania. Toto oznámenie musí o. i. obsahovať aj popis spôsobu splnenia povinnosti sprostredkovateľa vo vzťahu k tomuto subdodávateľovi.

Čl. IX
Ostatné dohodnuté podmienky

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

Čl. X
Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Sprostredkovateľ berie na vedomie povinnosť prevádzkovateľa zverejniť túto zmluvu a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy v plnom rozsahu.
2. Táto zmluva nadobúda platnosť podpisom oprávnených zástupcov zmluvných strán a účinnosť dňom nasledujúcim deň po dni zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Táto zmluva sa uzatvára na dobu určitú, do dňa skončenia platnosti a účinnosti zmluvy o poskytovaní služieb č. 12929-22/2023-BA.
4. Počas platnosti zmluvy o poskytovaní služieb je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane.

5. Práva a povinnosti neupravené touto zmluvou sa budú riadiť príslušnými ustanoveniami právnych predpisov platných na území SR.
6. Zmluvné strany štandardne komunikujú prostredníctvom elektronickej pošty. V prípadoch, keď to vyžaduje zmluva, všeobecne záväzný právny predpis alebo jedna zo zmluvných strán, doručí sa aj listinná podoba požiadavky, súhlasu a pod.
7. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.
8. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k zmluve.
9. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.
10. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave, dňa .....

Za prevádzkovateľa:

_____

Ing. Michal Ilko
generálny riaditeľ Sociálnej poisťovne

V Bratislave dňa .....

Za sprostredkovateľa:

_____

Ing. Juraj Ondriš
predseda predstavenstva SWAN, a.s.

_____

Ing. Miroslav Strečanský
podpredseda predstavenstva SWAN, a.s.

Zmluva
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 12929-25/2023-BA
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Čl. I
Zmluvné strany

Prevádzkovateľ

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

(ďalej len „**prevádzkovateľ**“)

a

Obchodné meno:	**SWAN, a.s.**
Sídlo:	Landererova 12, 811 09 Bratislava
Štatutárny orgán:	Ing. Juraj Ondriš, predseda predstavenstva Ing. Miroslav Strečanský, podpredseda predstavenstva
Zápis v registri:	Obchodný register Mestského súdu Bratislava III, oddiel Sa, vložka č. 2958/B.
IČO:	35 680 202
DIČ:	2020324317
IČ pre DPH:	SK2020324317
Bankové spojenie:	
IBAN:	[redacted] (ďalej len „**Poskytovateľ**“)

(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. Poskytovateľ je podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti Poskytovateľom, 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 o poskytovaní služieb č. 12929-22/2023-BA, predmetom ktorej je poskytovanie komplexných komunikačných služieb virtuálnej privátnej siete, časť: Primárne linky a integračné služby (ďalej len „Zmluva k VPS SocPoist“).
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 a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania sietí a informačných systémov prevádzkovateľa, s prevádzkou ktorého priamo súvisí výkon činností Poskytovateľa na základe Zmluvy k VPS SocPoist.

2. Výkon činností, ktoré priamo súvisia s realizáciou Zmluvy k VPS SocPoist.

Čl. IV
Práva a povinnosti zmluvných strán

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

2. Poskytovateľ 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. Poskytovateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú súčasťou a bezpečnostnej politiky prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve, a bezpečnostných politikách prevádzkovateľa. Poskytovateľ vyhlasuje, že s bezpečnostnými opatreniami súhlasí.

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

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

6. Poskytovateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy alebo aktualizovať bezpečnostnú dokumentáciu, ak si to vyžiadajú zmeny, ktoré sú aktuálne a musia zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi.

7. Poskytovateľ 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. Poskytovateľ je povinný doručiť prevádzkovateľovi zoznam zamestnancov Poskytovateľa, subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa Zmluvy k VPS SocPoist a tejto zmluvy a ktorí budú mať prístup k informáciám prevádzkovateľa (ďalej len „zoznam osôb“). Poskytovateľ je povinný oznámiť prevádzkovateľovi každú zmenu v zozname zamestnancov podľa tohto bodu a to elektronicky prostredníctvom Ústredného portálu verejnej správy (ďalej „UPVS“). Poskytovateľ 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 k VPS SocPoist. Po podpísaní vyhlásenia o mlčanlivosti budú týmto osobám sprístupnené bezpečnostné politiky prevádzkovateľa.

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

10. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Poskytovateľa 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. Poskytovateľ 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 Poskytovateľa pre prevádzkovateľa podľa Zmluvy k VPS SocPoist. Poskytovateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania Zmluvy k VPS SocPoist.
4. Odplata za plnenie povinností Poskytovateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených Poskytovateľom v súvislosti s plnením povinností Poskytovateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom Poskytovateľovi podľa Zmluvy k VPS SocPoist a na žiadne ďalšie peňažné plnenia Poskytovateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Čl. VI
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

Poskytovateľ 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 Poskytovateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa,
b. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Realizačnej zmluvy 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 Poskytovateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
e. predchádzať hrozbe vzniku kybernetických incidentov,
f. v prípade vzniku kybernetických incidentov, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
g. prijímať od prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
h. zasielať prevádzkovateľa 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. Poskytovateľ 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 je Prílohou č. 1 tejto zmluvy, 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, Poskytovateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky toto hlásenie doplní.
2. Poskytovateľ je povinný riešiť kybernetický incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení kybernetického incidentu na mieste, reakciou na kybernetický incident a podporou reakcií na kybernetický incident.
3. Pri riešení kybernetických incidentov je Poskytovateľ povinný poskytnúť prevádzkovateľovi a jemu nadriadeným orgánom najmä Národnému bezpečnostnému úradu a Ministerstvu investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI), vrátane jeho organizačného útvaru CSIRT, plnú súčinnosť pri riešení kybernetického incidentu a vyšetrovaní bezpečnostnej udalosti súvisiacej s plnením podľa Realizačnej zmluvy a všetky informácie získané z vlastnej činnosti podľa Zmluvy k VPS SocPoist alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického incidentu.
4. Poskytovateľ je povinný oznámiť prevádzkovateľovi skutočnosti, či v súvislosti s Kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Poskytovateľ je povinný v čase Kybernetického incidentu zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho prevádzkovateľovi.
6. Poskytovateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi vykonanie opatrenia na riešenie Kybernetického incidentu a jeho výsledok.
7. Po vyriešení Kybernetického incidentu je Poskytovateľ 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 Poskytovateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak je navrhované ochranné opatrenie zjavne neúspešné, je Poskytovateľ povinný spolupracovať s prevádzkovateľom na návrhu nového ochranného opatrenia.
8. Po schválení ochranného opatrenia prevádzkovateľom je Poskytovateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť prevádzkovateľovi.
9. Poskytovateľ 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. Poskytovateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením Zmluvy k VPS SocPoist a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. Poskytovateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na ostatné základné služby prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí prevádzkovateľa.
2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.
3. Poskytovateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu a zahrnúť tieto povinnosti do Vyhlásení o mlčanlivosti, ktoré musia zamestnanci Poskytovateľa a jeho subdodávateľov podpísať pred výkonom Zmluvy k VPS SocPoist.

Čl. IX
Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u Poskytovateľa audit zameraný na overenie plnenia povinností Poskytovateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Poskytovateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Poskytovateľa pre plnenie cieľov na základe zákona o kybernetickej bezpečnosti a tejto zmluvy.
2. Prípadné nedostatky zistené auditom je Poskytovateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní od ich zistenia.
3. Prevádzkovateľ môže audit u Poskytovateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti prevádzkovateľa pri výkone auditu realizuje prevádzkovateľom poverená tretia osoba.
4. Poskytovateľ 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 a Zmluvy k VPS SocPoist.
5. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom Poskytovateľa, ktorí sa podieľajú na plnení úloh a úseku kybernetickej bezpečnosti podľa tejto zmluvy a Zmluvy k VPS SocPoist.
6. V rámci auditu je Poskytovateľ povinný preukázať prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ je povinný oznámiť Poskytovateľovi najmenej sedem pracovných dní vopred svoj zámer vykonať u Poskytovateľa audit.
8. Vykonanie alebo nevykonanie auditu prevádzkovateľom nezbavuje zodpovednosti Poskytovateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy a Zmluvy k VPS SocPoist.
9. Ak Poskytovateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy a Zmluvy k VPS SocPoist.
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. Poskytovateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení 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. Poskytovateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základné služby prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Poskytovateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania kybernetických incidentov v Dokumente kybernetických incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa mu predložiť uvedenú dokumentáciu.
4. Poskytovateľ je povinný plniť povinnosti podľa tejto zmluvy odo dňa jej účinnosti.
5. V prípade, ak Poskytovateľ plní Zmluvy k VPS SocPoist prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s poskytovaním elektronických komunikačných služieb alebo sietí v súvislosti s prevádzkou základných služieb prevádzkovateľa, 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. Poskytovateľ 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. Poskytovateľ 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, Poskytovateľ zodpovedá za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, Realizačnej 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 preukázanú náhradu škody, pokuty alebo iné náklady, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov Poskytovateľa.
8. Po ukončení tejto zmluvy je Poskytovateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie protokolárne zničiť, ak osobitný predpis, právne predpisy EÚ alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane Poskytovateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.

Čl. XI
Kontaktné osoby pre kybernetickú bezpečnosť

1. Poskytovateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom UPVS, pričom Poskytovateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s Poskytovateľom na úseku kybernetickej bezpečnosti je: riaditeľ odboru bezpečnosti informačných systémov.
3. Kontaktná osoba Poskytovateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je: [redacted].
4. Kontaktné osoby podľa bodov 2. a 3. tohto článku zmluvy 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 k VPS SocPoist definovanej v článku II - Zmluva č. 12929-22/2023-BA.
4. Počas platnosti a účinnosti Zmluvy k VPS SocPoist 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 a právnymi predpismi EÚ.
6. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.

7. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve.

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

9. Neoddeliteľnou súčasťou tejto zmluvy je:

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

10. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.

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

V Bratislave, dňa .....

Za prevádzkovateľa:

…….....

Ing. Michal Ilko
generálny riaditeľ
Sociálnej poisťovne

V Bratislave, dňa .....

Za Poskytovateľa:

……

Ing. Juraj Ondriš
predseda predstavenstva
SWAN, a.s.

……

Ing. Miroslav Strečanský
podpredseda predstavenstva
SWAN, a.s.

Príloha č. 1 k Prílohe č. 10 - Zmluve č. 12929-22/2023-BA o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Bezpečnostné politiky

1. Všeobecné ustanovenia

(1) Poskytovateľ sa zaväzuje pri plnení zmluvy dodržiavať platné a účinné všeobecne záväzné právne predpisy Slovenskej republiky a právne predpisy EÚ.

(2) Vstup a pohyb zamestnancov Poskytovateľa, resp. jeho subdodávateľa, prípadne iných tretích osôb, prostredníctvom ktorých Poskytovateľ poskytuje služby (ďalej len „tretia osoba“) do priestorov prevádzkovateľa v súvislosti splnením predmetu zmluvy a Zmluvy k VPS SocPoist 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 Poskytovateľa, 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 Poskytovateľa, ak sa Poskytovateľ s prevádzkovateľom písomne nedohodne inak.

(2) Práca na diaľku sa povoľuje len pre určitý okruh zamestnancov Poskytovateľa, 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 Poskytovateľa.

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

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

(6) Žiadosť o zriadenie vzdialeného prístupu pre zamestnanca Poskytovateľa, resp. jeho subdodávateľa, alebo tretiu osobu postúpi príslušný zmluvný kontakt prevádzkovateľa oddeleniu centrálneho dispečingu a monitorovania služieb IS SP. V žiadosti špecifikuje rozsah prístupových oprávnení. Po schválení žiadosti riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa a po doručení záznamu o vykonaní kontroly fyzickej bezpečnosti na mieste výkonu práce, zrealizuje požiadavku príslušný administrátor prevádzkovateľa.

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 Slovenskej republiky a EÚ a vnútorných predpisov prevádzkovateľa.

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 Poskytovateľ plní predmet zmluvy a predmet Zmluvy k VPS SocPoist, schválených riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa.

2.5 Zmluvy o dôvernosti alebo utajení

Dohoda o zachovaní dôvernosti je súčasťou Realizačnej zmluvy prevádzkovateľa s Poskytovateľom. 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 Poskytovateľom 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 Poskytovateľom

3.1 Informačná bezpečnosť vo vzťahoch s Poskytovateľom

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

3.1.1 Politika informačnej bezpečnosti na vzťahy s Poskytovateľom

(1) Predtým, než sa Poskytovateľovi, prípadne jeho subdodávateľovi, alebo tretej osobe povolí prístup k chráneným informáciám prevádzkovateľa, bude vykonaná identifikácia rizík informačnej bezpečnosti a implementované vhodné opatrenia na pokrytie identifikovaných rizík na strane Poskytovateľa, 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 Poskytovateľa, resp. subdodávateľa, alebo tretej osoby k chráneným informáciám prevádzkovateľa nebude dovolený skôr, ako je podpísaná zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s Poskytovateľom a ako sú realizované primerané bezpečnostné opatrenia na ochranu aktív prevádzkovateľa.

(3) Zamestnancovi Poskytovateľa, 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 Poskytovateľa, resp. subdodávateľa, alebo tretej osobe za účelom testovania môže byť zriadené len do testovacieho prostredia a akceptačného 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 Poskytovateľom

(1) Zmluvy na výkon činností s Poskytovateľom 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 k VPS SocPoist 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 k VPS SocPoist s Poskytovateľom zaujme stanovisko riaditeľ odboru bezpečnosti informačných systémov, ktorý posúdi dostatočnosť bezpečnostných opatrení a notifikačných povinností, ktoré musia platiť počas celej doby platnosti Zmluvy k VPS SocPoist pre zaistenie kybernetickej bezpečnosti.

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

3.1.3 Monitorovanie a preskúmanie dodávateľských služieb

(1) Služby a záznamy poskytované Poskytovateľom sú priebežne kontrolované osobou zodpovednou za výkon Zmluvy k VPS SocPoist, 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 Poskytovateľom, jeho subdodávateľom alebo treťou osobou túto kontrolu vykonáva aj zodpovedná osoba prevádzkovateľa.

3.1.4 Riadenie zmien v službách Poskytovateľa

Zmeny v službách poskytovaných Poskytovateľom týkajúce 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 Poskytovateľa, jeho subdodávateľa alebo tretia osoba, ktorý má podozrenie, že odhalil slabé miesto, alebo zistil podozrenie z bezpečnostného incidentu, je povinný to bezodkladne oznámiť. Oznámenie vykoná nasledovne:

a) e-mailom odboru bezpečnosti informačných systémov prevádzkovateľa na adresu BIS@socpoist.sk a,

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

3.1.6 Informovanie o slabinách informačnej bezpečnosti

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

3.1.6.1 Hlavné kategórie bezpečnostných incidentov

(1) V oblasti ochrany zdravia zamestnancov a klientov

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

(2) V oblasti majetku prevádzkovateľa

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

(3) V oblasti informačnej bezpečnosti prevádzkovateľa

a) zverejnenie hesla používateľa,
b) zmena alebo resetovanie hesla na účte alebo zariadení neoprávnenou osobou,
c) diskreditácia bezpečnostného predmetu (GRID karty, tokenu, prvkov PKI),
d) prístup neoprávnenej (cudzia osoba, nevyškolená obsluha a pod.) osoby do IS SP,
e) vírusová infiltrácia do IS SP, zasielanie nežiadúceho obsahu, škodlivý kód,
f) prienik do IS alebo pokus o prienik,
g) kybernetický bezpečnostný incident,
h) inštalácie neschváleného hardvéru a softvéru na Komponentoch IS SP,
i) neoprávnené premiestnenie technických Komponentov IS SP,
j) používateľom vykonané zmeny hardvérovej konfigurácie počítača, servera, siete, komunikačných prvkov a pod.,
k) nevykonávanie záloh na serveroch zaradených do systému centralizovaných záloh alebo serverov s inak definovanou zálohovacou stratégiou,
l) zničenie alebo odcudzenie médií, na ktorých sú bezpečnostné zálohy serverov,
m) prepisovanie auditných záznamov,
n) krádež hardvéru alebo softwaru, ktorá ovplyvňuje prevádzky schopnosť IS SP,
o) krádež a deštrukcia dát IS SP,
p) zámerné zneužitie prístupu k zariadeniam IS SP,
q) neplánovaný výpadok elektrického prúdu,
r) poskytnutie, sprístupnenie, alebo zverejnenie osobných údajov konaním osoby alebo technickou poruchou IS v rozpore s pravidlami platných vnútorných predpisov prevádzkovateľa,
s) neoprávnené použitie vstupno-výstupných zariadení nepatriacich do vlastníctva prevádzkovateľa, spôsobujúce hrozbu nebezpečnej infiltrácie,
t) spracúvanie osobných údajov inou ako oprávnenou osobou,
u) porušenie bezpečnostných vnútorných predpisov prevádzkovateľa majúce za následok nedostupnosť služieb pre klientov alebo partnerov prevádzkovateľa,
v) porušenie vnútorných predpisov prevádzkovateľa s kontrolovateľným až katastrofálnym dopadom pre prevádzkovateľa.

3.1.7 Poučenie a záväzok mlčanlivosti

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

(2) Za nahlásenie a zabezpečenie účasti zamestnanca Poskytovateľa, resp. subdodávateľa a/alebo tretej osoby na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe Zmluvy k VPS SocPoist je zodpovedný Poskytovateľ. Nahlásenie vykoná kontaktná osoba.

Príloha č. 2 k Prílohe č. 10 - Zmluve č. 12929-22/2023-BA o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni

Obsah

Úvod

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

Cieľ dokumentu

Tento dokument sumarizuje 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))

Dokument neobsahuje podrobné implementačné detaily jednotlivých opatrení. Podrobné implementačné detaily budú musieť byť vypracované v projektovej dokumentácii, zmenovej dokumentácii a ostatných podkladových materiálov, ktoré spracujú zadávatelia projektov spolu s IT analytikmi, IT architektami, PM a internými či externými dodávateľmi a následne ich predložia odboru BIS na validáciu.

Obmedzenia

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

I. Štandardy implementácie

I.A. Bezpečnosť životného cyklu

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

I.B. 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.

I.C. Implementácia riešenia

1) Riešenie musí byť vyvíjané v bezpečnom vývojovom prostredí.
2) Pri implementácii by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky / knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb.
3) V prípade, že implementované riešenie potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.
4) Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie, pričom:
   a) jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
   b) commity by mali mať zmysluplné popisy,
   c) mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commite.
5) Nemali by byť použité funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v súčasnej dobe zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.
6) Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však:
   a) zapnuté všetky varovania a ochrany vývojových nástrojov
   b) varovania vývojového prostredia
7) Všetky varovania z predchádzajúceho bodu by mali byť opravené.
8) Počas vývoja musí byť vedená vývojárska dokumentácia:
   a) dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii
   b) v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená objednávateľom.
9) Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávateľovi spolu so samotným riešením.

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

I.D. 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.

I.E. 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.

I.F. Bezpečný návrh – Webové aplikácie

3) Webová stránka by mala pozostávať z verejných a neverejných zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.
4) Citlivé informácie by mali byť uchovávané v zašifrovanej podobe.
5) Validácia vstupov musí byť vykonávaná na strane servera a odporúča sa, aby bola vykonávaná aj na strane klienta.
6) 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.
7) Kód musí byť udržiavaný, prehľadný a dokumentovaný. Viď sekciu 5.11.
8) Prezentačná vrstva musí byť oddelená od aplikačnej a databázovej vrstvy.

II. Konfigurácia webového servera

II.A. Systém

1) Systém, nainštalované aplikácie a frameworky musia byť pravidelne aktualizované z pohľadu bezpečnosti.
2) Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.
3) Počas doby, kedy prebieha údržba, rozsiahlejšia alebo mimoriadna aktualizácia OS/SW a/alebo nasadzovanie bezpečnostných záplat, by mali byť webové servery oddelené od zvyšku siete organizácie alebo byť umiestnené v izolovaných sieťach.
4) Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.
5) Na serveri musia byť zatvorené všetky nepotrebné porty.
6) Autentifikácia používateľov na OS servera musí zodpovedať nasledujúcim požiadavkám:
7) Nepotrebné implicitné účty musia byť odstránené alebo zneplatnené.
8) Neaktívne kontá musia byť zneplatnené.
9) Na serveri by mali byť nakonfigurované používateľské skupiny, kontrola prístupu a udeľovanie privilégií by mali byť pre konkrétnych používateľov riadené ich zaradením do týchto skupín.
10) Heslo ku kontu musí zodpovedať požiadavkám organizácie na komplexnosť hesiel a má byť znemožnený útok hádaním či hrubou silou, viď príloha dokumentu.
11) 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).
12) Lokálny administrátor webservera musí byť unikátny pre každý webový server.
13) Servery s OS Windows buď nesmú byť v doméne alebo musia byť spravované RO doménovým radičom (RODC – read-only domain controller).

II.B. Webový server

1) Pri inštalácií webového servera a bezprostredne po nej by mali byť vykonané nasledovné kontroly a akcie:
   a) SW webového servera má byť inštalovaný na dedikovanom hostiteľskom zariadení alebo na dedikovanom virtualizovanom OS.
   b) Musia byť aplikované dostupné záplaty a aktualizácie na eliminovanie známych zraniteľností

c) Pre webový obsah by mal byť vytvorený dedikovaný fyzický disk alebo logická partícia (separátne od OS a SW webového servera).
d) Všetky služby inštalované popri webovom serveri, ktoré nie sú potrebné (napr. FTP server alebo služba vzdialenej administrácie) musia byť vypnuté alebo odstránené.
e) Nepotrebné východzie účty vytvorené pri inštalácií by mali byť odstránené alebo vypnuté.
f) Z webového servera majú byť odstránené testovacie a ukážkové súbory vrátane vykonateľných súborov a skriptov a dokumentácia výrobcu.
g) Odporúčame na server aplikovať hardenovací skript alebo bezpečnostnú šablónu, vhodný pre daný OS a webový server. Info možno čerpať z príručiek dostupných na webstránke CSIRT.SK.
h) Banner HTTP služby by mal byť rekonfigurovaný, podľa potreby aj s ďalšími bannermi tak, aby nereportovali typ a verziu webového servera a podkladového OS.

2) Webový server by mal podporovať iba HTTP metódy POST a GET.
3) Webový server nesmú podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
4) Webový server musí byť odolný voči SlowHTTP DoS útokom (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty, implementácia loadbalancerov)
5) Z webového servera musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy, ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.
6) Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.
7) Na serveri musí byť nakonfigurovaný defaultný virtuálny host na obsluhu prístupu na webserver prostredníctvom IP adresy (cez prehliadač). Nesmie byť zobrazovaná defaultná stránka použitého frameworku a pod.
8) Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.
9) Webový server by nemal podporovať funkcionalitu listovania adresára (Directory listing, Microsoft IIS tilde directory enumeration).
10) Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).
11) Webový server by mal byť chránený WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:
    a) Detekcia a prevencia známych útokov (Code injection – SQL, XSS, Command, XPATH, ...),
    b) Kontrola používateľských vstupov prostredníctvom whitelistingu a ich prekódovanie do HTML entít alebo podobných bezpečných náhrad.
12) Webový server s aplikáciou spracúvajúcou citlivé údajov a/alebo klasifikované informácie, musí byť chránený WAF, ktorého konfigurácia musí byť reštriktívna (kontrola business logiky a pod).
13) Na zvýšenie dostupnosti webového servera odporúčame použiť load balancery. Podľa možnosti môžu byť rozšírené o web cache. V prípade podpory web cache nesmú byť cacheované administrátorské stránky, prístupové údaje a podobné citlivé informácie.
14) Na zvýšenie dostupnosti webového servera môžu byť ako bezpečnostné brány použité reverzné proxy. Podľa možnosti môžu byť rozšírené o funkcie akcelerácie šifrovania, používateľskej autentifikácie alebo filtrovania obsahu.
15) Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov (kvôli DoS útoku).
16) Webový server musí dodržiavať negociačný postup negociácie TLS spojenia, popísaný v RFC 5746, kvôli zraniteľnosti Insecure renegociation a riziku útoku typu MitM.
17) Webový server by mal podporovať bezpečnú renegociáciu (Secure renegotiation)
18) V prípade viacerých virtuálnych hostov musí byť oddelené úložisko cookies minimálne na úrovni adresárov.

II.C. Administrácia, logovanie a zálohovanie

4) Správcovské rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).
5) Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.
6) Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.

7) Webové správcovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.
8) Na serveri musí byť aktívne logovanie:
   a) Malo by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent.
   b) Pre každý virtuálny host na fyzickom webserveri by mal existovať separátny log.
   c) V logoch musia byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná.
   d) Logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii.
   e) Na uchovávanie logov musí byť vyhradená dostatočná kapacita.
   f) Logy by mali byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov.
   g) Logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie, minimálne však raz týždenne. V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva organizácie, by mali byť logy kontrolované denne.
9) 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

II.D. Kontrola prístupu OS a webového servera

1) Proces webového servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.
2) Webový server by mal byť konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné na čítanie, no nie na zápis. Procesy webového servera by nemali mať právo zápisu do priečinkov, kde je uchovávaný verejný webový obsah (web content).
3) OS by mal byť nakonfigurovaný tak, aby proces webového servera mohol vytvárať log záznamy, no nemohol ich čítať.
4) OS by mal byť podľa možnosti nakonfigurovaný, aby dočasné súbory vytvorené procesmi webového servera boli obmedzené na určený a vhodne zabezpečený priečinok. Ak je to možné, prístup k dočasným súborom by mal byť obmedzený na procesy, ktoré ich vytvorili.
5) Webový obsah a všetky logy ním vytvárané by mali byť umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server.
6) Odporúča sa webový server izolovať od iných procesov použitím prostriedkov ako napríklad chroot, kontajnery, virtualizácia a pod.
7) Pre externé skripty a programy, vykonávané ako časť obsahu webového servera by mal byť vytvorený samostatný priečinok (napr. JavaScript knižnice a pod).
8) Mal by byť stanovený maximálny počet procesov webového servera a/alebo sieťových spojení, ktoré by server mal povoliť.
9) Spúšťanie skriptov, ktoré nie sú výlučne pod kontrolou administratívneho konta, malo by byť zakázané (napr. vytvorením a kontrolou prístupu k separátnemu priečinku, obsahujúcom autorizované skripty).
10) Použitie symbolických linkov by malo byť pre procesy webového servera zakázané.
11) Odporúčame vytvoriť kompletnú maticu prístupov k webovému obsahu (access matrix). V nej by malo byť definované, ktoré súbory a priečinky majú byť prístupné a pre koho.

12) V odôvodnených prípadoch odporúčame zaviesť kontrolu proti botom (napr. CAPTCHA, nofollow, filtrovanie kľúčových slov).

II.E. 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

II.F. Aplikácia (webový portál)

1) Aplikácia musí ošetrovať všetky chyby a výnimky.
2) Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.
3) V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.
4) Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).
5) Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.
6) Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.
7) Aplikácia nesmie ukladať citlivé údaje (napríklad identifikátor relácie) v URL adrese. V prípade zakázania cookies v prehliadači musí stránka zobraziť hlásenie o nutnosti použitia cookies (ak sa používajú).
8) Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy na SR).
9) Aplikácie nesmie používať odkazy na nedôveryhodné externé zdroje.
10) Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).
11) Aplikácia nesmie používať funkciu eval() alebo jej alternatívy.
12) Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

II.G. Autentifikácia a autorizácia

1) Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).
2) Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token).
3) Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.
4) Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.
5) Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.

6) Pre webové aplikácie, ku ktorým je na prístup nutná autentifikácia, je nutné zabezpečiť, aby žiadna webová stránka, ktorá má byť prístupné až po autentifikácii, nebola dostupná bez vykonania kompletného procesu autentifikácie.
7) Autentifikácia musí prebiehať prostredníctvom protokolu HTTPS.
8) Aplikácia musí vyžadovať používanie silných hesiel.
9) V prípade použitia iniciálnych náhodne generovaných hesiel pre nového používateľa musí aplikácia pri prvom prihlásení vyžadovať zmenu tohto hesla, v súlade s definovanými pravidlami pre tvorbu hesiel.
10) Aplikácia musí umožňovať administrátorom i používateľom zmeniť ich heslo.
11) Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.
12) Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.
13) Aplikácia musí pri zmene hesla vyžadovať opakované zadanie nového hesla (2 krát), pričom nové zadané heslá sa musia zhodovať.
14) Odporúčame pri zmene hesla používať viacfaktorové potvrdenie, napríklad Out-Of-Band kanálom (mail, SMS, KeyCloak, ...)
15) Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.
16) Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.
17) Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať soľ (angl. salt).
18) Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti. Funkcia odhlásenia má byť jednoducho identifikovateľná a dostupná z každej stránky, prístupnej po autentifikácii.
19) Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.
20) Odporúča sa, aby aplikácia podporovala simultánne paralelné prihlásenie k jednému účtu iba z jednej verejnej IP adresy. Odporúča sa, aby aplikácia pri zmene verejnej IP adresy prihláseného používateľa požadovala reautentifikáciu.
21) Odporúča sa naviazanie relácie na parameter User-Agent.
22) Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lockout) po istom počte neúspešných pokusov (maximálne 5) o prihlásenie.
23) Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie musí trvať aspoň 10 minút.
24) Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie do kritického systému by malo trvať aspoň hodinu.
25) Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out, neúspešný log-in, lockout konta, žiadosť o zmenu hesla).
26) V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.
27) Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať (napr. štandardné loginy ako admin, administrator, user a pod, názov alebo typ aplikácie, kombinácie uvedených a pod.).
28) Aplikácia nesmie pre kritické systémy umožniť funkcionalitu zapamätania si hesla.
29) Používateľské kontá by mali byť po určitej dobe nečinnosti znefunkčnené.
30) Používateľské kontá, ktoré neboli použité do 3 mesiacov od ich vytvorenia (používateľ sa počas danej doby nikdy neprihlásil), by mali byť deaktivované.
31) Každý používateľ a administrátor musia mať jedinečné ID.
32) Aplikácia nesmie umožniť vytváranie účtov s používateľským menom podobným administrátorským či servisným kontám. (admin, administrator, helpdesk, support a pod.)
33) Aplikácia musí korektne inštruovať prehliadač, aby neukladal citlivé informácie, prenášané prostredníctvom HTTPS, do cache (a aby neboli bez kontroly opäť prístupné z histórie prehliadania) minimálne v rozsahu:
    a) Server musí nastavovať vo svojich odpovediach hlavičky
    ◦ Cache-Control: no-cache, no-store, private, must-re-validate, max-age=0, no-transform
    ◦ Expires: 0

◦ Pragma: no-cache

II.H. Používateľské vstupy

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

II.I. Relácie

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

13) Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.
14) Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.
15) Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.

II.J. 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.

II.K. 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.

II.L. 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.

III. Interná infraštruktúra a vývojové prostredie

III.A. 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 mesiacov, odporúča sa aktualizovať aspoň raz za mesiac.
   e) Na serveroch by malo byť implementované anti-malware riešenie, ktoré je centrálne spravované a centrálne logované.
   f) Všetky servery majú nastavené lokálny NTP server ako autoritatívny zdroj času a pre preklad doménových mien na IP adresy používajú lokálne DNS servery
   g) Všetky zariadenia musia byť hardenované podľa odporúčaní výrobcu.

III.B. 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 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.

IV. Štandardy prepojenia

IV.A. 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
   b) Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),
   c) 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),
   d) používanie skupiny protokolov Internet Procotol Security (IPSEC) na zabezpečenie sieťových protokolov.

IV.B. 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).

IV.C. Špecifikácie prepojenia pomocou sieťových služieb

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

IV.D. Sieťová a komunikačná bezpečnosť

1) Aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov.
2) Na prenos informácií k tretím stranám uzatvorenie zmluvy o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami.
3) 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.
4) 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.
5) Vzdialený prístup do vnútornej siete SP musí podliehať autentifikácii a autorizácii, vyžaduje sa použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.
6) Zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a ich uchovávanie aspoň 4 mesiace.
7) Na všetkých serveroch podporujúcich základné služby informačných technológií SP sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.
8) Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.
9) Implementácia druhého sieťového firewallu od iného výrobcu tak, aby interné servery a klientske stanice boli vo vzťahu k externým sieťam chránené dvomi sieťovými firewallmi.
10) Implementácia Web Application Firewallu (WAF) na všetkých verejne dostupných a kritických webových aplikáciách.
11) Implementácia manažmentu logov.
12) Implementácia DNSSEC a jeho využitie pre všetky externe dostupné služby.
13) Konfigurácia a izolovanie klientskych portov na prístupových switchoch tak, aby pracovné stanice spolu nemohli priamo komunikovať (technológia PVLAN). Táto požiadavka nahrádza požiadavku zo Z2-Fl) o maximálnom počte MAC adries.
14) Zabezpečenie prístupu používateľov k Internetu a k službám mimo siete SP cez proxy server a uchovávanie prístupových logov aspoň 6 mesiacov.
15) Používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 mesiace.
16) Uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 6 mesiacov.
17) Rozdelenie siete do jednotlivých segmentov podľa účelu, pričom v rovnakých segmentoch môžu byť len zariadenia s rovnakými požiadavkami na úroveň zabezpečenia.
18) Zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 mesiacov.

V. Prenos elektronickej pošty

V.A. Prenos elektronickej pošty

1) Štandardom prenosu elektronickej pošty je
   a) používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronických poštových správ,
   b) podpora kryptografického protokolu Transport Layer Security (TLS) na zabezpečenie prenosu elektronických poštových správ.
2) SMTP banner by nemal obsahovať informácie o použitom softvéri ani iné citlivé informácie. Nesmie byť možné zistiť verziu použitého softvéru prostredníctvom help príkazov.
3) Mailové správy odchádzajúce z organizácie by nemali obsahovať informácie o infraštruktúre organizácie (napríklad privátne IP adresy v hlavičke Received-From).
4) Odpoveď na príkaz VRFY by nemala obsahovať informáciu o existencií adresy alebo používateľského mena. Odporúča sa odpovedať kódom 252 s generickou hláškou.
5) Nemala by byť povolená metóda EXPN.
6) SMTP server by nemal preposlať e-mail, ktorý neobsahuje zdrojovú hlavičkovú e-mailovú adresu.
7) SMTP server musí prijímať správy na doručenie z externých sietí len pre spravované domény.
8) SMTP server musí prijímať správy na preposlanie len od autentifikovaných používateľov alebo z určených SMTP serverov.
9) Server by mal detegovať a blokovať pokusy o rozoslanie veľkého množstva e-mailov.
10) SMTP server musí kontrolovať správy pomocou anti-spam filtra.
11) SMTP server musí kontrolovať správy na prítomnosť škodlivého kódu
12) SMTP server musí logovať všetky detegované anomálie.
13) SMTP server musí logovať informácie o spracovávaných e-mailoch a tieto informácie by mali byť uchovávané aspoň 6 mesiacov. Musia byť uchovávané aspoň 3 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.

V.B. 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) pri chránenom prístupe k verejným elektronickým poštovým službám.

V.C. Formát elektronických poštových správ

1) 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.

VI. Štandardy prístupu k elektronickým službám

VI.A. 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) 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.

VI.B. 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) pri chránenom verejnom prístupe k adresárovým službám.

VII. Štandardy webovej služby

VII.A. 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 klientských 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 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.

VIII. Štandardy integrácie dát

VIII.A. 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.

VIII.B. 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 § 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 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.

IX. 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),

X. Dátové štandardy

X.A. 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; v ostatných prípadoch sa použijú vlastné dátové prvky,

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

XI. 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

XII. 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.

XIII. Firewall

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

XIV. 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.

XV. 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:
   1. plnenia určených požiadaviek a kritérií pre oblasť BIS pri dodávke predmetu zmluvy,

2. ochrany informácií, ku ktorým je poskytnutý prístup,

3. oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa BIS a ďalších opatrení a postupov BIS špecifických na plnenie predmetu zmluvy,

4. riadenia a monitorovania prístupov do informačných technológií SP vrátane spôsobu a mechanizmu,

5. možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,

6. oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií SP zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,

7. spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,

8. 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

1. kritické komponenty a prvky služby,

2. možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,

3. možné riziká BIS vo vzťahoch medzi dodávateľmi a subdodávateľmi,

4. 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 inernej siete (komunikácia je fultrovaná sieťovým firewallom)

DNS - Domain Name System

DoS – Denial of Service

FW – Firewall

IB – Informačná bezpečnosť

ICS - Industrial Control System

MitM útok – Man in the Middle útok

MVC – návrhový vzor Model–View–Controller

MVP - návrhový vzor Model–View–Presenter

NAC – Network Access Control

NAP - Network Access Protection
NDP - Neighbor Discovery Protocol - protokol v IPv6, okrem iného, nahradzujúci ARP z IPv4

NTP - Network Time Protocol

OS - Operačný systém PVLAN – Private

VLAN princíp least privilege

RDP - Remote Desktop Protocol

QoS - Quality of Service

Sieťový firewall - firewall umiestnený v sieti filtrujúci komunikáciu viacerých zariadení, prípadne sietí (nie lokálny firewall)

SNMP – Simple Network Management Protocol

SSO – Single Sign-On

Telepresence

UAC – User Access Control

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VOIP – Voice over IP

WAF – Webaplikačný firewall - špeciálny typ firewallu, prispôsobený na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku.

Whitelisting - metóda kontroly prístupu k službám, ktorá povoľuje prístup iba špecifikovaným klientom a všetkým ostatným ho zakazuje

XSS - Cross-Site Scripting

Zdroje a Legislatívne východiská

- Slov-lex
- Eur-lex
- Sémantický znalostný strom vedomostí Knowww EU portál
- Vláda SR
- Ústredný portál verejnej správy
- Rokovania legislatívnej rady vlády SR
- Zoznam uznesení vlády SR
- Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
- CSIRT
- NASES
- NBÚ
- Interné normy SP
- NIST
- NSA
- OWASP
- IETF
- IAB
- RFC
- Zákon č. **294/1994** Z. z. o Sociálnej poisťovni
- 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. **452/2021** Z. z. o elektronických komunikáciách (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
- 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 GDPR)
- 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
- 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 prevádzkovanej služby (kritériá základnej služby)
- Vyhláška Národného bezpečnostného úradu č. **165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov v aktuálne platnom znení
- Vyhláška Národného bezpečnostného úradu č. **166/2018** Z. z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- Vyhláška Národného bezpečnostného úradu č. **362/2018** Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- Výnos MF SR č. **55/2014** Z. z., o štandardoch pre IS VS v aktuálne platnom znení.
- Nariadenia Európskeho parlamentu a Rady (EÚ) **2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov),
- Nariadenie Európskeho parlamentu a Rady (EÚ) **2018/1725** z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES
- Nariadenie Európskeho parlamentu a Rady (EÚ) **2019/881** zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
- Smernica Európskeho parlamentu a Rady (EÚ) **2016/1148** zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
- Smernica Európskeho parlamentu a Rady (EÚ) **2016/2102** z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora
- Smernica Európskeho parlamentu a Rady (EÚ) **2019/1024** z 20. júna 2019 o otvorených dátach a opakovanom použití informácií verejného sektora
- Smernica č. **7/2019** o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT
- Metodika Používateľské princípy pre návrh a rozvoj elektronických služieb verejnej správy https://www.mirri.gov.sk/sekcie/oddelenie-behavioralnych-inovacii/index.html
- Metodika Jednotný dizajn manuál elektronických služieb verejnej správy - Metodické usmernenie UVSR č. 002089/2018/oLŠISVS-7 zo dňa 11.05.2018 https://www.mirri.gov.sk/wp-content/uploads/2018/10/Metodicke-usmernenie-ID-SK-publikovat.pdf
- Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (Číslo spisu v DKS: 004307/2019/oBI) https://www.mirri.gov.sk/wp-content/uploads/2019/04/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-verejnej-spravy.pdf
- Metodika riadenia QAMPR https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html
- Metodický pokyn k zabezpečeniu centrálneho nákupu produktov a služieb spoločnosti ORACLE v rámci Centrálnej rámcovej dohody na poskytovanie licencií a produktov ORACLE a služieb s nimi súvisiacich https://www.mirri.gov.sk/wp-content/uploads/2020/02/Metodicky_pokyn_ORACLE_CRD_2019.pdf
- Metodické usmernenie nariadeniu (GDPR) k spracúvaniu osobných údajov (prostredníctvom web stránok) v súlade s požiadavkami Nariadenia Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20190901.html

- Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT) – aktuálne znenie MetodikaZabezpeceniaIKT_v2.1.pdf (gov.sk)

Klasifikačné stupne informačných aktív

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

Dôvernosť

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako

verejné informačné aktíva určené pre verejnosť, ktoré sú získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie,

interné informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,

chránené informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,

prísne chránené informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

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

Integrita

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

nízka zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu,

stredná zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

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

Dostupnosť

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako

nízka zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,

stredná zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

vysoká zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.