Evidenčné číslo Objednávateľa: 2022-0133-1211601
Evidenčné číslo Poskytovateľa: IPS-SZ/005/2022

Servisná zmluva na technickú podporu APM dátového koncentrátora.

uzavretá podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník
v znení neskorších predpisov (ďalej len „Obchodný zákonník")
(ďalej len „Zmluva")

I. ZMLUVNÉ STRANY

1.1 **Objednávateľ**:

	Slovenská elektrizačná prenosová sústava, a.s.
	Mlynské nivy 59/A
	824 84 Bratislava
Zapísaný:	v Obchodnom registri Okresného súdu Bratislava I.,
	oddiel: Sa, vložka č. 2906/B
IČO:	35 829 141
DIČ:	2020261342
IČ DPH:	SK2020261342
bankové spojenie:	TATRA BANKA, a.s., Bratislava
číslo účtu:	2620191900/1100
číslo účtu v tvare	SK30 1100 0000 0026 2019 1900
IBAN/SWIFT:	BIC(SWIFT): TATRSKBX
Menom spoločnosti koná:	Ing. Peter Dovhun, generálny riaditeľ
	Juraj Saktor, vrchný riaditeľ úseku ICT
Osoby oprávnené konať vo veciach:	
zmluvných:	Ing. Vladimír Beňo, výkonný riaditeľ sekcie tech. pod.SED a ASDR
technických:	Ing. Ľubomír Ďurčanský, vedúci odboru zabezpečenia prev. SED
	Ing. Marek Vandlíček, špecialista

(ďalej len „**Objednávateľ**" alebo „**SEPS**")

1.2 **Poskytovateľ**:

	IPESOFT spol. s r.o.
	Bytčická 2
	Žilina 010 01
Zapísaný:	v Obchodnom registri Okresného súdu Žilina
	oddiel: Sro, vložka č. 1304/L
IČO:	31 589 898
DIČ:	2020445746
IČ DPH:	SK2020445746
bankové spojenie:	Slovenská sporiteľňa, a.s.
číslo účtu:	0076566203/0900
číslo účtu v tvare	SK74 0900 0000 0000 7656 6203
IBAN/SWIFT:	GIBASKBX
Menom spoločnosti koná:	Ing. Florián Kevický , PhD., prokurista

Osoby oprávnené konať vo veciach:

zmluvných:	Ing. Florián Kevický , PhD., prokurista
technických:	Ing. Tomáš Rajčan, vedúci oddelenia EUM

(ďalej len „**Poskytovateľ**")

(Objednávateľ a Poskytovateľ ďalej spoločne ako „**Zmluvné strany**" alebo jednotlivo ako „**Zmluvná strana**").

II. PREAMBULA

2.1 Účelom tejto Zmluvy je zabezpečiť kontinuitu prevádzky APM dátového koncetrátora vo vlastníctve Objednávateľa a stanoviť práva a povinnosti Zmluvných strán pri zabezpečovaní technickej podpory pre dodaný softvér na základe zmluvy č. 2022-0121-1176520.

2.2 Podkladom pre uzatvorenie tejto Zmluvy je výberové konanie a ponuka Poskytovateľa ako úspešného uchádzača zo dňa 27.06.2022.

III. PREDMET ZMLUVY

3.1 Predmetom tejto servisnej Zmluvy je poskytovanie služieb technickej podpory (ďalej len „služby") APM dátového koncetrátora.

3.2 Služby APM dátového koncetrátora sú špecifikované v Prílohe č.1, v kapitole 7 tejto Zmluvy „Technická špecifikácia pre APM dátový koncentrátor".

3.3 V prípade potreby Poskytovateľ služieb na základe tejto Zmluvy poskytne Objednávateľovi aj služby nad rámec tejto zmluvy, ktoré budú realizované formou samostatných objednávok, podľa bodu 7.3 Prílohy č. 1 tejto zmluvy.

3.4 Objednávateľ sa zaväzuje za poskytnuté služby zaplatiť Poskytovateľovi dohodnutú cenu.

IV. MIESTO A ROZSAH PLATNOSTI ZMLUVY

4.1 Miestami dodania predmetu Zmluvy sú:
Slovenská elektrizačná prenosová sústava, a. s., AB Bratislava a DC Podunajské Biskupice.

4.2 Povinnosťou Poskytovateľa je poskytovať plnenie podľa tejto Zmluvy po dobu jej platnosti podľa článku V. ČAS PLNENIA, pričom tieto povinnosti sa vzťahujú na služby, ktoré sú uvedené v Prílohe č. 1 tejto Zmluvy.

4.3 Rozsah poskytovaných služieb je špecifikovaný v Prílohe č. 1, ktorý je môžné meniť len na základe písomného dodatku k Zmluve.

V. ČAS PLNENIA

5.1 Táto Zmluva sa uzatvára na dobu štyroch rokov od dátumu účinnosti podľa bodu 14.1 tejto Zmluvy..

VI. CENA

6.1 Cena za predmet Zmluvy v zmysle článku III. PREDMET ZMLUVY za celé obdobie trvania Zmluvy je **59 400,00 EUR bez DPH**,

slovom: päťdesiatdeväťtisícštyristo EUR bez DPH,

z toho cena za rok je **14 850,00 EUR bez DPH**,

slovom: štrnásťtisícosemstopäťdesiat EUR bez DPH.

6.2 Cena za služby nad rámec tejto zmluvy sa bude fakturovať na základe vystavenia samostatných objednávok.

6.3 Cena v uvedenej výške podľa bodu 6.1 zahŕňa všetky súvisiace náklady.

6.4 K cene bude fakturovaná DPH v zmysle zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len „zákon o DPH).

VII. PLATOBNÉ PODMIENKY

7.1 Cena za technickú podporu podľa tejto Zmluvy bude fakturovaná Poskytovateľom Objednávateľovi štvťročne, pričom každá faktúra za uplynulý štvrťrok bude vystavená na cenu za služby uvedenú v bode 6.1 vo výške 25% ceny za rok, t. j. **3 712,50 EUR bez DPH**. V prípade, ak fakturačné obdobie nebude celý kalendárny štvrťrok, Poskytovateť vystaví faktúru za služby v alikvótnej výške zo štvrťročnej platby Faktúry budú vystavené do 15 dní od skončenia príslušného fakturačného obdobia, v ktorom boli služby poskytnuté. Poskytovateľ je oprávnený vystaviť faktúru na základe protokolu o odsúhlasení poskytnutých služieb. Dňom vzniku daňovej povinnosti je posledný deň príslušného fakturačného obdobia, za ktorý sa servisné služby poskytovali.

7.2 Cena podľa bodu 6.2 bude Poskytovateľom fakturovaná samostatnými faktúrami, do 15 dní odo dňa vzniku daňovej povinnosti. Poskytovateľ je oprávnený vystaviť faktúru na základe protokolu o prevzatí predmetu objednávky. Dňom vzniku daňovej povinnosti je deň prevzatia predmetu objednávky Objednávateľom na základe protokolu o prevzatí predmetu objednávky."

7.3 Faktúra sa považuje za doručenú v listinnej (tlačenej) forme na adresu sídla Objednávateľa a v elektronickej forme výlučne na adresu efaktury@sepsas.sk. Elektronická faktúra doručená na inú e-mailovú adresu sa nepovažuje za elektronickú faktúru doručenú Objednávateľovi v zmysle tejto Zmluvy.

7.4 Faktúra musí obsahovať náležitosti v zmysle platných právnych predpisov, evidenčné číslo Zmluvy Objednávateľa, číslo bankového účtu v tvare IBAN. V prípade, že faktúra nebude obsahovať uvedené náležitosti, je Objednávateľ oprávnený vrátiť ju Poskytovateľovi. V takom prípade sa preruší plynutie lehoty splatnosti a nová lehota splatnosti začne plynúť doručením opravenej faktúry Objednávateľovi.

7.5 Objednávateľ sa zaväzuje uhradiť Poskytovateľovi dohodnutú zmluvnú cenu na základe doručenej faktúry, ktorej splatnosť je 60 dní odo dňa jej doručenia Objednávateľovi.

7.6 Objednávateľ podpisom tejto Zmluvy udeľuje Poskytovateľovi súhlas v zmysle ustanovenia § 71 ods. 1 písm. b) zákona o DPH, aby vystavoval a spracúval faktúry v elektronickej forme, za podmienky predchádzajúceho informovania Objednávateľa o používaní elektronickej formy fakturácie v zmysle bodu 7.7 Zmluvy.

7.7 Do 10 dní od nadobudnutia účinnosti tejto Zmluvy, je Poskytovateľ povinný písomne oznámiť Objednávateľovi, či bude pri fakturácii podľa tohto zmluvného vzťahu používať elektronickú formu alebo listinnú (tlačenú) formu faktúr. Písomné oznámenie Poskytovateľa o forme spôsobu fakturácie sa považuje za záväzné dňom jeho doručenia Objednávateľovi. V prípade doručovania faktúr elektronicky, bude v oznámení uvedená aj e-mailová adresa, z ktorej budú elektronické faktúry odosielané.

7.8 Ak si Poskytovateľ, nesplní riadne a včas svoju povinnosť podľa bodu 7.7 tejto Zmluvy, za záväznú formu fakturácie sa považuje listinná (tlačená) forma.

7.9 Poskytovateľ je oprávnený písomne požiadať Objednávateľa o zmenu formy fakturácie aj v priebehu trvania zmluvného vzťahu. Spôsob fakturácie sa považuje za zmenený odo dňa písomného potvrdenia zmeny spôsobu fakturácie zo strany Objednávateľa Poskytovateľovi.

VIII. POVINNOSTI POSKYTOVATEĽA

8.1 Poskytovateľ poskytne Objednávateľovi služby podľa podmienok Zmluvy a Prílohy č. 1 tejto Zmluvy.

8.2 Poskytovateľ nesmie vykonávať žiadne zásahy do iných ICT prostriedkov, než do prostriedkov špecifikovaných v Prílohe č. 1.

8.3 Pre zabezpečenie prístupu zamestnancov Poskytovateľa na pracovisko Objednávateľa na dobu dlhšiu ako jeden deň dodá Poskytovateľ oprávnenej osobe Objednávateľa menný zoznam týchto zamestnancov (meno, pracovné zaradenie).

8.4 Poskytovateľ sa zaväzuje evidovať všetky incidenty v elektronickej evidencii Poskytovateľa od ich otvorenia až po ich uzavretie tak, aby existovala prehľadná evidencia servisných zásahov. Poskytovateľ sa zaväzuje počas priebehu zásahu na požiadanie Objednávateľa emailom informovať o priebehu riešenia. Informácia musí obsahovať evidenčné číslo incidentu z evidencie Poskytovateľa.

8.5 Poskytovateľ je povinný pri prácach postupovať tak, aby neprerušil prevádzku (ak nebola výluka prevádzky vopred dohodnutá) a je povinný bezodkladne telefonicky a následne písomne upozorniť Objednávateľa na stav, kedy došlo k prerušeniu prevádzky alebo prác.

8.6 Poskytovateľ zabezpečí kontinuálny postup prác a spoluprácu všetkých organizačných zložiek Poskytovateľa, ktoré sa zúčastňujú na plnení predmetu Zmluvy.

8.7 Poskytovateľ zabezpečí ochranu autorských a licenčných práv na dodávané produkty.

8.8 Pri plnení Zmluvy je Poskytovateľ povinný počínať si tak, aby nedochádzalo ku škodám na zdraví, na majetku, na prírode a životnom prostredí. Ak Poskytovateľ, resp. jeho subdodávatelia spôsobia v súvislosti s činnosťami, ktoré sú vykonávané v rámci plnenia predmetu Zmluvy Objednávateľovi škodu, Poskytovateľ sa zaväzuje Objednávateľovi nahradiť túto škodu v plnom rozsahu.

8.9 Poskytovateľ je povinný pri poskytovaní dohodnutých služieb dodržiavať „Všeobecné zmluvné podmienky zabezpečovania BOZP a OPP" uvedené v Prílohe č. 2 Zmluvy.

8.10 Poskytovateľ sa zaväzuje nakladať so vzniknutým odpadom v súlade so zákonom č.79/2015 Z.z. o odpadoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Poskytovateľ zabezpečí uloženie odpadov vzniknutých pri servisných činnostiach na vyhradené miesto, ktoré mu určí Objednávateľ. Zhodnotenie, resp. zneškodnenie uvedeného druhu odpadu zabezpečí Objednávateľ na vlastné náklady.

8.11 Poskytovateľ je povinný dodržiavať všeobecné zmluvné podmienky zabezpečovania informačnej bezpečnosti, ktoré sú definované v Prílohe č. 3.

8.12 Poskytovateľ bude viesť zoznamy všetkých oprávnených pracovníkov s prístupom do APM Dátový koncentrátor počas ich prítomnosti pri implementácii predmetu diela u Objednávateľa, vrátane ich špecifických elektronických a fyzických práv do systémov, serverov, databáz a termínu, v ktorom bude prístup ukončený. Objednávateľ bude informovaný o všetkých zmenách zoznamu účtov jeho oprávnených pracovníkov a ich oprávnení v APM Dátový koncentrátor.

8.13 Ak Poskytovateľ počas plnenia predmetu diela vytvorí alebo upraví softvér APM Dátový koncentrátor nad rámec štandardného SW, dodá Objednávateľovi dokumentáciu, zdrojové kódy a príslušné kompilátory vrátane oprávnenia na ich modifikáciu Obstarávateľom alebo Obstarávateľom určenými tretími stranami.

IX. POVINNOSTI OBJEDNÁVATEĽA

9.1 Za Objednávateľa sú osobami, ktoré zodpovedajú za preberanie poskytovaných služieb predmetu Zmluvy a koordinujú plnenie predmetu Zmluvy, osoby oprávnené konať vo veciach technických tejto Zmluvy.

9.2 Objednávateľ poskytne Poskytovateľovi včas všetky informácie potrebné pre korektné plnenie predmetu Zmluvy, ako napríklad technické špecifikácie, organizačné schémy, informácie o zmluvných záväzkoch voči tretím osobám, ak sa týkajú plnenia Zmluvy.

9.3 Objednávateľ poskytne potrebnú súčinnosť dohodnutú v Zmluve.

9.4 Objednávateľ zabezpečí spoluprácu všetkých organizačných zložiek Objednávateľa, ktoré sa zúčastňujú na plnení predmetu Zmluvy.

9.5 Objednávateľ Poskytovateľovi včas poskytne všetky informácie o prerušení prác, ak sa tretie strany pri plnení svojich povinností súvisiacich s plnením predmetu Zmluvy dostali do omeškania.

9.6 Objednávateľ zabezpečí udržiavanie záložných kópií všetkého prevádzkovaného systémového softvéru tak, aby boli prístupné v prípade, že budú potrebné pri riešení problému.

X. OCHRANA DÔVERNÝCH INFORMÁCIÍ

10.1 V tejto Zmluve "dôverné informácie" znamenajú všetky informácie, ktoré sa týkajú alebo môžu týkať poskytovania služieb, vrátane a bez obmedzenia všetkých údajov a informácií, dokumentov a správ, ponúk, cien, návrhov kontraktov, know-how, vzorcov, postupov, projektov, fotografií, výkresov, špecifikácií, softvérových programov a akýchkoľvek iných médií nesúcich alebo zahrňujúcich takéto informácie a akýchkoľvek materiálov, ktoré budú pri použití týchto dokumentov spracované a budú tieto informácie obsahovať.

10.2 Poskytovateľ sa zaväzuje použiť všetky dôverné informácie takto poskytnuté výlučne pre potreby poskytovania služieb. Akékoľvek ďalšie použitie informácií bude podliehať predchádzajúcemu písomnému súhlasu Objednávateľa.

10.3 Poskytovateľ sa zaväzuje prezradiť/poskytnúť dôverné informácie len na základe písomného súhlasu iba subdodávateľom, dodávateľom a zamestnancom týchto subjektov ale len tým, ktorí preukázateľne potrebujú poznať takéto dôverné informácie pre účely riadneho a včasného poskytovania služieb v zmysle tejto Zmluvy.

10.4 Poskytovateľ nebude robiť kópie dôverných informácií, pokiaľ to nebude nevyhnutné pre potreby oprávnených osôb, zaviazaných mlčanlivosťou.

10.5 Pre potreby masmédií môžu poskytovať informácie iba poverení zástupcovia Objednávateľa.

10.6 Objednávateľ sa zaväzuje použiť všetky dôverné informácie poskytnuté Poskytovateľom výlučne pre potreby realizácie tejto Zmluvy. Akékoľvek ďalšie použitie informácií bude podliehať predchádzajúcemu písomnému súhlasu Poskytovateľa.

XI. ZODPOVEDNOSŤ ZA VADY

11.1 Poskytovateľ zodpovedá za to, že služby budú poskytované podľa podmienok tejto Zmluvy a v súlade s platnými všeobecne záväznými právnymi predpismi a príslušnými normami a že poskytované služby zodpovedajú dohodnutým službám v tejto Zmluve.

11.2 Objednávateľ sa zaväzuje, že prípadnú poruchunahlási bezodkladne po jej zistení písomnou formou.

XII. ZMLUVNÉ POKUTY

12.1 Ak Poskytovateľ nedodrží termín zahájenia opravy resp. nedodrží dohodnuté termíny odstránenia vád podľa Prílohy č. 1 kapitola 7, bod 7.1 tejto Zmluvy, môže Objednávateľ uplatniť zmluvnú pokutu vo výške 0,2% pre kritické chyby, 0,1% pre podstatné chyby a 0,05% za ostatné chyby z ceny za rok, za každé jednotlivé nedodržanie dohodnutého termínu a za každý jeden deň omeškania.

12.2 Ak Poskytovateľ spôsobí pri prácach neplánované prerušenie prevádzky, má Objednávateľ právo uplatniť si zmluvnú pokutu vo výške 0,5 % z ceny za rok, za každé jednotlivé porušenie.

12.3 Ak Poskytovateľ nedodrží povinnosť definovanú v bode 8.10, má Objednávateľ právo uplatniť si zmluvnú pokutu uvedenú v Prílohe č. 2 tejto zmluvy.

12.4 Za každé jednotlivé porušenie povinnosti podľa bodu 14.3 tejto Zmluvy je Objednávateľ oprávnený uplatniť si u zhotoviteľa zmluvnú pokutu vo výške 1.500,- EUR EUR (slovom tisícpäťsto eur).

12.5 Za každé jednotlivé porušenie povinnosti v zmysle čl. X tejto Zmluvy je Objednávateľ oprávnený uplatniť si u zhotoviteľa zmluvnú pokutu vo výške 5 000,- EUR (slovom päťtisíc eur).

12.6 V prípade omeškania Objednávateľa s úhradou zmluvnej ceny na základe doručenej faktúry má poskytovateľ právo na uplatnenie úroku z omeškania vo výške 1M EURIBOR + 8% p. a. z dlžnej sumy za každý deň omeškania. Pre výpočet úroku sa použije hodnota 1M EURIBOR, ktorá je platná k prvému dňu omeškania s platbou. Ak 1M EURIBOR nedosiahne kladnú hodnotu (záporná hodnota), pri výpočte úroku sa použije 1M EURIBOR rovný nule.

12.7 Vznikom nároku na zmluvnú pokutu podľa tohto článku, jej uplatnením, vyúčtovaním, alebo zaplatením, nie je dotknutá povinnosť Poskytovateľa vzniknuté vady odstrániť, a nezaniká právo Objednávateľa na uplatnenie náhrady škody spôsobenej porušením zmluvných povinností Poskytovateľom v plnom rozsahu.

XIII. UKONČENIE ZMLUVY

13.1 Zmluvu je možné ukončiť vzájomnou dohodou Zmluvných strán, výpoveďou bez udania dôvodu zo strany Objednávateľa alebo odstúpením od tejto Zmluvy.

13.2 Podstatným porušením Zmluvy v zmysle ustanovení § 344 a nasl. Obchodného zákonníka a teda dôvodom na okamžité odstúpenie od tejto Zmluvy sa považuje:

13.2.1 nesplnenie povinností Poskytovateľom poskytovať služby v zmysle tejto Zmluvy, ako aj v súlade so súťažnými podkladmi pre poskytovaní predmetných služieb a to ani v dodatočnej lehote na odstránenie nedostatkov stanovenej Objednávateľom v predchádzajúcej písomnej výzve;

13.2.2 viacnásobné (t. j. viac ako trikrát za dobu trvania Zmluvy) prekračovanie zmluvne dohodnutých časov v zmysle Prílohy č. 1;

13.2.3 strata oprávnenia Poskytovateľa vykonávať podnikateľskú činnosť;

13.2.4 ak je Objednávateľ v omeškaní so zaplatením ceny o viac ako 60 dní odo dňa splatnosti faktúry.

13.3 Nepodstatným porušením tejto Zmluvy sa rozumie nedodržanie ostatných zmluvných podmienok tejto Zmluvy okrem podmienok uvedených v bode 13.2. Na nepodstatné porušenie

tejto Zmluvy Objednávateľ Poskytovateľa písomne upozorní. Po opakovanom porušení tej istej Zmluvnej povinnosti je Objednávateľ oprávnený od tejto Zmluvy odstúpiť.

13.4 Odstúpenie od tejto Zmluvy je účinné dňom doručenia písomného oznámenia o odstúpení od tejto Zmluvy druhej Zmluvnej strane. Odstúpením sa zrušuje táto Zmluva ex nunc a Poskytovateľ je povinný zastaviť všetky práce potrebné na poskytovanie služieb v zmysle tejto Zmluvy do troch dní od oznámenia tejto skutočnosti Objednávateľom a je oprávnený na základe zápisu o poskytnutí služieb (potvrdenom oboma Zmluvnými stranami) vzniknuté náklady fakturovať. Vzniknuté preukázané a Objednávateľom uznané náklady Objednávateľ uhradí do 30 dní.

13.5 Podstatné porušenie tejto Zmluvy alebo jej opakované porušenia, ktoré nie sú podstatné, predstavujú závažné porušenie profesijných povinností v zmysle bodu 101 preambuly smernice Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES a v zmysle § 32 ods. 1 písm. h) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých predpisov.

13.6 Zmluvné strany sa dohodli, že Objednávateľ je oprávnený vypovedať Zmluvu bez uvedenia dôvodu. Výpovedná lehota je 6 mesiacov a začína plynúť prvým dňom v mesiaci nasledujúcim po mesiaci, v ktorom bola výpoveď doručená Poskytovateľovi.

XIV. ZÁVEREČNÉ USTANOVENIA

14.1 Zmluva nadobúda platnosť dňom jej podpisu oboma Zmluvnými stranami a účinnosť prvým dňom nasledujúceho mesiaca po prevzatí predmetu zákazky na základe zmluvy č: 2022-0121 -1176520 za podmienky jej predchádzajúceho zverejnenia. .

14.2 Zmluvné strany sa dohodli, že Zmluva a daňové doklady súvisiace so Zmluvou budú zverejnené takým spôsobom, ktorý pre povinne zverejňované zmluvy, objednávky a faktúry vyplýva z § 5a a 5b zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov. Tým nie je dotknutá ochrana utajovaných skutočností, ochrana osobnosti a osobných údajov, ochrana obchodného tajomstva, ako aj ďalšie obmedzenia prístupu k informáciám, ktoré zverejnenie obmedzujú, alebo vylučujú. Taktiež nie je dotknuté ustanovenie bodu 14.1 tejto Zmluvy.

14.3 Zoznam subdodávateľov podľa Prílohy č. 5 tejto Zmluvy je možné meniť len na základe vzájomnej dohody oboch Zmluvných strán formou dodatku k tejto Zmluve, ktorého obsahom bude nový zoznam subdodávateľov.

14.4 Práva a povinnosti Zmluvných strán, ktoré nie sú upravené v tejto Zmluve, sa riadia ustanoveniami Obchodného zákonníka a ustanoveniami ostatných súvisiacich všeobecne záväzných právnych predpisov platných na území SR.

14.5 S poukazom na skutočnosť, že v rámci poskytovania služby môže dochádzať k spracúvaniu osobných údajov dotknutých osôb, Poskytovateľ je povinný poskytovať služby tak, aby boli plne v súlade s požiadavkami na ochranu osobných údajov, ktoré ukladajú nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje Smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (spolu ďalej len „Legislatíva o ochrane osobných údajov") v znení ich prípadných neskorších zmien. Poskytovateľ je povinný poskytovať služby tak, aby najmä avšak nielen obsahovalo účinné bezpečnostné,

technické, resp. iné ďalšie opatrenia s cieľom zaistiť čo možno najvyššiu úroveň bezpečnosti a ochrany osobných údajov vyžadovanú Legislatívou o ochrane osobných údajov.

14.6 Poskytovateľ podpisom tejto Zmluvy potvrdzuje, že sa oboznámil s dokumentom spoločnosti SEPS s názvom „Politika ochrany osobných údajov v spoločnosti Slovenská elektrizačná prenosová sústava, a.s." zverejnenom na webovej stránke spoločnosti SEPS www.sepsas.sk, ktorého obsahom sú informačné povinnosti a ďalšie fakty o spracúvaní osobných údajov fyzických osôb zo strany spoločnosti SEPS v zmysle Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje Smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

14.7 Nakoľko spoločnosť SEPS je prevádzkovateľom základnej služby v sektore Energetika, podsektor Elektroenergetika v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon o kybernetickej bezpečnosti") a predmetom Zmluvy sú činnosti, ktoré súvisia s prevádzkou sietí a informačných systémov spoločnosti SEPS, Zmluvné strany sú povinné prijať a dodržiavať bezpečnostné opatrenia a plniť notifikačné povinnosti podľa Zákona o kybernetickej bezpečnosti s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov spoločnosti SEPS počas celej doby trvania zmluvného vzťahu založeného Zmluvou. Podmienky a spôsob zabezpečenia plnenia bezpečnostných opatrení a notifikačných povinností Zmluvných strán je vymedzený v Prílohe č. 4 tejto Zmluvy, ktorá je jej neoddeliteľnou súčasťou.

14.8 Ak by niektoré z ustanovení tejto Zmluvy bolo, alebo sa stalo neúčinným, neplatným, nezákonným alebo nevykonateľným (ďalej aj ako "vada pôvodného ustanovenia"), nebude tým dotknutá, ani obmedzená platnosť, účinnosť a vykonateľnosť ostatných ustanovení tejto Zmluvy. Zmluvné strany sa zaväzujú, že takto dotknuté ustanovenia Zmluvy nahradia novým ustanovením, ktoré netrpí vadou pôvodného ustanovenia a v čo najvyššej možnej miere zodpovedá duchu a účelu úpravy práv a povinností, obsiahnutých v zrušenom ustanovení.

14.9 Zmluvné strany vyhlasujú, že Zmluva nebola uzavretá v tiesni ani za nápadne nevýhodných podmienok a predstavuje prejav ich vôle, ktorý je urobený slobodne, vážne, určite a zrozumiteľne, a ktorý nie je urobený v omyle a svojím obsahom alebo účelom neodporuje alebo neobchádza zákon. Ďalej Zmluvné strany vyhlasujú, že sú spôsobilé na uzatvorenie tejto Zmluvy a jej plnenie je možné, sú oboznámené s jej obsahom a bez výhrad s ním súhlasia, na znak čoho k tejto Zmluve pripájajú svoje podpisy.

14.10 Pre prípad sporu na základe tejto Zmluvy sa dojednáva príslušnosť slovenského súdu.

14.11 Zmluvu je možné meniť alebo dopĺňať len písomnou dohodou Zmluvných strán formou dodatku k Zmluve.

14.12 Táto Zmluva je vypracovaná v dvoch rovnopisoch, z ktorých si každá zo Zmluvných strán ponechá jedno vyhotovenie.

14.13 Neoddeliteľnou súčasťou tejto Zmluvy sú Prílohy:

Príloha č. 1: Technická špecifikácia pre APM dátový koncentrátor.
Príloha č. 2: Všeobecné zmluvné podmienky zabezpečovania BOZP a OPP.
Príloha č. 3: Všeobecné zmluvné podmienky zabezpečovania informačnej bezpečnosti.
Príloha č. 4: Zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností.
Príloha č. 5: Zoznam subdodávateľov.

Príloha č. 6: Zoznam zodpovedných osôb.
Príloha č. 7: Preberací protokol.

V Bratislave dňa ..

V Žiline dňa .....

Za Objednávateľa:

Za Poskytovateľa:

.....
Ing. Peter Dovhun
generálny riaditeľ

.....
Ing. Florián Kevický, PhD.
prokurista

.....
Juraj Saktor
vrchný riaditeľ úseku ICT

Príloha č. 1

Technická špecifikácia pre APM dátový koncentrátor

30.3.2022

Obsah

1 Úvod

Predmetom zákazky je vybudovanie modulárneho APM Dátového koncentrátora (Asset Performance Management), ktorý bude automatizovane zbierať dáta z existujúcich monitorovacích systémov transformátorov a monitorovacích systémov vypínačov (MST a MSV), konsolidovať ich do jednotného formátu, ukladať v spoločnej historickej databáze a vykonávať nad nimi prehľadné číselné a grafické zobrazenia v jednotnom grafickom prostredí. Ide o komplexné integrálne riešenie, produkt s jednotným projektom, ktorého jednotlivé moduly sú založené na spoločnej technologickej platforme, bezpečne prepojené a uchádzač už odskúšal ich interoperabilitu v rámci iných projektov.

APM Dátový koncentrátor musí obsahovať nasledovné časti:

Softvérová časť:

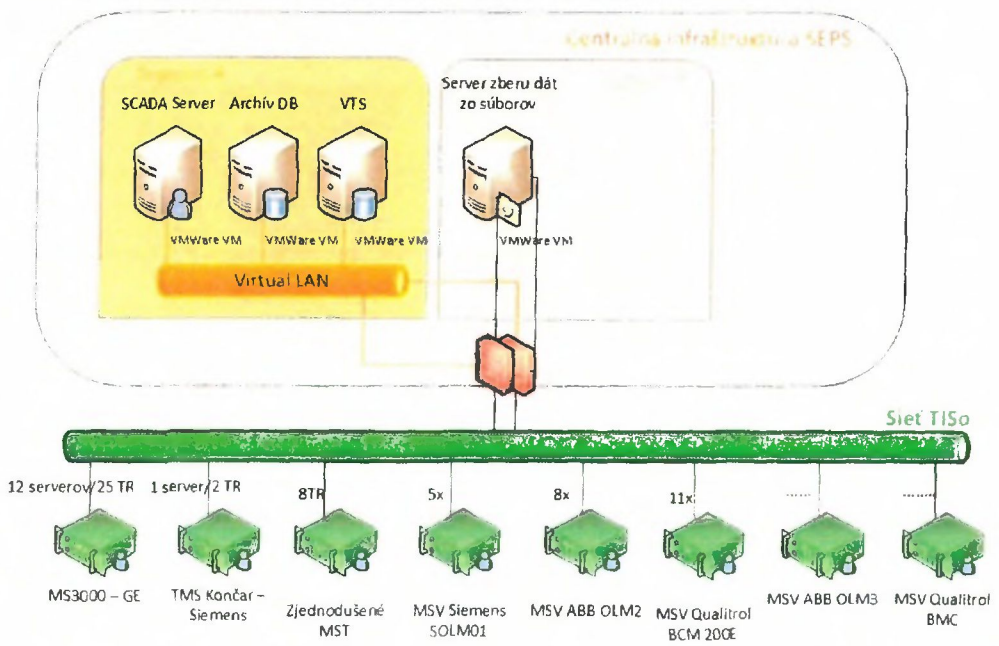
- modul pre realtime komunikáciu (RT modul),
- archivačný modul,
- server pre zber dát zo súborov,
- softvérová podpora,
- priprava komponentov na APM službu.

Softvérové komponenty musia byť dodávateľom navrhnuté tak, aby zabezpečili bezpečný a spoľahlivý chod (definovaný v kapitole 6. Požiadavky na výkonnosť) celej aplikácie a komponentov uvedených v kapitole 3. na obdobie minimálne 7 rokov.

Hardvérová časť:

Hardvér nebude predmetom dodávky, systém bude využívať prvky centrálnej infraštruktúry (virtualizácia, diskové úložiska, prvky kyberbezpečnosti) dodané SEPS vo forme súčinnosti na základe požiadaviek dodávateľa špecifikovaných v ponuke a upresnených v detailnom návrhu riešenia schválenom Obstarávateľom.

Požiadavky na hardvérové komponenty formou protiplnenia SEPS musia byť dodávateľom navrhnuté tak, aby zabezpečili bezpečný a spoľahlivý chod (definovaný v kapitole 6. Požiadavky na výkonnosť) všetkých softvérových modulov uvedených v kapitole 4.5 na obdobie minimálne 7 rokov.



2 Popis súčasného stavu

2.1 Monitorovacie systémy transformátorov

- MS3000 – GE (12 serverov/25 TR) a TMS Končar – Siemens (1 server/2 TR)

Oba typy MST majú implementovaný komunikačný protokol IEC 60870-5-104 a sú pripojené do siete TISo. Tento protokol je nutné nakonfigurovať tak, aby do RT modulu prúdili požadované dáta. Konfiguráciu IEC 60870-5-104 vykoná na strane APM Zhotoviteľ a Objednávateľ v spolupráci s výrobcami MST na strane MST. Na komunikáciu budú použité aktuálne používané prenosové linky.

- Zjednodušené MST (8 TR)

Dáta zo zjednodušených MST budú prepojené podľa technických možností danej verzie a spôsobu realizovateľnosti v nasledovnom poradí:

- technológiou Modbus RTU/TCP samostatne zo snímača plynov Hydrocal 1005 a samostatne z monitoringu priechodiek ZVCM,
- zber dát zo snímača plynov Hydrocal 1005 importovaním Access databázového súbor* do RT modulu. Dáta z monitoringu priechodiek ZVCM prenášať pomocou Modbus RTU/TCP,
- import Access databázového súboru*, ktorý generuje snímač plynov Hydrocal 1005 a ktorý obsahuje aj dáta z monitoringu priechodiek ZVCM.

*Toto riešenie si aktuálne vyžaduje prepojenie s už existujúcim dedikovaným serverom MS3000 v sieti TISo, na ktorom je nepretržite spustená aplikácia Hydrosoft s nastaveným automatickým periodickým sťahovaním dát zo zjednodušených MST (VARI T401, LMAR T401 a T402, SUCA T201 a T401). Softvér Hydrosoft bude počas implementácie APM preinštalovaný na „Server pre zber dát zo súborov". Najmenší časový interval automatického sťahovania dát, ktorý sa dá nastaviť je jedna hodina. Pri plánovanom stiahnutí dát sa aktualizuje Access databáza „data.mdb", ktorá je uložené na disku. Každý zjednodušený MST má svoju vlastnú databázu. V rámci riešenia diaľkového zberu dát z databáz APM Dátovým koncentrátorom je nutné vyriešiť transfer vybraných dát na diskový priestor pre APM. Konfiguráciu potrebných softvérov vykoná a zabezpečí na strane APM Zhotoviteľ a Objednávateľ v spolupráci s výrobcami MST na strane MST. Komunikačné linky na prepojenie zjednodušených MST a RT modulu sú vybudované.

Dodávateľ v rámci RT modulu v tomto kroku podľa požiadaviek SEPS vytvorí jednotné vizualizačné prostredia pre zobrazenie požadovaných procesných veličín a podmienky generovania alarmov.

2.2 Monitorovacie systémy vypínačov

MSV Siemens SOLM01

S jednotlivými zariadeniami SOLM01, ako aj s lokálnym serverom na príslušnej ESt je možná komunikácia prostredníctvom siete TISo, pričom po tejto sieti v rámci ESt beží komunikácia po vlastnom protokole zariadení. Všetky dáta z jednotlivých zariadení sa ukladajú do spoločnej databázy ORACLE. V rámci riešenia diaľkového zberu dát z databáz APM Dátovým koncentrátorom je nutné vyriešiť online prístup do databázy a transfer vybraných dát na diskový priestor pre APM. Konfiguráciu potrebných softvérov vykoná na strane APM Zhotoviteľ a Objednávateľ v spolupráci s výrobcami na strane MSV. Na komunikáciu budú použité aktuálne prenosové linky v rámci siete TISo.

MSV ABB OLM2

S jednotlivými zariadeniami OLM2 je možná komunikácia len po sériovom rozhraní RS485. Všetky monitorovacie zariadenia rovnako komunikujú po sériovej linke aj s lokálnym

priemyselným počítačom, ktorý je pripojený do siete TISo. Diaľková komunikácia s lokálnymi počítačmi je teda realizovaná prostredníctvom rozhrania Ethernet. Všetky dáta z jednotlivých zariadení sa ukladajú do spoločnej databázy MS Access 2003. V rámci riešenia diaľkového zberu dát z Access databáz verzie 2003 APM Dátovým koncentrátorom je nutné vyriešiť online prístup do databázy a transfer vybraných dát na diskový priestor pre APM. Konfiguráciu potrebných softvérov vykoná na strane APM Zhotoviteľ a Objednávateľ v spolupráci s výrobcami na strane MSV. Na komunikáciu budú použité aktuálne prenosové linky v rámci siete TISo.

MSV Qualitrol BCM 200E

S jednotlivými zariadeniami BCM 200E je možná komunikácia len po sériovom rozhraní RS485. Všetky monitorovacie zariadenia komunikujú po sériovej linke aj s lokálnym priemyselným počítačom, ktorý je pripojený do siete TISo. Diaľková komunikácia s lokálnymi počítačmi je realizovaná prostredníctvom rozhrania Ethernet. Všetky dáta z jednotlivých zariadení sa ukladajú do spoločnej databázy MS Access 1997. V rámci riešenia diaľkového zberu dát z Access databáz verzie 1997 APM Dátovým koncentrátorom je nutné vyriešiť online prístup do databázy a transfer vybraných dát na diskový priestor pre APM. Konfiguráciu potrebných softvérov vykoná na strane APM Zhotoviteľ a Objednávateľ v spolupráci s výrobcami na strane MSV. Na komunikáciu budú použité aktuálne prenosové linky v rámci siete TISo.

MSV v implementácii

V rámci projektu počítame aj s integráciou nových typov MSV:

- MSV ABB OLM3
- MSV Qualitrol BMC

Na komunikáciu APM Dátový koncentrátor s novými typmi MSV sa využijú protokoly definované v kapitole 3.1.1. Integrácia na vyššie uvedené nové typy MSV je súčasťou rozsahu projektu.

3 Koncepčná konfigurácia

Hlavné funkcionality APM Dátového koncentrátora:

- automatizovane a kontinuálne zbierať dáta z MST a MSV,
- on-line zobraziť dáta v jednotnej štruktúre v užívateľsky prijateľnom prostredí,
- vykonávať kontrolu funkčnosti a toku dát z MST a MSV,
- dáta zozbierané on-line agregovať a ukladať na základe požadovaných algoritmov do databázy v jednotnej dátovej štruktúre,
- ukladať dáta na základe užívateľsky nastaviteľných algoritmov (napr. možnosť meniť vzorkovanie, vylúčiť ukladanie dát a duplicitne generovaných alarmov v prípade poruchy MST a pod.)
- vytvárať zálohy dát tak, aby nedošlo k ich poškodeniu a strate,
- generovať inteligentné mailové notifikácie na základe dohodnutých algoritmov,
- možnosť užívateľsky upravovať dohodnuté algoritmy mailových notifikácií,
- zasielať mailové notifikácie špecifickým skupinám užívateľov,
- súčasné trvalé prihlásenie a používanie aplikácií minimálne siedmymi užívateľmi v súlade s kap. 6.4,
- možnosť manažovať dátové toky zariadení v prípade poruchy a dočasnej náhrady za zariadenie rovnakého typu (napr. v prípade poruchy snímača a jeho výmeny za

náhradný, možnosť nastaviť adresovanie nového v systéme t.j. systém umožní kontinuálne ukladanie dát z náhradného snímača do databázy.),

- zabezpečiť dáta a aplikácie tak, aby spĺňali podmienky kybernetickej bezpečnosti,
- pripraviť APM Dátový koncentrátor tak, aby ho bolo možné rozšíriť o ďalšie zariadenia a ďalšie typy zariadení prostredníctvom protokolov uvedených v kap. 3.1.1.
- celý systém bude onsite na SEPS a dáta neopustia prostredie SEPS

3.1 Softvérová časť

3.1.1 RT modul

RT modul navrhnutý a optimalizovaný na zber dát a komplexné monitorovanie primárnych a sekundárnych zariadení prenosových a distribučných staníc v reálnom čase.

Funkcionality RT modulu:

- zber dát
- autorizácia užívateľov,
- definovanie rolí/ právomocí,
- vypršanie platnosti relácie,
- kryptovanie komunikácie,
- záznam udalostí/ alarmov,
- reportovanie,
- grafické rozhranie a zobrazenie procesných veličín.
- podporované protokoly a rozhrania:
  - IEC 60870-5-101,
  - IEC 60870-5-104,
  - IEC 61850
  - Modbus RTU,
  - Modbus TCP,
  - DDE,
  - ODBC,
  - OPC.

RT modul a Archív musia byť doplnené o vývojovo testovacie prostredie. Bližší popis je v kapitole Aplikácia a vývoj systému (archivačné výpočty).

RT modul musí umožňovať online zobrazenie dostupných procesných veličín v užívateľsky nastaviteľnom, prijateľnom a jednotnom prostredí v závislosti od verzie a typu pripojeného monitorovacieho systému. Pozostáva z grafického prostredia, ktoré musí obsahovať:

- základnú obrazovku zobrazujúcu súhrnný stav monitorovaných zariadení podľa elektrických staníc.
- menu a objektové ikony, ktorými je možné zobraziť:
  - podmenu s najdôležitejšími veličinami,
  - ďalšie podmenu s podrobnými veličinami.

- zoznam alarmov:
    - zoznam aktívnych nepotvrdených výstrah a alarmov,
    - zoznam aktívnych potvrdených výstrah a alarmov,
    - zoznam neaktívnych nepotvrdených výstrah a alarmov,
    - výstrahy a alarmy farebne rozlišovať podľa stavu,
    - musí obsahovať názov procesnej veličiny, názov elektrickej stanice, označenie monitorovaného zariadenia, dátum a čas vzniku, aktuálny status, poznámku,
    - všetky výstrahy a alarmy počas celého obdobia musia byť ukladané do historickej databázy,
    - výstrahy a alarmy musí byť možné filtrovať podľa požiadaviek.
- inteligentné notifikácie, ktoré sú užívateľsky nastaviteľné tak, aby boli odfiltrované falošné hlásenia (napr. pri zapnutí transformátora do času zastabilizovania veličín sú vygenerované výstrahy/alarmy. Tie sa postupne zastabilizujú a výstrahy/alarmy spontánne odpadnú. Systém je potrebné ošetriť voči generovaniu notifikácii pre výstrahy/alarmy pri zapínaní.)
- inteligentná mailová notifikácia:
    - odosielať výstrahy a alarmy na konkrétne skupiny užívateľov,
    - možnosť administrácie užívateľov.
- kontrolu toku dát resp. funkčnosti MST a MSV,
- možnosť integrovať procesné a odvodené veličiny a archiváciou súčasných historických dát, upresnené pri detailnom návrhu riešenia. Minimálny rozsah je uvedený v kapitole 4.2, v tabuľke 4-1: Minimálny požadovaný súbor údajov na uloženie a archiváciu.

3.1.2 Archivačný modul

Zbiera a ukladá presným a spoľahlivým spôsobom rôzne typy údajov v databáze navrhnutej na archiváciu stoviek tisíc hodnôt v priebehu dlhého časového obdobia. Spracovanie a organizácia údajov ďalej umožňuje jednoduchú interpretáciu a vizualizáciu (číselnú a grafickú) pre rôznych užívateľov. Riešenie funkcionalitou zálohovania „backup & recovery".

Funkcionality archivačného modulu a zobrazení systému:

- automatická centrálna archivácia s možnosťou manuálnej úpravy údajov (doplnenia údajov) ,
- ľahká a prehľadná vizualizácia historických dát a udalostí/ alarmov,
- konfigurácia vlastných pohľadov, tabuliek a grafov,
- prispôsobenie vlastnej pracovnej plochy a časových úsekov,
- porovnávanie rôznych grafov, kopírovanie a presun premenných zo zobrazení do grafov,
- export nadefinovaných dát do čitateľného formátu (txt, csv,...) na ďalšie spracovanie,
- individuálna konfigurácia pracovnej plochy užívateľov,
- možnosť užívateľsky definovať zobrazenie rôznych typov grafov, tabuliek a reportov (zo zoznamu),
- plná konfigurovateľnosť vybraných grafov podľa potrieb užívateľa,

- úprava parametrov vizualizácie ako je typ grafu, farby, čiary a výplne,
- usporiadanie grafov jednoduchým presunutím okna a jeho ukotvenia na novom mieste.
- import historických údajov upresnené pri detailnom návrhu riešenia

Archivačný modul musí umožňovať pristupovať k dátam z viacerých prostredí a platforiem pomocou distribuovaného prostredia **REST API (Asset monitoring a Asset simulácia)**.

Požiadavkou na archivačný modul je dlhodobo ukladať agregované dáta z RT modulu. Dodávateľ archivačného modulu musí pripraviť a po odsúhlasení Obstarávateľom implementovať model agregácie konkrétnych procesných veličín.

Ďalšou úlohou archivačného modulu je graficky zobrazovať agregované historické dáta v prehľadných a užívateľsky nastaviteľných pohľadoch.

Úprava pohľadov musí byť riešená pomocou rolí (užívateľ alebo administrátor) určených pre jednotlivé skupiny užívateľov.

3.1.3 Server pre zber dát zo súborov

Server pre zber dát zo súborov bude umiestnený v samostatnom segmente siete a oddelený od modulov RT a Archív, firewallom. Bezpečnostná úroveň segmentu siete bude rovnaká ako v prípade siete TISo a bude konfigurovaná plne v réžii Obstarávateľa. Server bude automaticky zbierať v súboroch uložené dáta zo siete TISo, spracovávať ich do formátu vhodného na import do modulu RT/archívu a následne daný import riadiť (spojenie bude výhradne iniciované zo servera pre zber dát).

Základné vlastnosti zberu dát zo súborov:

- pre zber údajov budú využívané štandardné protokoly pre prenos dát po sieti,
- tam kde je to možné sa použije šifrovaná komunikácia,
- výsledné dáta budú prenášané do archivačného systému šifrovaným protokolom,
- systém zberu bude prebiehať plne automaticky s možnosťou parametrizácie zamestnancami obstarávateľa,
- importované súbory s údajmi a exportované údaje budú ukladané na disku, bude parametrizovateľná ich hĺbka archivácie. Obstarávateľom je preferovaná komprimácia súborov.

[Príklad:

Server pomocou skriptov zabezpečí periodické sťahovanie súborov s dátami (inkrementálne txt alebo celé súbory MS Access). Po ich spracovaní budú tieto vstupné súbory odložené do samostatného adresára. Podľa nastavených parametrov prebehne ich automatická komprimácia a súbory staršie ako požadovaná hĺbka archivácie budú automaticky vymazané.

Výstupné súbory budú spracované do formátu vhodnej pre import do modulov RT/ Archív. Server pre zber dát bude priamo riadiť ich prenos. Výstupné súbory budú archivované na disku počas stanoveného obdobia (parametrizovateľné) pre prípad potreby opätovného importu do RT/ Archívneho modulu a následne automaticky vymazané.]

- V automatickom režime bude systém zberu blokovať opätovné spracovanie časového intervalu spracovaných zbieraných údajov, toto bude umožnené len po manuálnom zásahu administrátora.
- Zdrojový kód všetkých programov vyvinutý pre obstarávateľa bude zdokumentovaný a odovzdaný s možnosťou jeho úpravy aj tretími stranami (vlastníctvo vzniknutého kódu prejde na Obstarávateľa).
- Server bude zasielať do APM správu o úspešnosti zberu dát a jednotlivých svojich moduloch v pravidelných intervaloch (heartbeat)

3.1.4 Softvérová podpora

APM Dátový koncentrátor je plánované používať minimálne po dobu 7 rokov. Počas celej životnosti dátového koncentrátora je požadovaná technická podpora dodávateľa (nadstavbová softvérová podpora počas plánovanej životnosti). Technická podpora musí byť zameraná na funkčnosť a stabilitu systému, aktualizáciu a opravu systémových chýb, udržiavanie systému tak, aby spĺňal požiadavky na spoľahlivosť a kybernetickú bezpečnosť.

Podpora APM Dátového koncentrátora musí zahŕňať SW licencie na obdobie 4 rokov:

- Podporu obstarávateľa pri inštalácii aktualizácií antivírusov, antimalware a firewallov v rámci centrálnej infraštruktúry,
- Podporu obstarávateľa pri inštalácii patchov (záplat) na všetky dodané softvéry.

Podpora APM Dátového koncentrátora nezahŕňa:

- prechod všetkých dodaných softvérov na nové, resp. vyššie verzie, ak to nie je nevyhnutné z dôvodov aktualizácii VMWare a OS.

Detailné požiadavky na poskytovanie technickej podpory pre systém APM Dátový koncentrátor (SLA) sú uvedené v kapitole 7.

3.1.5 Príprava komponentov na APM službu

Pod pojmom APM služba treba rozumieť nadstavbu, ktorá nie je súčasťou predmetu obstarávania **(cloud riešenie APM služby je vylúčené z technického riešenia)**. V budúcnosti bude využívať dáta APM Dátového koncentrátora s nasledujúcimi funkcionalitami:

- extrahovanie online dát z APM Dátového koncentrátora,
- importovanie offline dát z užívateľského rozhrania APM služby,
- analyzovanie údajov pomocou širokej škály nástrojov,
- integrácia a konfigurácia výkonnostných modelov SEPS alebo tretích strán,
- generovanie odporúčaní založených na analytike,
- vytvorenie viacerých dashboardov užívateľmi,
- upozornenie užívateľov na kritické zmeny stavu zariadení.

Ponúkané riešenie musí byť perspektívne rozšíriteľné o túto nadstavbovú službu.

3.2 Hardvérová časť

Hardvér bude zabezpečovať obstarávateľ formou integrácie APM dátového koncentrátora do centrálnej infraštruktúry SEPS.

4 Architektúra systému

Táto špecifikácia koncepčne rozdeľuje systém APM Dátový koncentrátor na „modulové" systémy, ktoré zahŕňajú systémy v pracujúce reálnom čase RT, archivačné a podporné systémy v jednej geografickej lokalite, ktoré zahŕňajú:

- modul pre komunikáciu v reálnom čase (RT modul),
- archivačný modul,
- server pre zber dát zo súborov.

Pracovné stanice (klientske aplikácie) musia umožňovať spustenie konzoly všetkých systémových komponentov v závislosti na pridelených užívateľských právach a stave systému. Projekt navrhovaného systému musí byť dostatočne flexibilný, aby umožnil obstarávateľovi reorganizáciu konfigurácie prípadne zmenu umiestnenia systému. Dodávka špecifických

staníc nie je požadovaná, budú využité štandardné pracovné stanice Obstarávateľa zapojené v sieti SEPS.

4.1 Modul pre realtime komunikáciu (RT modul)

Kompetencie užívateľa sú rozdelené podľa oblastí zodpovednosti do užívateľských rolí. Z funkčného hľadiska modulu RT sú kompetencie rozdelené na užívateľské, administrátorské a monitorovacie prístupové práva.

4.1.1 RT modul a zber hodnôt

Prevádzku zariadení elektrizačnej sústavy musí monitorovať špecializovaný počítačový systém pracujúci v reálnom čase. Užívateľské rozhrania musia umožňovať multifunkčné, plne grafické zobrazenia.

Tento počítačový systém bude plniť nasledovné úlohy:

- zobrazenie aktuálneho prevádzkového stavu monitoringov a zariadení elektrizačnej sústavy v reálnom čase,
- spracovanie získaných hodnôt v reálnom čase,
- komplexný prístup k hodnotám,
- užívateľské zobrazenia sú organizované vo forme okien, ktoré musia mať intuitívne a jednoduché ovládanie s integrovaným ovládaním všetkých funkcií.

Systém bude získavať hodnoty v reálnom čase:

- pravidelným zhromažďovaním (tzv. polling) (vzťah master-slave medzi RT modulom a zdrojom hodnôt),
- automatickým zberom hodnôt (peer-to-peer),
- zberom hodnôt na požiadanie
- zberom hodnôt z externých IS.

4.1.2 Základné spracovanie získaných hodnôt

Aby mohol počítačový systém vykonávať spoľahlivé monitorovanie zariadení elektrizačnej sústavy, musí podporovať spracovanie nasledovných základných typov hodnôt:

- stavové hodnoty (jednobitové a dvojbitové),
- analógové hodnoty,
- vypočítané hodnoty,
- ručné vstupy hodnôt,
- hodnoty odvodené z aplikácií,
- historické hodnoty,
- plánované/predikované hodnoty,
- hodnoty s časovou značkou (vyššie uvedené typy môžu zahŕňať aj časovú značku),
- monitorovacie správy týkajúce sa softvéru,

Hodnoty s časovou značkou majú čas hodnoty pridelený v jednotlivých pripojených zariadeniach alebo systémoch. Hodnotám bez časovej značky musí systém v čase príchodu doplniť časovú značku (systémový čas).

4.1.3 Zoznam príznakov hodnoty

Každá hodnota musí obsahovať niekoľko príznakov (časová značka a kvalitatívne príznaky) napríklad:

- aktuálna procesná hodnota,
- neplatná hodnota,
- neaktualizovaná hodnota
- ručný vstup hodnoty,
- aktualizácia hodnôt nedovolená (zastavenie/zablokovanie aktualizácie),
- vypočítaná hodnota,
- hodnota mimo dovoleného rozsahu,

V systéme musí byť implementované príslušné mapovanie príznakov hodnoty (pre jednotlivé kanály modifikovateľné) týkajúcich sa komunikačného protokolu.

Všetky kvalitatívne príznaky, ktoré sa vzťahujú na nejaký bod, budú v databáze vedené pre tento bod a budú prístupné pre zobrazenie, zaradenie do reportov, zoznamov a pre použitie systémovými funkciami. Typicky bude v zobrazení, zobrazení alarmov, reporte, zozname prezentovaný iba najprísnejší príznak. Bude však možné jednotlivo sprístupniť a prezentovať najprísnejší príznak a všetky príznaky. Systém bude poskytovať obstarávateľovi schopnosť špecifikovať poradie príznakov kvality, ktoré bude použité v celom systéme. Príznak kvality vypočítanej hodnoty bude najprísnejším príznakom kvality argumentov.

Kvalitatívne príznaky zdrojov hodnôt používajúcich štandardné protokoly, ako sú IEC 60870-5-104, IEC 60870-5-101, MODBUS (RTU/TCP), budú zmapované do príznakov kvality systému. Podobne, hodnoty prenesené zo systému do iných počítačových systémov zmapujú kvalitatívne príznaky systému do príznakov kvality výstupného rozhrania (REST API).

Kontrola primeranosti - možnosť monitorovania primeranosti hodnoty analógového údajového bodu vzhľadom k jeho technicky prípustným hodnotám (definovaných parametrom). Zistenie porušenia takéhoto parametra môže spustiť príslušný alarm.

Každá analógová hodnota bude porovnaná so súborom vopred definovaných a nastaviteľných limít, ktoré budú jednotlivo definovateľné pre každý údajový bod. Zistenie porušenia limitu musí spustiť príslušný alarm. Bude zabezpečená aj indikácia návratu do normálu, keď sa alarmová podmienka vráti do normálu.

4.1.3.1 Podpora ručných vstupov

Systém musí podporovať pre používateľa jednoduché zadávanie ručných vstupov hodnôt. Manuálne zadané hodnoty budú vybavené náležitou identifikáciou príznakov a operátora. Príznaky musia byť vhodne zobrazené. Ručné vstupy hodnôt budú vystupovať v systéme rovnako ako všetky ostatné hodnoty.

4.1.3.2 Signalizácie a alarmy

V systéme musia byť ľahko definovateľné rôzne typy alarmovej indikácie (blikanie, nastavenie do rôznych záznamov, zoznamy, aktivácia iných funkcií, archivácia (pri súčasnom zohľadnení oblastí zodpovednosti, ako aj postupov pre potvrdenie) a pod.). Alarmové správy je možné potvrdzovať jednotlivo a aj hromadne.

Prerušenie realtime komunikácie je zobrazené:

- ako záznamy v zozname alarmov,
- primeraná reprezentácia na zobrazení monitoringu komunikácie,

- primeraná reprezentácia na užívateľskom zobrazení (s hodnotami z danej komunikácie).

V zoznamoch alarmov a zobrazeniach alarmov musí byť potvrdenie implementované pre jednotlivé alarmy ako aj pre všetky viditeľné alarmy v tomto zobrazení.

4.1.4 Tvorba a práca s alarmami

Odsek popíše spôsob práce s alarmami z hľadiska typov alarmov z hľadiska konfigurácie, blokovania reprezentácie alarmu, spracovanie alarmov a ukladanie alarmov.

4.1.4.1 Blokovanie reprezentácie alarmu

Systém musí umožňovať blokovanie akejkoľvek aktivácie alarmu používateľom s príslušnými prístupovými právami. Toto blokovanie môže byť aplikovateľné na celý systém (pre všetkých používateľov súčasne), alebo len na daného používateľa, ktorý toto blokovanie vykonal.

4.1.4.2 Jednoduchá konfigurácia alarmov

Funkcionalita alarmov musí umožniť, aby boli typy alarmových správ, ktoré vstupujú do systému, zaznamenané a primerane archivované. Postup definovania vykonaný používateľom, ako aj postup modifikácie alarmu musí byť jednoduchý na definovanie toho, ako je indikovaná zmena stavu, prekročenie limitu.

Alarmy musia byť v systéme členené minimálne na:

- výstraha,
- alarm.

4.1.5 Prideľovanie prístupových práv

Prideľovanie prístupových práv musí byť dynamicky prispôsobované jednotlivým používateľom.

Systém musí podporovať vytváranie typizovaných používateľských rolí. Pod používateľskou rolou sa rozumie súbor funkcionality, ktorá prináleží danému typu používateľa.

Pre každú používateľskú rolu bude možné definovať súbor objektov, ktoré budú pre všetkých používateľov s danou používateľskou rolou dostupné v rámci celého systému APM Dátový koncentrátor . V rámci riadenia prístupu k objektom bude pre každý objekt možné nastaviť nasledovný typ práv:

- bez prístupu – používatelia s danou rolou nebudú mať k dispozícii daný objekt.
- čítanie – používatelia s danou rolou budú mať k dispozícii daný objekt len na prezeranie.
- modifikácia – používatelia s danou rolou budú môcť meniť hodnoty, kvalitatívne príznaky a ostatné atribúty daného objektu.

4.1.6 Upozornenia na udalosti v systéme

Systém musí obsahovať funkcionalitu upozornení na udalosti v systéme. Táto musí umožniť nastaviť na akúkoľvek udalosť v systéme (zmenu hodnoty databázového bodu, zmenu alarmu, zmenu stavu servera, iného zariadenia, ...) výstražné upozornenie.

Každé upozornenie je možné prezentovať nasledovnými spôsobmi (aj súčasne):

- otvorením upozornenia na obrazovke konzoly systému,
- zaslaním e-mailu na definovaný zoznam príjemcov,

Upozornenia sa musia zasielať:

- periodicky v čase (s možnosťou definovania časovej periódy správcom systému),

- periodicky podľa počtu (s možnosťou definovania minimálneho počtu upozornení, ktoré sa majú zaslať súčasne správcom systému),
- vždy pri vytvorení upozornenia.

Všetky upozornenia musí mať možnosť vytvárať správca systému a používatelia s príslušnými prístupovými právami.

4.2 Archivačný modul

- Archivovanie hodnôt - ukladanie a vyhľadávanie informácií

Systém musí podporovať kompletné konfigurovanie všetkých typov archivovania všetkých údajových bodov. Hodnoty môžu byť získané z nasledujúcich zdrojov:

- komunikácie v reálnom čase,
- výsledky aplikačného programu,
- ručné vstupy hodnôt,
- hodnoty importované zo súborov (XML, CSV, TXT, ASCII, MDB)
- komunikačné rozhrania pre výmennú dát (napr. REST API).

Archivačný systém by mal podporovať archiváciu týchto typov hodnôt:

- Momentálna / aktuálne platná hodnota (z komunikácie),
- Maximálna, minimálna a priemerná hodnota v špecifikovanom časovom intervale (napr. 1 minúta, 15 minút, 1 hodina, 1 deň, 1 mesiac). Systém musí ukladať hodnoty v špecifikovaných časových intervaloch (definovateľné parametre pre údajový bod ale aj ako súbor hodnôt) do archivačnej databázy.
- Kalkulované hodnoty z archivovaných hodnôt podľa definovaných vzorcov (požadujú sa: aritmetické operácie +/-, *, /, logické operácie AND, OR a podmienky if, <, =,>, else, výraz vo forme skriptu). Požaduje sa automatický prepočet hodnôt pri ručnej zmene niektorej vstupnej veličiny. Vypočítané hodnoty budú vystupovať v systéme rovnako ako všetky ostatné hodnoty.
- Odvodené archívy - z každého zdrojového archívu veličiny musí byť možné vytvoriť odvodené archívy v špecifikovaných intervaloch (napr. 1 min, 15 minút, 1 hodina, 1 deň, 1 mesiac, 1 rok), ktoré musí systém automaticky ukladať do archivačnej databázy.

- Archivovanie príznakov

Systém musí vedieť ukladať / archivovať aj všetky príslušné príznaky hodnoty. Spúšťacia udalosť, ktorá iniciovala zber hodnôt, musí byť uložená s príslušnou časovou značkou.

- Spätný prepočet hodnôt

Systém zároveň musí podporovať spätný prepočet už uložených odvodených, teda počítaných archívnych hodnôt:

- na požiadanie,
- za zvolené obdobie,
- pri dodatočnej zmene zdrojovej hodnoty.

- Archivácia udalostí v systéme

Systém musí podporovať archiváciu všetkých udalostí (zmeny hodnôt, alarmy) v systéme na zmenovom princípe. Následne musí umožniť ich zobrazenie, filtrovanie, vyhľadávanie, ...

- Monitorovanie zmien hodnôt v archívnej databáze

Každá ručná zmena hodnoty v archívnej databáze musí byť monitorovaná a zaznamená. Každý záznam musí obsahovať identifikačný kód užívateľa, čas zmeny hodnoty, pôvodnú a novú hodnotu.

- Údajová architektúra

Dodávateľ poskytne štruktúru všetkých databáz použitých v rámci systému APM Dátový koncentrátor a jeho archivačného systému (napr. databáza reálneho času a archívna relačná databáza).

Súčasťou riešenia musí byť dodaná knižnica štandardných prístupových programov na prepojenie databáz s ostatnými komponentmi systému. Tieto štandardné prístupové programy môžu byť použité ako generické API pre databázový prístup.

- Grafický nástroj na údržbu databázy

Musí byť k dispozícii nástroj údržby, v ktorom bude navigácia založená na grafickom prehliadači s prehľadnou štruktúrou, ktorý súčasne sprístupňuje štruktúru a hodnoty. Takýto navigačný prostriedok musí podporovať monitorovanie údajov, zadávanie údajov, zmenu atribútov a iné spracovanie údajov. Tento prostriedok môže byť použitý aj na zmenu DB štruktúry, doplňovanie, vymazanie, presun a úpravu údajových bodov v DB.

- Tvorba a správa databáz

Nástroje dodávateľa pre tvorbu a správu databáz musia podporovať tvorbu a údržbu všetkých databáz v rámci APM Dátový koncentrátor. Funkcionalita tvorby a správy databáz musí akceptovať interaktívne užívateľské príkazy v grafickom prostredí, napr. kopírovanie konfigurácie objektov, export/import konfigurácie, premenovanie prvku, zobrazenie vzťahov medzi objektmi (dependency). Všetky zápisy do konfiguračnej databázy musia byť kontrolované z hľadiska platnosti (validita) a referenčnej integrity. Všetky úpravy databáz musia byť zaznamenávané do záznamu úprav (logu). APM Dátový koncentrátor musí zabezpečovať schopnosť identifikovať pre správcu databázy všetky odkazy na vybratý databázový objekt. Všetky parametre v systéme APM Dátový koncentrátor budú definované v databáze a nastaviteľné obsluhou a používateľmi systému v grafickom rozhraní. Všetky softvérové parametre musia byť nastaviteľné pracovníkmi obstarávateľa.

- Archivne údaje a ich objem

Modul pre ukladanie a archiváciu údajov musí byť súčasťou kompletného systému. Pre základné škálovanie výkonnosti modulu ukladania a archivácie údajov možno použiť hodnoty z nasledujúcej tabuľky.

Minimálny požadovaný súbor údajov na uloženie a archiváciu:

Časová hĺbka archivácie [deň]			
Typ hodnôt	Počet bodov	Časová hĺbka archivácie do minulosti[deň]	Časová hĺbka archivácie do budúcnosti [deň]
Primárne / zdrojové – analógové, digitálne	45 000	1*365	1*365
Odvodené, s periódou 1 minúta	50000	1*365	10*365

Odvodené, s periódou 15 minút	25 000	5*365	10*365
Odvodené, s periódou 1 hodina	25 000	10*365	10*365
Odvodené, s periódou 1 deň	1 000	30*365	10*365

Tabuľka 4-1: Minimálny požadovaný súbor údajov na uloženie a archiváciu

Odvodené:

- štatistiky (priemer, minimum, maximum, integrál, stredná hodnota, ...),
- výpočty nad primárnymi dátami (obecný výraz, maskovanie hodnoty, ...).

Súčasťou projektu je aj úvodná migrácia dát v hĺbke uvedenej v tabuľke 4-1.

4.3 Rozhrania APM dátového koncentrátora

4.3.1 Užívateľské rozhranie HMI

Užívateľské rozhranie (HMI) musí byť dodané ako plne grafický produkt spĺňajúce požiadavky normy ANSI/ISA-101.01-2015 (Human Machine Interfaces for Process Automation Systems).

- Základné vlastnosti HMI
  - Informačný systém na báze práce s oknami, ktorý umožňuje súčasné prehliadanie viacerých okien na rovnakej zobrazovacej jednotke
  - zobrazovanie v oknách - súčasné zobrazenie viacerých okien na pracovnej ploche zloženej z viacerých monitorov,
  - použitie viacmonitorovej techniky pre pracovné stanice,
  - použitie dialógov, menu, základného výberového okna, rýchlej voľby (poke points), tlačidiel, hot spots, roletového/pull-up menu a ikoniek pre komunikáciu používateľa.
- Jednotnosť a štandardizovanosť

Celkový zobrazovací formát zobrazovacej jednotky (monitora) musí byť štandardizovaný do takej miery, aby mali polia/okná, v záujme efektívnej prevádzky, rovnaký vzhľad. Po prihlásení/odhlásení používateľa do/zo systému sa musia zobraziť vopred definované štandardné zobrazenia, ktoré budú závislé na užívateľských rolách.

Aby sa zabránilo neúmyselnej, neoprávnenej činnosti, prístup do zobrazení, interaktívnych okien a výberového menu musí korelovať s odpovedajúcim prístupovým právom aktuálneho používateľa.

- Jazyk v HMI

Všetky HMI musia byť v slovenskom jazyku s tým, že výnimky súvisiace s administratívnymi zobrazeniami budú dohodnuté počas implementácie.

- Logovanie činnosti používateľa

Každá činnosť užívateľa a administrátora (prihlásenie, odhlásenie, potvrdenie alarmu, atď.), ktoré môžu ovplyvniť proces, stav zariadenia, musí byť zaznamenaná v monitorovacej databáze.

4.3.2 Užívateľské rozhrania systému APM koncentrátor

Hlavným rozhraním je grafické zobrazenie, ktoré integruje všetky časti systému APM dátový koncentrátor. Grafické rozhranie musí umožniť intuitívne a pre používateľa optimálne zobrazenie všetkých typov údajov. Každý typ údajov je možné zobraziť primerane a nezávisle

na jeho zdroji (ako numerickú hodnotu, ako grafickú indikáciu, vo forme časového diagramu a pod). Rovnakým spôsobom majú byť spracovávané stavové údaje počítačov, komunikačné podsystémové údaje a iné systémové údaje.

- Hlavné okno aplikácie

Základné výberové okno ako kľúčový prvok HMI musí:

- byť užívateľsky čo najprívetivejšie,
- vždy zobrazovať špecifické informácie (logo SEPS, dátum a čas),
- podporovať jednoduchý a rýchly prístup ku všetkým zobrazeniam, zoznamom, funkciám a aplikáciám,
- byť prispôsobené potrebám prihlasujúcich sa špecifických používateľov (v závislosti od typu používateľa sa zobrazia zvolené prvky a ovládacie tlačidlá),
- byť prispôsobené potrebám prihlasujúcich sa aplikačných používateľov, administrátorov, ... (v závislosti od typu užívateľskej role).

- Užívateľské zobrazenia (počet v rámci dodávky 20)

Obsah jednotlivých užívateľských zobrazení bude zadefinovaný v rámci detailného návrhu riešenia odsúhlaseného Obstarávateľom.

- Správa reportov

Užívateľské rozhranie musí poskytovať účinný a jednoduchý nástroj na prácu s reportami. Používateľ musí mať možnosť rýchlo a jednoducho vybrať report a spustiť jeho vytváranie na jeho pracovnej stanici s využitím kancelárskeho SW pracovnej stanice (prednostne MS Office). Generovanie reportov musí rešpektovať privilégia používateľa.

4.3.3 Rozhranie pre správu systému / administráciu

Popri požiadavkách týkajúcich sa rozhraní pre aplikácie APM Dátový koncentrátor musí rozhranie pre správu systému podporovať aj nasledovné funkcie:

- parametrizácie SW, systému a komunikácií,
- parametrizácie RT modulu, databáz, aplikácií (vkladanie, mazanie a modifikovanie parametrov),
- tvorba a manipulácia so zobrazeniami,
- tvorba reportov a manipulácia s nimi,
- tvorba bezpečnostných záloh systému,
- iné administratívne a prevádzkové monitorovanie systému.

Systém musí umožniť realizovať všetky štandardné konfiguračné činnosti pre samotný systém ako aj pre rozhrania na partnerské vnútropodnikové systémy z konfiguračného nástroja dodaného k systému bez nutnosti realizovať parametrizáciu na viacerých miestach v dodanom systéme (priamo cez aplikáciu alebo formou odkazu na konfiguračný súbor).

Systém bude podporovať hromadné vytváranie a úpravy konfigurácie databázových bodov (aj s využitím exportu/importu konfiguračných súborov)

- Monitorovanie príslušných komponentov a funkčných skupín

Systém musí plne podporovať efektívne monitorovanie za účelom riadenia systému APM Dátový koncentrátor. Stav systému musí byť zobrazený pomocou HMI nasledovne:

- musí poskytovať celkový prehľad konfigurácie systému, monitorovanie modulov a stavu komunikácie so všetkými pripojenými zariadeniami,

- jednotlivé informácie sa musia zobrazovať v príslušných prehľadoch, zoznamoch a zobrazeniach alarmov.

4.4 Podporné aplikácie

Systém APM Dátový koncentrátor musí byť prevádzkovaný na štandardnom operačnom systéme tretej strany (napr. MS Windows Server, Red Hat,...). Softvér operačného systému bude štandardným produktom a dodávateľ ho neupraví. Ak áno, dodá postup úprav ako súčasť plánu obnovy.

- Zdrojové kódy systému a kompilátory

Dodávateľ dodá zdrojové kódy nad rámec štandardného SW a príslušné kompilátory vrátane oprávnenia na ich modifikáciu Obstarávateľom alebo Obstarávateľom určenými tretími stranami.

- Systémové služby

Sieťové súborové služby budú poskytovať používateľom systému prístup k súborom z vyhradených miest v sieti obstarávateľa.

Prístup k súborom bude obmedzený prideľovaním užívateľských výhradných práv, vrátane minimálne žiadneho prístupu, čítania, zapisovania, vykonávania a ich kombinácií.

Súbory systému musia byť prístupné až po autentifikácii používateľa. Prístup bez autentifikácie (guest, everyone) bude odmietnutý. Používateľ musí disponovať iba minimálnymi právami na súbory, ktoré sú nevyhnutné pre vykonávanie jeho pracovnej činnosti.

Služby systémového plánovania (scheduling) budú obsahovať prostriedok pre plánovanie aplikačnej činnosti na základe dennej doby, obdobia a iných udalostí.

- Aplikácia a vývoj systému (archivačné výpočty)

APM Dátový koncentrátor bude obsahovať iba zdokumentované API a dodávateľ dodá kompletnú dokumentáciu.

Systém APM Dátový koncentrátor musí obsahovať vlastný doplnkový programovací jazyk. Programovací jazyk musí spĺňať podmienku, aby bolo možné program napísať, odladiť a spustiť bez potreby samostatnej kompilácie v inej aplikácii alebo v programe operačného systému a vytvorenia spustiteľného programu (napr. s príponou exe). Programovanie v tomto jazyku musí prebiehať v grafickom prostredí.

Programovací jazyk pre tvorbu aplikačného kódu musí mať minimálne nasledovné vlastnosti:

- umožňuje navrhnúť bezpečný a spoľahlivý kód (jednoduchú syntax, štruktúrované výrazy, podpora dátových štruktúr, kontrola pretypovania premenných),
- podporuje modularizáciu kódu ("podprogramy"),
- obsahuje mechanizmus pre detekciu a reakciu na mimoriadne run-time podmienky ("exception handling"),
- obsahuje jednoducho škálovateľný rozsah hodnôt (bez možnosti pretypovania) znemožňujúci pretečenie (integer, floating-point, fixed-point),
- podporuje štandardné knižnice pre I/O, manipuláciu s textovými premennými, numerické výpočty, polia, prácu s databázovými tabuľkami (vkladanie, zmena, vymazanie, transakcie),
- podporuje súbežný beh programov,
- podporuje možnosť spúšťania programov operačného systému a iných aplikácií,
- podporuje možnosť paralelného spúšťania úloh (periodických, spúšťaných udalosťou) so stanovením time-out,

- možnosť prepojenia kódu s grafickou reprezentáciou (s Grafickým editorom),
- pre výpočty musia byť k dispozícii minimálne nasledovné operátory:
  - štruktúrované podmienené príkazy (CASE, IF, THEN, ELSE),
  - booleovské operácie (AND, OR, NOT, XOR, atď.),
  - porovnávacie operácie (>,>= , = , =<, <),
  - elementárne aritmetické operátory (+, -, *, /),
  - operácie s časom,
  - štatistické funkcie za danú periódu (1 minúta, 15 minút, 1 hodina, 1 deň, ...) ako sú vážený priemer, súčet, maximum, minimum.

Systém musí informovať o syntaxových chybách a umožniť postupné vykonanie úkonov s možnosťou sledovania odpovedajúcich hodnôt jednotlivých premenných.

Počas výpočtu sú príslušné príznaky vstupných hodnôt prenesené do príznakov výsledkov. Prenos príznakov do výslednej hodnoty musí byť výpočtovo konfigurovateľný.

Grafický editor bude podporovať správu systému pomocou kompletnej sady grafických nástrojov a nasledujúcich funkcionalít:

- priamy prístup do konfigurácie všetkých zobrazení, ktoré sú v systéme, možnosť ich vytvárania a modifikácie,
- hodnoty databázových bodov v zobrazeniach môžu byť prezentované zobrazením ich číselnej hodnoty, grafickou zmenou ich vizualizácie na základe hodnoty, textovým poľom meniacim sa na základe ich hodnoty, ... (tieto formy zobrazenia musia byť definovateľné v šablónach),
- podpora konfigurácie prvkov vo viacerých vrstvách zobrazenia a priradenia prvkov k nim,
- podpora tvorby skupín prvkov (umožňuje súčasnú zmenu polohy celej skupiny),
- podpora kopírovania prvkov v rámci zobrazenia, medzi zobrazeniami ako aj kopírovanie celých zobrazení,
- podpora obsluhy udalostí pre jednotlivé prvky zobrazenia (OnClick,...),
- podpora špecifickej obsluhy zobrazení (skriptovací jazyk zobrazenia).

4.5 Súčinnosť SEPS a Integrácia do Centrálnej infraštruktúry SEPS

4.5.1 Integrácia do Centrálnej infraštruktúry SEPS

Systém APM dátový koncentrátor bude integrovanou súčasťou centrálnej infraštruktúry SEPS. Centrálna infraštruktúra SEPS využíva virtuálne prostredie na základe technológie VMWARE. HW zariadenia pre centrálnu infraštruktúru nebudú súčasťou dodávky systému APM dátový koncentrátor. Zhotoviteľ v čase vypracovania detailného návrhu riešenia (minimálne mesiac pred samotnou implementáciou) navrhne požadované parametre virtuálnych serverov, operačných systémov, databázových systémov, sieťovej infraštruktúry a iné požiadavky na centrálnu infraštruktúru SEPS v zmysle technickej špecifikácie. Obstarávateľ využitím prostriedkov centrálnej infraštruktúry SEPS poskytne zhotoviteľovi prístup k požadovaným prostriedkom za účelom následnej inštalácie a odovzdania diela. Inštaláciu virtuálnych serverov a ich operačných systémov (vrátane zabezpečenia licencií zo strany Obstarávateľa) podľa požiadaviek vykoná obstarávateľ v spolupráci so Zhotoviteľom. Za prevádzku centrálnej infraštruktúry je zodpovedný obstarávateľ.

- Navrhovaná schéma konfigurácie systému APM koncentrátor

Zhotoviteľ vypracuje prehľadnú schému kompletného riešenia zobrazujúcu prepojenia virtuálnych serverov systému APM dátových koncentrátor s počítačovými sieťami a jednotlivými zariadeniami vstupných údajov v rámci detailného návrhu riešenia odsúhlaseného Obstarávateľom.

- Diskové pole

Diskové pole potrebné pre aplikačné a archivačné servery bude spĺňať podmienky pre nepretržitú prevádzku, ktorá bude riešená formou redundancie na úrovní HW centrálnej infraštruktúry SEPS.

- Zálohovanie

Pre systém APM dátový koncentrátor bude využité centrálne zálohovanie v rámci centrálnej infraštruktúry SEPS. Zhotoviteľ na základe technických možností a v spolupráci s obstarávateľom navrhne optimálny spôsob zálohovania s využitím prostriedkov centrálnej infraštruktúry SEPS. Preferovaný spôsob zálohovania dát je periodický (každý deň) s možnosťou parametrizácie periódy a spôsobu zálohovania full/incremental.

- Počítačové siete systému APM Dátový koncentrátor

Jednotlivé servery systému APM dátový koncentrátor môžu byť v rámci centrálnej infraštruktúry SEPS rozdelené minimálne do dvoch oddelených segmentov počítačovej siete. Na oddelenie jednotlivých segmentov siete budú slúžiť redundantné firewally obstarávateľa. Detailný návrh sieťovej konfiguráciu bude upresnený počas vypracovania detailného návrhu riešenia a bude sa riadiť podľa požiadaviek a pravidiel kyberbezpečnosti obstarávateľa.

- Bezpečnostná architektúra siete a počítačová bezpečnosť

Dodávateľ poskytne zoznam všetkých potrebných a požadovaných portov, služieb a adries vyžadujúcich prístup cez všetky firewally podporujúce normálne a núdzové funkcie a funkcie prebiehajúcej údržby.

Všetky prístupy implementované počas vývoja systému, továrenských skúšok a skúšok na mieste budú zdokumentované a preskúmané z hľadiska odstránenia pred uvedením systému do prevádzky.

Software APM Dátový koncentrátor bude bezprostredne pred dodaním preskúšaný z pohľadu kritérií bezpečnosti obstarávateľa. Obstarávateľ si vyhradzuje právo delegovať bezpečnostný audit a testovanie (napr. penetračné testy) na nezávislú spoločnosť.

- Odstránenie nepoužitých služieb

Všetky aplikácie, utility, systémové služby, skripty, konfiguračné súbory, databázy, užívateľské účty a celý ostatný softvér, ktorý nie je potrebný pre prevádzku APM Dátový koncentrátor bude pred uvedením do prevádzky odstránený.

- Aktualizácie softvéru a skenovanie vírusov

Všetky aktualizácie operačného systému a aplikačného softvéru, ktoré riešia počítačovú bezpečnosť a kompatibilitu SW komponentov, budú nainštalované v súlade s internými pravidlami obstarávateľa. Dodávateľ v spolupráci s obstarávateľom musí zabezpečiť pripojenie na mechanizmus centralizovanej aktualizácie OS serverov v rámci centrálnej infraštruktúry SEPS.

- Diaľková alebo automatická deaktivácia softvéru

Softvér APM Dátový koncentrátor nesmie obsahovať vložené chyby, skryté (back-door) mechanizmy, ktoré umožňujú dodávateľovi softvéru a inej strane diaľkovo deaktivovať niektoré, prípadne všetky funkcie softvéru, ovplyvňovať ich výkonnosť a akýmkoľvek spôsobom degradovať jeho prevádzku.

Softvér nesmie obsahovať žiadny mechanizmus, ktorý automaticky deaktivuje niektoré, prípadne všetky funkcie softvéru, degraduje ich prevádzku v určitom dni a po vzniku špecifickej udalosti.

- Zistenie neoprávnených úprav softvéru

Dodávateľ bude spolupracovať s obstarávateľom pri zavedení mechanizmu pre pravidelné skenovanie integrity softvéru na diskoch APM Dátový koncentrátor s cieľom určiť, či boli vykonané neoprávnené úpravy softvéru. Podrobnosti budú upresnené počas vypracovania detailného návrhu riešenia.

- Antivírusový softvér a softvér na zisťovanie škodlivého softvéru

Tam, kde je to technicky realizovateľné a kde existujú vhodné komerčné produkty (napr. prostredia Microsoft Windows), dodávateľ v spolupráci s obstarávateľom implementuje systémy na zisťovanie vírusov, spyware a iného škodlivého softvéru vrátane prestupu na aktualizačné servery pre vírusy u obstarávateľa. Typ antivírusového softvéru určí obstarávateľ.

Tieto produkty budú nainštalované a budú bežať počas celého vývoja, skúšania, uvedenia do prevádzky a prevzatia systému s cieľom zabezpečiť, aby bol známy a otestovaný ich dopad na výkonnosť.

- Monitorovanie bezpečnosti

Požadované funkcie monitorovania bezpečnosti:

- APM Dátový koncentrátor zaznamená všetky pokusy o prístup do aplikačného prostredia.
- APM Dátový koncentrátor bude viesť záznamy o systémových udalostiach dostatočne podrobné na vytvorenie historických kontrolných záznamov a umožnenie analýzy koreňových príčin počas obdobia minimálne 90 kalendárnych dní.
- Systém musí podporovať možnosť kopírovania údajov o systémových udalostiach na alternatívne pamäťové médium pre uloženie na dlhšie obdobie ako 90 dní, ak je to požadované ako súčasť dlhodobejšieho vyšetrovania.

Záznamy budú zachytávať pri používateľoch, ako aj aplikačných prístupoch, nasledovné:

- všetky pokusy o prihlásenie, úspešné i neúspešné,
- všetky žiadosti o zmenu výhradných práv, úspešné i neúspešné,
- všetky činnosti používateľov ovplyvňujúce bezpečnosť, ako sú napríklad zmeny hesiel,
- všetky pokusy o sprístupnenie súborov, pri ktorých používateľ nedisponuje dostatočnými prístupovými výhradnými právami,
- pokusy o vykonanie činnosti, ktorú bezpečnostná schéma nedovoľuje,
- dodávateľ systému pristupuje do systému a aplikácie pod svojimi účtami, ktoré sú predmetom uplatňovania bezpečnostnej politiky obstarávateľa.

APM Dátový koncentrátor generuje alarm, keď môže prístupová činnosť indikovať pokusy o získanie neoprávneného prístupu k službám, údajom systému.

- Generické a štandardné účty

Dodávateľ odstráni, deaktivuje (podľa možností technickej realizácie) všetky generické účty, hosťovské účty, účty vývojových prác, účty údržbárskych prác a štandardné účty poskytované hardvérom, operačným systémom, aplikačným programom a inými poskytovateľmi. V prípadoch, kde nie je možné špecifické účty odstrániť, tieto budú premenované, deaktivované, aby sa predišlo neoprávnenému prístupu.

- Autentifikácia používateľov

Systém musí umožňovať prihlásenie užívateľa jedným z nasledujúcich spôsobov: SSO (integrácia s desktop SSO prostredníctvom MS Windows AD - Kerberos), menom a heslom. Výber použitej autentizačnej metódy musí systém umožniť na základe zmeny konfigurácie. V prípade zlyhania autentizácie prostredníctvom SSO (MS-AD účtu užívateľa), systém musí užívateľovi umožniť alternatívne prihlásenie menom a heslom. Autentizačné údaje nesmú byť prenášané a ukladané v otvorenej podobe. V prípade autentizácie na úrovni systému musí systém zaistiť overenie užívateľov v súlade s požiadavkami zákona o kybernetickej bezpečnosti.

- Autorizačný proces

Dodávateľ bude viesť zoznamy všetkých oprávnených pracovníkov s prístupom do APM Dátový koncentrátor počas ich prítomnosti pri implementácii u dodávateľa, vrátane ich špecifických elektronických a fyzických práv do systémov, serverov, databáz a termínu, v ktorom bude prístup ukončený. Obstarávateľ bude informovaný o všetkých zmenách zoznamu účtov jeho oprávnených pracovníkov a ich oprávnení v APM Dátový koncentrátor.

- Zariadenie pre časovú synchronizáciu

Synchronizácia času bude prebiehať ntp protokolom z aktívnych sieťových prvkov obstarávateľa (časový normál).

Vlastnosti synchronizácie

- Systémový čas bude priebežne synchronizovaný s časovým normálom.
- Veľké odchýlky medzi systémovým časom a časovým štandardom budú hlásené a logované. Časová synchronizácia musí byť súčasťou štartovacej procedúry každého servera a to aj v prípade nábehu bez spustenia aplikácií systému APM Dátový koncentrátor.
- Počas poruchy časového štandardu sa systém musí prepnúť na ďalší časový štandard podľa zadefinovaných priorít.
- Automatické spracovanie prechodov na letný/zimný čas a príslušná aktualizácia všetkých funkcií a programov. Bude zabezpečená schopnosť aktivovať, deaktivovať a meniť plánovaný dátum a čas automatického prechodu na letný čas.

- Podpora prístupu vzdialených používateľov

Riadenie prístupu vzdialených používateľov a diaľkový prístup počas implementácie a na údržbu bude prebiehať IT prostriedkami obstarávateľa rešpektujúc zásady bezpečnosti riadenia prístupu v zmysle pravidiel SEPS. Spôsob implementácie bude schválený počas detailného návrhu riešenia.

- Centralizovaná správa systému APM Dátový koncentrátor

Systém APM dátový koncentrátor musí zahŕňať funkciu centralizovanej správy pre správu konfigurácií a monitorovanie zariadení, vrátane serverov, aplikácií a databáz. Nástroje pre správu konfigurácií musia byť integrálnou súčasťou.

- Otvorenosť konfigurácie

V rámci dodávanej funkcionality musí byť taktiež zabezpečená schopnosť doplňovať do schémy správy nové servery a komunikačné zariadenia.

- Detekcia chýb

Všetky chyby a ostatné udalosti zistené funkciou správy APM dátový koncentrátor musia byť zaznamenané a hlásené používateľovi/správcovi systému. Závažné chyby musia byť hlásené v počítačovom prevádzkovom zozname (prehľad prevádzkových alarmov a udalosti).

- Monitorovanie kritických procesov

Systém APM dátový koncentrátor umožní monitorovať všetky kritické procesy a upozorni používateľa, ak je zistený zablokovaný proces. Zistenie kritického procesu, ktorý sa zablokoval, automaticky vyvolá reštart procesu s pokusom o nápravu situácie a prípadný reštart servera. Parametre pre reštart ako počet pokusov reštartu kritických procesov a podmienky reštartu celého servera musia byť plne konfigurovateľné administrátormi systému. Rovnako musí byť možné a parametrizovateľné odoslať správu email-om o poruche akéhokoľvek kritického procesu.

- Monitorovanie a evidencia chýb zariadení a funkcií

Všetky servery a funkcie budú monitorované z hľadiska závažných a opraviteľných chýb. Všetky zistené chyby a poruchy budú zaznamenávané pre účely údržby.

4.5.2 Súčinnosť SEPS

Súčinnosť a protiplnenie SEPS bude poskytnuté formou:

- Dodávka HW a základného SW (virtuálne servery, operačné systémy, databázové servery, antivírusový SW...)
- Konfigurácia sieťových prvkov v sieti IIS a TISo
- Konfiguráciu IEC 60870-5-104 zabezpečí na strane MST Objednávateľ v spolupráci s dodávateľmi MST
- Konfiguráciu potrebných softvérov na strane MSV zabezpečí Objednávateľ v spolupráci s dodávateľmi MSV

5 Komunikácie

Dodávateľ je povinný uskutočniť predimplementačnú analýzu súčasného stavu výmeny dát s okolitým prostredím (monitoringy ....) a výsledky analýzy implementovať do svojho návrhu riešenia.

Procesné údaje sú získavané v systéme APM Dátový koncentrátor prostredníctvom rôznej komunikácie. Implementácia telekomunikačnej siete nie je súčasťou dodávky. Požaduje sa však, aby dodávateľ spolupracoval s obstarávateľom pri testovaní vo všetkých príslušných etapách projektu pri konfigurovaní pripojení do telekomunikačnej siete.

Komunikácia medzi APM dátový koncentrátor a jednotlivými zariadeniami bude výhradne prebiehať cez telekomunikačnú sieť SEPS. V tejto fáze projektu sa počíta s komunikáciou v reálnom čase (IEC 60870-5-104, MODBUS TCP) a zberom dát prostredníctvom súborov. Prepojenie s inými systémami SEPS bude preferovane prebiehať prostredníctvom rozhrania na výmenu dát REST API.

- Všeobecné požiadavky

Systém musí podporovať redundantnú komunikáciu so zdrojmi údajov minimálne pre sériové protokoly. Pre sieťové protokoly je redundancia riešená na úrovni telekomunikačnej siete. V rámci telekomunikačnej siete musí byť schopný systém komunikovať s primárnym zdrojom dát a v prípade výpadku (a dostupnosti záložného zdroja dát) sa systém automaticky prepne na záložný zdroj dát.

Konfigurácia a výkonnosť nového systému APM Dátový koncentrátor musí byť pripravená na zvládnutie rozšírenia existujúcej komunikácie z hľadiska počtu komunikačných kanálov na 100 a existujúceho počtu údajových bodov o 100%.

- Diagnostika komunikácií

APM Dátový koncentrátor bude zabezpečovať minimálne nasledovné schopnosti:

- Monitorovanie a zobrazovanie informácií odoslaných do a prijatých z údajových zdrojov a počítačových systémov,
- Monitorovanie a zobrazovanie stavu údajových komunikačných zariadení,
- Poskytovanie komunikačných štatistík vrátane počtu chýb, opakovaných pokusov, prenesených bytov, atď.,
- Zber údajov prostredníctvom súborov

Obstarávateľ preferuje pri automatizovanom zbere údajov zo súborov využitie štandardných protokolov ako FTP, sFTP.... Tam kde je to možné, bude použitý protokol so šifrovaním dát.

- REST API

V rámci systému sa zrealizuje implementácia samostatných REST API webových služieb určených pre rýchlu výmenu správ. Výmena dát s jednotlivými systémami musí prebiehať šifrovane prostredníctvom prihlásenia menom a heslom. Jednotlivé užívateľské účty pre REST API musia rešpektovať rovnaké pravidlá ako ostatné účty v systéme APM Dátový koncentrátor (práva na prístup k dátam, užívateľské role).

Konfigurácia REST API bude prebiehať v prehľadnom grafickom rozhraní. V grafickom rozhraní bude možné mapovať príznaky výstupných a vstupných dátových bodov.

6 Požiadavky na výkonnosť systému

6.1 Požiadavky na výkon systému

Požiadavky na činnosť systému popísané v tejto časti budú overené počas preberacej skúšky u obstarávateľa (Site Acceptance Test (SAT)). Pre účely špecifikácie výkonu pri rôznych úrovniach aktivity systému, sú definované termíny „ustálený stav" a „stav vysokej aktivity".

Ustálený stav zahŕňa minimálne zber dát cez všetky realtime komunikácii, zber dát zo súborov v štandardne nastavených časoch, odvodené výpočty spracované v štandardných časoch.

Stav vysokej aktivity zahŕňa minimálne zber dát cez všetky realtime komunikácii, zber dát zo súborov v štandardne nastavených časoch, manuálne spustený zber dát za poslednú hodinu, odvodené výpočty spracované v štandardných časoch, spätné prepočty dát za prechádzajúcu hodinu. Konkrétne definovanie stavov pre testovanie výkonu systému bude súčasťou detailného návrhu riešenia. Komunikačný systém musí byť schopný uskutočniť zber údajov v požadovanom čase, tak ako je uvedené v nasledujúcej tabuľke.

Mód	Komunikačný RT modul v ustálenom stave	Komunikačný RT modul v stave vysokej aktivity
Zmena stavu na vstupe zariadenia sa zobrazí na zvolenej schéme	+4,0 s	10,0s
Zmena analógovej hodnoty na vstupe zariadenia s prekročením limity sa zobrazí na zvolenej schéme	4,0 s	10,0 s
Odozva HMI na požiadavku užívateľa (napr. potvrdenie alarmu)	1s	1s

6.2 Redundancia a systém pre vývoj programov, testovanie a patchovanie (VTS)

Obstarávateľom minimálna požadovaná zostava sú 4 virtuálne servery: jeden testovací server (vývojovo testovací server – VTS), server pre RT modul ,archívny server, server zberu dát zo súborov. Obstarávateľ požaduje, aby architektúra systému bola Dodávateľom navrhnutá tak, aby umožňovala nepretržitú prevádzku systému a jeho súčasti bez straty zbieraných dát (s výnimkou dát s možnosťou dodatočnej obnovy). Do nepretržitej prevádzky sa nezapočítava doba potrebná na vykonanie inštalácie bezpečnostných záplat alebo aktualizácii vyvolaných aktualizáciou prvkov centrálnej infraštruktúry SEPS. Architektúra systému musí umožniť testovanie plánov obnovy. Redundancia serverov nie je požadovaná, ak je Dodávateľ schopný navrhnúť architektúru systému umožňujúcu uvedené funkcionality bez redundancie serverov len s využitím technológii centrálnej infraštruktúry obstarávateľa (napr. VMWare Cluster).

Súčasťou dodávky bude dodanie plne funkčného testovacieho prostredia (VTS) vrátane všetkých potrebných produktových licencií určených na testovacie prostredie. Dodávateľ dodá samostatne obrazy virtuálnych serverov pre nasadenie systému v konfigurácii pre testovanie. Systém VTS musí byt nakonfigurovaný tak, aby bolo možné realizovať vývoj a testovanie integračných rozhraní, upgrade funkcionalít, upgrade systémových častí, inštaláciu bezpečnostných záplat a aktualizácii.

6.3 Dostupnosť systému

Dostupnosť sa musí rešpektovať počas obdobia jedného roka (8 760 po sebe nasledujúcich hodín). Do meraného obdobia sa nebude započítavať čas potrebný na údržbu (vynútené reštarty kôli aktualizáciám a pod.).

Ak sa uskutoční test dostupnosti v čase kratšom ako jeden rok, potom je potrebné prepočítanie hodnoty dostupnosti. Systém musí počas testu dostupnosti preukázať meranú dostupnosť 99.5%. Softvér je pokladaný za dostupný, keď všetky funkcie popísané v tejto špecifikácii, fungujú tak, ako je špecifikované, vo svojej plánovanej periodicite a v rámci stanovených časových parametrov.

6.4 Používateľské účty

Systém bude z pohľadu výkonnosti a licenčného pokrytia škálovaný minimálne na rozsah dvoch používateľov s vysokými oprávneniami a 10 bežných užívateľov pri behu minimálne piatich súbežných (concurrent) užívateľov.

7 Poskytovanie technickej podpory pre systém APM Dátový koncentrátor (SLA)

Súčasťou dodávky musí byť okrem dodania vlastného diela, jeho časti, aj poskytnutie technickej podpory na obdobie 4 rokov.

7.1 Definícia pojmov

Kritická porucha je taká, bez ktorej riešenia nie je dielo použiteľné vo svojich základných funkciách teda sa vyskytuje funkčná porucha znemožňujúca činnosť diela. Tento stav môže ohroziť bežnú prevádzku zadávateľa, prípadne môže spôsobiť preukázateľné finančné alebo iné škody. Niektoré príklady situácií, kedy vznikla Kritická porucha sú:

- zastavenie systému,
- neplnenie povinností vyplývajúcich z legislatívy a zmluvných záväzkov obstarávateľa,
- zlyhanie funkčnosti systému spôsobuje stratu dát,
- zlyhanie funkčnosti systému spôsobuje výpadok poskytovania dát tretím stranám,
- chyba v systéme neumožňuje spustenie, pokračovanie behu softvérových aplikácií,

- je identifikovaná možnosť porušenia bezpečnostného zabezpečenia.

Podstatná porucha je porucha, bez riešenia ktorej je dielo vo svojich funkciách degradované tak, že tento stav obmedzuje bežnú prevádzku a prevádzku HighAvailability a DisasterRecovery riešení. Niektoré príklady situácií, kedy vznikla Podstatná porucha sú:

- zhoršená, porušená funkčnosť so značným vplyvom na beh aplikácie,
- časté zlyhanie aplikácie, ktorá ale nespôsobuje stratu údajov,
- vážne, ale predvídateľné, zlyhanie systému,
- zlyhanie jedného prvku v rámci redundantného riešenia,
- značná degradácia výkonových parametrov systému.

Ostatná porucha je porucha, ktorá svojou povahou neobmedzuje bežnú prevádzku (spôsobuje pokles používateľského komfortu). Niektoré príklady situácií, kedy vznikla Ostatná porucha sú:

- chyby, ktoré majú obmedzený, ale nie priamy dopad na výkon a funkčnosť aplikácie,
- chybná funkčnosť s obmedzeným dopadom.

Odstránením poruchy sa rozumie stav, keď dodávateľ odstráni poruchu a vykoná funkčné testy, na základe ktorých preukázateľne a oprávnene dospeje k záveru, že porucha je odstránená. Táto skutočnosť musí byť protokolárne potvrdená oprávnenou osobou obstarávateľa.

Zoznam a špecifikácia SW vybavenia, ktorých sa týka služba technickej podpory a profylaktiky, bude podrobnejšie rozčlenená v prílohe zmluvy o poskytovaní tejto služby.

- Incident manažment

Pre účely tejto Zmluvy definuje Objednávateľ kontaktné osoby, ktoré sú oprávnené zadávať incidenty aplikácii APM Dátový koncentrátor. Incidenty sú zadávané do Service Desku Objednávateľa, pričom zadávateľ zároveň určí aj kategóriu problému. Service Desk potom štandardným spôsobom odošle informáciu o incidente Zhotoviteľovi, ktorý je povinný potvrdiť Objednávateľovi jeho prijatie, a podľa kategórie zahájiť jeho riešenie. Zároveň Zhotoviteľ oznámi Objednávateľovi aj meno a kontakt zodpovedného riešiteľa problému.

7.2 Servisné činnosti v rámci fixne poskytovaných služieb

7.2.1 Technická podpora pre kompletné programové vybavenie

Táto služba musí zahŕňať všetky práce spojené s udržiavaním programového zariadenia (SW) v prevádzkyschopnom stave, ako aj odstraňovanie prípadných porúch v stanovenom čase a aktualizácie systémov z dôvodu kybernetickej bezpečnosti.

Bude tvorená udržiavacími poplatkami (Maintenance Fee) za základné programové vybavenie systému dodané Zhotoviteľom APM dátový koncentrátor, aplikačné programové vybavenie a programové vybavenie tretích strán.

Po nahlásení chyby dodávateľ musí vykonať analýzu problému a spôsob riešenia odkonzultovať so zodpovedným pracovníkom obstarávateľa. V prípade potvrdenia poruchy bude dodávateľ povinný do 24 hodín, resp. nasledujúce pracovné dni (podľa nasledujúcej tabuľky), zaslať detailný popis príčin poruchy a spôsobu jej odstránenia. Uvažovaná podpora sa týka aj programového vybavenia tretích strán.

Spôsob nahlasovania porúch bude k dispozícii nepretržite 365 x 24 hodín pre oprávnených pracovníkov obstarávateľa podľa definovaných pravidiel do Service Desku Objednávateľa.

Požadované garantované reakčné časy na začatie vykonávania servisnej služby a na odstránenie SW poruchy od jej nahlásenia v závislosti od závažnosti poruchy sú uvedené v nasledovnej tabuľke:

	Kritické poruchy	Podstatné poruchy	Ostatné poruchy
1.Reakčný čas na začatie vykonávania servisnej služby	4 hod	8 hod	72 hod
2.Odstránenie poruchy formou funkčného dočasného riešenia	24 hod	2 PD	5 PD
3. Analýza príčin, implementácia opráv SW vybavenia a úplné odstránenie poruchy	72 hod	5 PD	15 PD

Význam skratiek: PD – pracovný deň

Začatie vykonávania servisnej služby: buď fyzická prítomnosť alebo diagnostika vzdialeným prístupom iba cez prostriedky Objednávateľa pre vzdialený prístup podľa interných smerníc.

Ak bude porucha natoľko komplikovaná, že jej odstránenie si z objektívnych dôvodov ako aj z dôvodov vyššej moci (živelná pohroma apod.) vyžiada čas dlhší ako je definované v tabuľke, dodávateľ musí oznámiť túto skutočnosť obstarávateľovi a požiada ho o predĺženie doby na odstránenie poruchy. Dodávateľ následne zabezpečí odstránenie poruchy v dohodnutom termíne.

Príklady SW porúch jednotlivých kategórií:

- Kritická chyba – nefunkčnosť jedného zo modulov RT, Archív
- Podstatná chyba - nefunkčnosť importu ...
- Ostatná chyba – iné chyby neohrozujúce prevádzku

7.2.2 Profylaktická kontrola a údržba programového a technického vybavenia

Servisné úkony v rámci profylaktickej údržby činnosti systémov, zamerané na optimalizáciu ich činnosti vrátane zabezpečenia ich bezporuchového chodu, budú vo všeobecnosti zamerané na profylaktickú kontrolu základného a aplikačného programového vybavenia systému APM dátový koncentrátor.

Profylaktická kontrola základného a aplikačného programového vybavenia musí byť zameraná na:

- kontrolu funkčnosti a optimálneho chodu informačného systému APM dátový koncentrátor,
- kontrolu vyťaženosti a chybovosti základného programového vybavenia systému,
- kontrolu vyťaženosti a chybovosti aplikačného programového vybavenia systému,
- kontrolu konzistentnosti databáz,
- kontrolu režimu zálohovania, vrátane kontroly konzistentnosti dát v archívnych databázach.

V rámci vykonávania tejto servisnej služby (profylaktika SW) musia byť dodávateľom vypracované postupy (po schválení Obstarávateľom) a ich okamžitá realizácia dodávateľom pre optimalizáciu činnosti systému.

Táto kontrola sa musí vykonávať v pravidelných intervaloch, 2x ročne. Výstupom z tejto kontroly bude protokol o vykonaní kontroly s popisom kontrolovaných častí, nájdených chýb a popisom vykonaných prác pri odstraňovaní zistených chýb chodu systému.

Prevádzkový monitoring nad aplikáciami APM Dátový koncentrátor bude riešený prostredníctvom aplikácie Zabbix (komplexné open source softvérové riešenie monitorovania dostupnosti a výkonu IT infraštruktúry). Bezpečnostný monitoring nad aplikáciami bude riešený prostredníctvom aplikácie SIEM.

7.2.3 Aktualizácia dodaného programového vybavenia

Dodávateľ sa zaväzuje priebežne a operatívne pravidelne zisťovať dostupnosť opráv SW. Dostupnosť hlásiť Obstarávateľovi a dohodnúť inštaláciu. Funkčné opravy hlásiť do 7 dní, kritické do 24 hodín. Na základe dohody s Objednávateľom následne dodávateľ bude testovať a inštalovať nové verzie dodaného programového vybavenia. Táto požiadavka sa vzťahuje jednak na APM dátový koncentrátor (prípadne jeho časti) ako aj na kompletné programové vybavenie, teda aj, systémové patche, antivírové programy, bezpečnostné opravy SW, zmeny operačného systému. Všetky tieto úpravy SW, musia byť pred implementáciou dodávateľom vopred otestované jeho špecialistami.

7.2.4 Aktualizácia a testovanie plánu obnovy

Dodávateľ sa zaväzuje priebežne aktualizovať plán obnovy systému APM Dátový koncentrátor a jedenkrát ročne po odsúhlasení Obstarávateľa vykonať test plánu obnovy.

7.2.5 Aktualizácia dokumentácie

Dodávateľ sa zaväzuje priebežne aktualizovať dokumentáciu systému APM Dátový koncentrátor, ak je vyvolaná poskytovaním technickej podpory podľa kapitoly 7.

7.3 Služby na vyžiadanie

Služby na vyžiadanie sa budú týkať úprav existujúcej funkcionality, ako aj doplnenia nových vlastností aplikačného programového vybavenia a konfigurácií existujúceho technického riešenia v nadväznosti na nové prevádzkové požiadavky, interné predpisy prevádzkovateľa a legislatívne zmeny. Služby na vyžiadanie sa budú realizovať formou samostatných objednávok podľa interných predpisov Objednávateľa. Proces vyžiadania a implementácie služby musí byť zaevidovaný do Service Desku Objednávateľa.

8 Organizácia projektu

Táto kapitola stanovuje a rieši základné podmienky a predstavy obstarávateľa o postupoch, prácach, zodpovednosti a okruhoch problémov pre úspešný priebeh implementácie projektu APM dátový koncentrátor, jeho testovanie, až po jeho nasadenie do prevádzky.

8.1 Dokumentácia

Dokumentácia musí byť poskytnutá ku všetkým zariadeniam a funkciám dodávaných dodávateľom, ako časť tejto dodávky. Dokumentácia bude popisovať APM dátový koncentrátor, vrátane všetkého jeho softvéru a rozhraní, a bude pokrývať funkčnosť, testovanie, inštaláciu, spúšťanie, prevádzku a údržbu.

- Jazyk dokumentácie

Všetka dokumentácia bude poskytnutá v slovenskom jazyku a iba v prípade písomnej dohody so zadávateľom bude akceptovaná aj iná jazyková verzia. Navyše dokumentácia pre používateľov systému bude dodaná výhradne v slovenskom jazyku.

- Dokumentácia projektu a systému

Bude sa rozlišovať medzi dokumentmi vytvorenými na riadenie projektu a dokumentmi vytvorenými na popis, použitie a údržbu APM dátový koncentrátor.

Dokumentácia vzťahujúca sa k riadeniu projektu zahŕňa:

- plán dokumentácie,
- dokumentácia riadenia projektu,
- dokumentácia testov.

Dokumentácia vzťahujúca sa k systému zahŕňa:

- prehľad systému,
- dokumentácia softvéru,
- dokumentácia databáz,
- dokumentácia grafického prostredia,
- používateľská príručka,
- príručka administrátora
- požiadavky na inštaláciu systému,
- dokumentácia úvodných oboznámení,
- dokumentácia údržby,
- dokumentácia podľa skutočného stavu (as-built).

- Formát dokumentov

Obstarávateľ uprednostňuje, aby boli dokumenty zasielané vo forme, ktorú bude môcť obstarávateľ editovať. Dodávateľovi sa odporúča, aby na dokumenty používal softvér textového procesora MS Office.

Výkresy a diagramy môžu byť dodávané vložené v súboroch dokumentov ako AutoCad alebo MS Visio. Detailný návrh formátu dokumentov a postupu ich schvaľovania bude vzájomne odsúhlasený počas tvorby detailného návrhu riešenia.

- Dokumentácia softvéru

Pre všetok softvér musia byť poskytnuté nasledovné dokumenty:

- zoznam dodávaného softvéru,
- kódovacie štandardy softvéru.

Pre všetok softvér, vytvorený dodávateľom, subdodávateľmi budú poskytnuté nasledovné dokumenty:

- definície databáz,
- funkčný popis softvéru,
- inštalačné sady a zdrojový program.

Pre všetok softvér, vytvorený špeciálne pre tento kontrakt budú poskytnuté nasledovné dokumenty:

- dokument detailného riešenia.
- zoznam dodávaného softvéru

Zoznam podrobne uvedie každú softvérovú položku a bude obsahovať informácie o verzii a licenciách. Pre každú softvérovú položku bude uvedené distribučné médium. Zoznam tiež pre každú položku uvedie, či je dodávaný zdrojový program.

- Inštalačné sady a zdrojový program

Všetok softvér bude dodaný vo formách ako distribučné sady, vhodné na inštaláciu do systému.

Pre obstarávateľa bude možné kompletne vygenerovať, postaviť, nainštalovať a konfigurovať celý APM dátový koncentrátor z distribučných sád, zdrojových programov a obslužných programov poskytnutých so systémom APM dátový koncentrátor.

- Dokument detailného návrhu riešenia

Dokument detailného návrhu riešenia sa bude vzťahovať k jednému funkčnému popisu softvéru. Pre dodávané riešenie sa predpokladá, že dodávateľ najprv dodá funkčný popis softvéru a aplikačných častí na schválenie obstarávateľovi pri splnení minimálnych požiadaviek uvedených v tomto dokumente. Po schválení dodávateľ vytvorí dokument podrobného návrhu na schválenie. Implementácia bude prebiehať po schválení dokumentu detailného návrhu riešenia.

- Príručka na údržbu systému

Príručka na údržbu systému bude obsahovať popis procedúr na obnovenie normálnej činnosti po poruche APM dátový koncentrátor, popis diagnostiky systémov a riešenie štandardných poruchových situácií. Táto príručka bude tiež popisovať procedúry na konfiguráciu počítačového systému APM dátový koncentrátor a zálohovanie systému. Súčasťou príručky musí byť plán obnovy systému (Disaster Recovery).

- Príručka administrátora

Príručka administrátora bude obsahovať popis procedúr s riešením bežných administrátorských situácií ako sú konfigurácia a modifikácia komunikačných rozhraní, archívnej databázy, vytváraním a úpravou grafických zobrazení spolu uvedením príkladov. Príručka (elektronická) musí byť integrálnou súčasťou systému.

- Užívateľská príručka

Príručka bude organizovaná tak, aby umožňovala rýchly prístup ku každému podrobnému popisu užívateľských postupov, ktoré sú používané na interakciu a prácu s funkciami APM dátový koncentrátor. Príručka (elektronická) musí byť integrálnou súčasťou systému. Užívateľská príručka bude uvádzať jasným a výstižným spôsobom všetky informácie, ktoré

používateľ potrebuje k tomu, aby porozumel systému APM dátový koncentrátor a vedel ho uspokojivo používať.

8.2 Oboznámenie používateľov

Úvodné oboznámenie používateľov bude vedené personálom dodávateľa, ktorý bude mať znalosti a skúsenosti v oblasti výroby, výstavby, testovania a údržby a bude plynule ovládať slovenský jazyk (resp. dodávateľ zabezpečí kvalifikovaný preklad do slovenského jazyka). Slovenský jazyk môže byť nahradený i českým jazykom.

Všetok potrebný materiál na oboznámenie bude poskytnutý dodávateľom a bude v slovenskom, po súhlase Obstarávateľa prípadne aj v anglickom jazyku. Každý účastník dostane svoj výtlačok všetkých používaných dokumentov. Dodaná dokumentácia musí odpovedať dodávanej verzii systému.

- Administrácia APM Dátový koncentrátor

Oboznámenie s administráciou systému bude účastníkov zoznamovať s procedúrami potrebnými na to, aby APM dátový koncentrátor pracoval ako integrovaný celok, na rozpoznanie zlyhaní a odozvu na ne a na vykonávanie údržbových funkcií. Oboznámenie bude zahŕňať konfiguráciu a modifikáciu komunikačných rozhraní, archívnej databázy, vytváranie a úpravu grafických zobrazení a o tvorbe doplnkového aplikačného kódu v prostredí systému.

- Oboznámenie s údržbou systému

Oboznámenie s údržbou systému bude zamerané na obnovenie normálnej činnosti po poruche APM dátový koncentrátor, popis diagnostiky systémov a riešenie štandardných poruchových situácií. Bude tiež zamerané na inštaláciu a počiatočnú konfiguráciu počítačového systému APM dátový koncentrátor a zálohovanie systému. Súčasťou musí byť aj postup pri obnove systému (Disaster Recovery).

8.2.1 Minimálne požiadavky na počet účastníkov

Minimálny počet účastníkov je zobrazený v nasledovnej tabuľke. Tabuľka tiež uvádza požadovaný minimálny rozsah oboznámení. Jeden turnus je v predpokladanej dĺžke jeden pracovný týždeň, t.j 40 pracovných hodín.

Oboznámenie	Počet účastníkov	Počet turnusov
Administrácia APM Dátový koncentrátor	2	1
Oboznámenie s údržbou systému	3	1

Tabuľka 8-1: Základný rozsah úvodných oboznámení

Termíny oboznámení budú stanovené s rešpektovaním prevádzkových obmedzení obstarávateľa.

8.3 Licencie

Dodávateľ dodá všetky potrebné licencie na odovzdané dielo, jednak svoje a jednak tretích strán, prípadne dokladuje overenou kópiou vyriešenie licenčných vzťahov medzi dodávateľom a tretími stranami. Počas podpory svojho produktu bude aktualizovať, ak je to nutné, všetky dodané licencie a udržiavať ich platnosť a aktualizáciu. Dodávateľ odovzdá v deň odovzdania diela ako celku zoznam použitých licencii, ich platnosť a rozsah. Všetky licenčné poplatky (napr. databázy ...) musia byť kalkulované na obdobie 4 rokov a musia byť zahrnuté v cenovej ponuke uchádzača.

8.4 Implementácia projektu

Dodávateľ musí vypracovať podrobný harmonogram v súlade so zmluvnými podmienkami. Dodávateľ predloží obstarávateľovi na schválenie podrobný harmonogram implementácie. Ten bude popisovať všetky projektové aktivity dodávateľa aj obstarávateľa. Tento harmonogram bude obsahovať najmenej:

- analýzu súčasného stavu a vypracovanie detailného návrhu riešenia,
- termíny dodania dodávateľom poskytovaných dát a softvéru,
- vývoj softvéru, identifikovanie všetkých softvérových modulov a softvérových rozhraní k funkciám dodaným obstarávateľom,
- testovanie softvérových blokov,
- integrácia a testovanie subsystémov,
- testovanie rozhraní,
- príprava testovacích plánov a procedúr,
- testy u dodávateľa a testy u používateľa,
- oprava zmien a opätovné testovanie,
- úvodné oboznámenia,

- Organizácia a koordinácia projektu

Prvotnými bodmi kontaktu medzi obstarávateľom a dodávateľom budú ich vedúci projektu.

Obstarávateľov vedúci projektu určený v zmluve o dielo bude zodpovedný za reprezentovanie záujmov obstarávateľa v celom projekte. Všetka korešpondencia s obstarávateľom bude adresovaná obstarávateľovmu vedúcemu projektu.

Dodávateľ vymenuje vedúceho projektu (**Dodávateľov vedúci projektu**), ktorý bude zodpovedný za koordináciu všetkých prác na projekte a za komunikáciu medzi dodávateľom a obstarávateľom.

Dokumentácia projektu bude výslovne obsahovať nasledovné dokumenty, ktoré budú dodané obstarávateľovi podľa dátumov, stanovených v referenčných častiach (kde je tiež obsah dokumentu ďalej definovaný).

Dokumentácia projektu

Dokument
Plán dokumentácie
Správa o postupe projektu
Zápisy z jednaní
Programy jednaní
Harmonogram implementácie
Dokumentácia testov
Dokumentácia oboznámení so systémom

8-2: Dokumentácia projektu

Dokumentácia projektu musí byť v slovenskom jazyku. Plán dokumentácie musí byť súčasťou detailného návrhu riešenia. Správy o postupe projektu budú pripravované dodávateľom a posielané obstarávateľovi každý mesiac až do začiatku skúšobnej prevádzky. Dodávateľ

pripraví zápis z každej porady v slovenskom jazyku. Obaja, obstarávateľ i dodávateľ, zápisy posúdia a schvália.

8.4.1 Testovanie, inštalácia a spustenie systému

Poradie aktivít, začínajúce od implementácie systému na prostriedkoch dodávateľa, cez testovanie, odoslanie, inštaláciu a odovzdávanie obstarávateľovi, je rozhodujúce pre úspech projektu. Táto časť stanovuje poradie týchto aktivít a obsahuje aj zodpovednosti obstarávateľa a dodávateľa za tieto aktivity.

Presná klasifikácia porúch bude zahrnutá v procedúrach testov a podlieha schváleniu obstarávateľom. Počas testu sa nesmú vykonávať žiadne úpravy, opravy, modifikácie. Ak je počas testu nutná nejaká úprava, bude to klasifikované ako kritická porucha a použije sa procedúra kritickej poruchy.

Príprava na testy u používateľa

Príprava na testy SAT APM dátový koncentrátor u obstarávateľa sa začnú podľa harmonogramu len v prípade ukončených inštalačných testov pri splnení požiadaviek TŠ. Aktivity prípravy zahŕňajú prevádzku komunikačných rozhraní na všetky relevantné vonkajšie zariadenia a externé systémy. Špecifické úlohy obsahujú:

- overenie všetkých rozhraní so zdrojmi dát a systémami dodanými dodávateľom,
- overenie platnosti APM dátový koncentrátor databáz, zobrazení a správ s použitím dát z vonkajších zariadení,
- overenie platnosti výstupov zo APM dátový koncentrátor funkcii s použitím dát z vonkajších zariadení.

Všetky procedúry testov musia byť plne definované a dokumentované a tiež schválené obstarávateľom pred vykonaním týchto testov. Procedúry testov budú dodané v dostatočnom predstihu, t.j. minimálne jeden mesiac pred začiatkom testov SAT.

- Prostredie testov

Preberacie testy u používateľa sa budú vykonávať za nasledujúcich podmienok:

- pri normálnych podmienkach pracovného prostredia,
- všetky komunikačné zdroje a spolupracujúce systémy sú pripojené,
- klientske aplikácie sú nainštalované

- Test spoľahlivosti

Po dokončení testov sa vykoná 168 hodinový test (7 dní) spoľahlivosti pre APM dátový koncentrátor. Test sa bude vykonávať pri aktuálnych prevádzkových podmienkach. Účelom testov je overiť spoľahlivosť dodaného systému.

- Testovacie kritériá testu spoľahlivosti:

Test pohotovosti je úspešný, ak počas jeho trvania bol systém bez kritickej poruchy minimálne 99,9% času. Po ukončení testu spoľahlivosti, sa uskutoční počiatočný test obnovy chodu systému APM dátový koncentrátor po výpadku, v súlade s vypracovaným plánom obnovy systému.

Príloha č. 2

Všeobecné zmluvné podmienky zabezpečovania BOZP a OPP.

1. Poskytovateľ v zmysle rozsahu predmetu zmluvy a počas doby jej plnenia v plnom rozsahu zodpovedá za bezpečnosť práce svojich zamestnancov, zamestnancov svojich subdodávateľov ako aj spolupôsobiacich fyzických osôb – podnikateľov pri výkone zmluvných činností pre objednávateľa .
2. Objednávateľ, v zmysle zmluvy a počas doby jej plnenia, zabezpečí pred začatím jej plnenia pre zodpovedného zástupcu Poskytovateľa

   Meno a priezvisko: Mgr. Darina Žipaj - Mišková

   Funkcia: autorizovaný bezpečnostný technik

   a technika požiarnej ochrany Poskytovateľa

   Meno a priezvisko: Mgr. Darina Žipaj - Mišková

   Číslo osvedčenia: BOZP – EV. č.: ABT – 000720-06; PO – č.: 5/2017

   oboznámenie zamerané na problematiku dodržiavania predpisov bezpečnosti a ochrany zdravia pri práci a školenie o ochrane pred požiarmi. Zodpovedný zástupca objednávateľa bude oboznámený s určením niektorých prác spojených so zvýšeným ohrozením zdravia vyplývajúcim z pracovných podmienok .
3. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia preberá na seba povinnosti ustanovené legislatívnymi predpismi Slovenskej republiky a osobitnými predpismi pre oblasť bezpečnosti a ochrany zdravia pri práci:
   - ⇨ Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
   - ⇨ Zákon č. 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
   - ⇨ Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
4. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia, preukázateľne zabezpečí pred začatím plnenia zmluvy pre svojich zamestnancov, zamestnancov svojich subdodávateľov ako aj spolupôsobiacich fyzických osôb – podnikateľov oboznámenie a odbornú spôsobilosť ako aj pravidelné oboznámenie ustanovené osobitnými predpismi, potvrdené podpismi všetkých zúčastnených osôb. Pre vlastných zamestnancov, zamestnancov svojich subdodávateľov ako aj pre spolupôsobiace fyzické osoby – podnikateľov, zabezpečí školenie o ochrane pred požiarmi, ktorí sa s vedomím Poskytovateľa zdržujú v objektoch a priestoroch SEPS, hore uvedeným technikom požiarnej ochrany. Poskytovateľ je povinný aj v prípade zmeny u svojich zamestnancov, zamestnancov subdodávateľov a spolupôsobiacich fyzických osôb - podnikateľov (zvýšenie počtu, výmena skupín a pod.) preukázateľne vykonať oboznámenie a školenie týchto osôb.
5. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia predloží na požiadanie objednávateľovi, ešte pred uzavretím zmluvy, fotokópie platných dokladov odbornej a zdravotnej spôsobilosti, doklady o oboznámení s predpismi na zaistenie bezpečnosti a ochrany zdravia pri práci a doklady o školení z predpisov o ochrane pred požiarmi na výkon zmluvne dohodnutých pracovných činností svojich zamestnancov, zamestnancov svojich subdodávateľov ako aj spolupôsobiacich fyzických osôb - podnikateľov.
6. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia zabezpečí pre všetky spolupôsobiace osoby bez odbornej spôsobilosti v zmysle vyhlášky č. 508/2009 Z. z., v znení neskorších predpisov stály dozor pri práci fyzickou osobou, ktorá spĺňa požiadavky odbornej spôsobilosti

elektrotechnika na riadenie činnosti alebo na riadenie prevádzky a podľa STN 34 3100 pre práce na elektrických zariadeniach v blízkosti častí pod napätím. Dozor pri práci nesmie vykonávať vedúci práce určený v príslušnom príkaze „ B „.

7. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia je povinný plniť povinnosti ustanovené v legislatívnych predpisoch pre oblasť ochrany pred požiarmi a súvisiacich slovenských technických noriem:
   - ⇨ Zákon č. 314/2001 Z. z. o ochrane pred požiarmi a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
   - ⇨ Vyhláška MV SR č. 121/2002 Z. z. o požiarnej prevencii v znení neskorších predpisov,
8. Poskytovateľ je povinný umožniť kontrolu plnenia podmienok výkonu diela zamestnancom objednávateľa, v zmysle Zákona č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov.
9. V prípade vzniku mimoriadnej udalosti (pracovný úraz, nebezpečná udalosť, závažná priemyselná havária, požiar) počas výkonu pracovnej činnosti pre objednávateľa, je Poskytovateľ povinný vykonať ohlásenie tejto udalosti v zmysle Zákona č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov resp. Zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov a zabezpečiť povinnosti vyplývajúce z uvedených zákonov. Vznik tejto udalosti je Poskytovateľ povinný ihneď ohlásiť a následne písomne oznámiť aj objednávateľovi s cieľom zabezpečenia objektívneho vyšetrenia.
10. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia zodpovedá za kompletné vybavenie a používanie osobných ochranných pracovných prostriedkov svojimi zamestnancami, zamestnancami subdodávateľa a spolupôsobiacimi fyzickými osobami – podnikateľmi v zmysle Nariadenie vlády SR č. 395/2006 Z. z. o minimálnych požiadavkách na poskytovanie a používanie osobných ochranných pracovných prostriedkov v znení neskorších predpisov.
11. Poskytovateľ je povinný zabezpečiť jednotné oblečenie a viditeľné označenie svojich zamestnancov názvom - logom firmy, ako aj zamestnancov svojich subdodávateľov a spolupôsobiacich fyzických osôb - podnikateľov.
12. Poskytovateľ je povinný rešpektovať zákaz fajčenia, prinášať a požívať na pracoviskách a v priestoroch v pôsobnosti objednávateľa akékoľvek alkoholické nápoje alebo omamné a psychotropné látky. Za nedodržanie tohoto bodu je povinný a zaväzuje sa uhradiť zmluvnú pokutu vo výške **1000,- €** za každého zamestnanca, porušujúceho uvedené zákazy ako aj za spolupôsobiacich dodávateľov. Záznam o písomnom oboznámení všetkých zúčastnených osôb so zákazom fajčenia a požívať na pracoviskách a v priestoroch objednávateľa akékoľvek alkoholické nápoje alebo omamné a psychotropné látky , musí Poskytovateľ na požiadanie predložiť zodpovednému zástupcovi objednávateľa.
13. Poskytovateľ je povinný písomne požiadať objednávateľa o povolenie vjazdu vozidiel s uvedením typu, EČV a účelu vjazdu vozidla. V objektoch objednávateľa sú vozidlá Poskytovateľa a jeho spolupôsobiacich dodávateľov povinné dodržiavať miestne dopravné značenie, maximálnu povolenú rýchlosť a pokyny zodpovedného zástupcu objednávateľa. Zamestnancom dodávateľských a servisných organizácií je vstup do objektov umožnený až po schválení žiadosti na vstup v zmysle internej dokumentácií SEPS – Režimové opatrenia pre vstup a pobyt osôb v objektoch elektrických staníc spoločnosti, formulár F0221 Povolenie na vstup a po predložení dokladu o absolvovaní oboznámenia sa s predpismi BOZP a OPP v zmysle príslušných predpisov.
14. Za nedodržanie zákazu parkovania na vyhradených miestach je Poskytovateľ povinný uhradiť zmluvnú pokutu vo výške **200,- €** za každé vozidlo parkujúce na vyhradenom mieste a zároveň v prípade vzniku mimoriadnej udalosti (pracovný úraz, nebezpečná udalosť, závažná priemyselná havária, požiar) uhradiť škody spôsobené znemožnením príjazdu vozidiel hasičského a záchranného zboru alebo rýchlej zdravotnej služby.

15. V prípade nerešpektovania dopravného značenia a povolenej rýchlosti vozidlom Poskytovateľa alebo jeho spolupôsobiaceho dodávateľa v objekte objednávateľa, bude s okamžitou platnosťou vydaný objednávateľom resp. zmluvným prevádzkovateľom zákaz vjazdu pre uvedené motorové vozidlo do objektu objednávateľa.
16. Objednávateľ nezodpovedá za škody vzniknuté na motorových vozidlách Poskytovateľa spôsobené nerešpektovaním dopravného značenia a parkovaním na vyhradených miestach pre vozidlá hasičského a záchranného zboru alebo rýchlej zdravotnej služby.
17. Poskytovateľ je povinný na pracovisku objednávateľa dodržiavať všetky zmluvné podmienky a predpisy bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi pri prácach, ktoré bude v zmysle zmluvy a počas doby jej plnenia vykonávať. Na skutočnosti odporujúce predpisom bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi je povinný písomne upozorniť zodpovedného zástupcu objednávateľa.
18. Povinnosťou Poskytovateľa je preukázateľne upozorniť objednávateľa na riziká, vyplývajúce z činností pre splnenie predmetu zmluvy, ktoré bude na pracoviskách a v priestoroch objednávateľa vykonávať.
19. Zamestnanci Poskytovateľa resp. jeho spolupôsobiaci dodávatelia sú povinní počas pracovnej doby zdržiavať sa na mieste výkonu práce, udržiavať na pracoviskách a v priestoroch SEPS čistotu a poriadok počas celej doby trvania a plnenia predmetu zmluvy.
20. Objednávateľ, Poskytovateľ a jeho spolupôsobiaci dodávatelia sú povinní na spoločnom pracovisku zabezpečiť koordináciu činnosti a vzájomnú informovanosť o možných ohrozeniach, preventívnych opatreniach a opatreniach na poskytnutie prvej pomoci, na zdolávanie požiarov, na vykonanie záchranných prác a na evakuáciu osôb prítomných na pracovisku. Poskytovateľ je povinný organizovať všetky zmluvne dohodnuté pracovné činnosti tak, aby svojou činnosťou nenarušoval plynulý, bezpečný a včasný výkon ostatných pracovných činností prítomných osôb ako aj bezpečnosť prevádzkovaných zariadení.
21. Poskytovateľ v zmysle zmluvy a počas doby jej plnenia je povinný dodržiavať interné bezpečnostné, prevádzkové a technologické predpisy objednávateľa, ktoré mu boli poskytnuté, napr.: pri zaisťovaní, preberaní a odovzdávaní pracoviska a zariadení. V prípade porušenia týchto predpisov zo strany zamestnancov Poskytovateľa resp. jeho spolupôsobiacich dodávateľov bude týmto odobraté oprávnenie pre vstup do objektu objednávateľa bez dopadu na plnenie zmluvných záväzkov Poskytovateľa.
22. **Za nedodržanie zmluvných podmienok BOZP a OPP je Poskytovateľ povinný uhradiť zmluvnú pokutu vo výške 2000,- €.** V prípade, ak objednávateľ zistí, že zamestnanci Poskytovateľa alebo jeho spolupôsobiaci dodávatelia zjavným spôsobom porušujú zásady bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi, zmluvné podmienky zabezpečovania BOZP a iné písomne dohodnuté podmienky, **môže uložiť ďalšiu pokutu až do dvojnásobku pokuty uvedenej v tomto bode** alebo odstúpiť od zmluvy bez toho, aby Poskytovateľovi vznikol nárok na náhradu prípadnej škody alebo nabehnutých nákladov.

Uložením zmluvnej pokuty nie je Poskytovateľ zbavený zodpovednosti za nedostatky v oblasti BOZP a OPP zistené kontrolnými orgánmi, ktoré boli spôsobené činnosťou Poskytovateľa. Ak bude na základe zisteného porušenia právnych predpisov činnosťou Poskytovateľa uložená pokuta objednávateľovi, Poskytovateľ uhradí uloženú pokutu v plnej výške.

Príloha č. 3

Všeobecné zmluvné podmienky zabezpečovania informačnej bezpečnosti

1 Rámec

1.1 Úvod

Tento dokument definuje základné bezpečnostné pravidlá a požiadavky SEPS navrhnuté za účelom optimálneho zabezpečenia dôvernosti, dostupnosti a integrity informácií ako Objednávateľa, tak aj informácií Poskytovateľa, proti neautorizovanej úmyselnej alebo náhodnej modifikácii, poškodeniu, zničeniu alebo prezradeniu.

1.2 Rozsah

Rozsah tejto politiky je definovaný v zmysle zavedeného systému riadenia informačnej bezpečnosti v spoločnosti SEPS v súlade s požiadavkami ISO 27001:2013.

1.3 Organizácia

Osoba oprávnená rokovať vo veciach zmluvných za SEPS: Každý zmluvný partner / Poskytovateľ má v zmluve definovanú Osobu oprávnenú rokovať vo veciach zmluvných za SEPS, zodpovednú za vlastníctvo obchodného vzťahu a jeho celkové vykonávanie vrátane dodržiavania súladu s bezpečnostnými požiadavkami.

Gestor informačného systému za SEPS: zodpovedá za opodstatnenosť a primeranosť schválených oprávnení a rozsahu ICT prostriedkov (HW, SW, sieťové služby) Poskytovateľovi prác, služieb alebo tovarov v oblasti ICT. Gestor informačného systému za SEPS ďalej zodpovedá za stanovenie technických a špecifických bezpečnostných požiadaviek a pravidiel vo vzťahu k samotným informačným systémom, aplikáciám, databázam ako aj k sieťovému prostrediu a jeho komponentom a za primerané nastavenie kvality dodávaných služieb prostredníctvom detailne definovaných SLA v zmluvách a za ich následnú kontrolu počas plnenia predmetu zmluvy.

Štandardne je to za SEPS v zmluvách uvádzaná osoba oprávnená rokovať vo veciach technických.

Vedúci odboru bezpečnosti BOZP a OPP SEPS: Vedúci odboru bezpečnosti BOZP a OPP SEPS musí zhodnotiť riziká spojené so zmluvnými partnermi voči Objednávateľovi a v prípade potreby navrhnúť primerané technické, organizačné alebo personálne opatrenia na zníženie identifikovaných rizík na akceptovateľnú úroveň. Z uvedených dôvodov je vedúci odboru bezpečnosti BOZP a OPP SEPS oprávnený vykonať u Poskytovateľa bezpečnostný audit v rozsahu definovanom medzinárodným štandardom ISO 27001. Vedúci odboru bezpečnosti BOZP a OPP SEPS musí úzko spolupracovať s Manažérom bezpečnosti Poskytovateľa na udržiavaní primeranej odozvy na bezpečnostné incidenty/výsledky auditov a poskytnúť aktualizácie akýchkoľvek prebiehajúcich zmien bezpečnostných postupov a politík Objednávateľa.

Manažér Poskytovateľa & Manažér bezpečnosti Poskytovateľa: Manažér Poskytovateľa (štandardne je to osoba Poskytovateľa definovaná v zmluve ako osoba oprávnená rokovať vo veciach zmluvných) musí identifikovať Manažéra bezpečnosti Poskytovateľa zodpovedného za dodržiavanie bezpečnostných pravidiel a politík Objednávateľa. Manažér bezpečnosti Poskytovateľa spolupracuje pri bezpečnostných auditoch vykonaných vedúcim odboru bezpečnosti BOZP a OPP SEPS alebo ním povereným externým subjektom a je zodpovedný za implementáciu primeraných organizačných, technických alebo personálnych opatrení za účelom zníženia rizík identifikovaných bezpečnostným auditom. Manažér bezpečnosti Poskytovateľa je ďalej zodpovedný za priebežnú aktualizáciu a riadenie rizík súvisiacich s dodávanými prácami, službami alebo tovarmi s potenciálnym dopadom na Objednávateľa. Zodpovednosťou manažéra Poskytovateľa je aj informovanie Objednávateľa za SEPS o akýchkoľvek subdodávkach resp. outsourcovanej práci pri plnení predmetu zmluvy a udržiavanie primeranej bezpečnostnej úrovne a dohôd aj u subdodávateľov.

2 Všeobecné bezpečnostné požiadavky

2.1 Bezpečnostný audit

2.1.1 SEPS ako Objednávateľ je oprávnený vykonávať bezpečnostné audity v rozsahu definovanom štandardom ISO 27001 u Poskytovateľa tovaru, služieb alebo prác so zameraním na predmet zmluvy. Objednávateľ môže vykonaním bezpečnostného auditu poveriť aj externý subjekt. Poskytovateľ musí poskytnúť primeranú súčinnosť pri bezpečnostných auditoch. Objednávateľ je povinný písomne informovať Poskytovateľa o plánovanom audite najmenej 15 pracovných dní pred začatím auditu.

2.1.2 Manažér bezpečnosti Poskytovateľa musí preskúmať spolu s vedúcim odboru bezpečnosti BOZP a OPP SEPS všetky riziká identifikované prostredníctvom preverenia infraštruktúry a auditov.

2.1.3 Poskytovateľ musí byť pripravený na požiadanie poskytnúť potrebnú technickú, prevádzkovú alebo bezpečnostnú dokumentáciu súvisiacu s dodávanými tovarmi, službami alebo prácami ako podporu pre externé audity ISMS v SEPS.

2.1.4 Okrem auditov zmluvných dohôd/záväzkov vo vzťahu k SEPS, musí Poskytovateľ vyhovieť žiadosti Objednávateľa ako aj zabezpečiť súčinnosť pri vykonaní jednej komplexnej bezpečnostnej previerky/auditu za rok, vrátane, ale bez obmedzenia na preskúmanie politík, procesov, postupov, dokumentácie a opatrení týkajúcich sa fyzickej bezpečnosti, siete, systémov a aplikácií v súlade s ISO 27001. Žiadosť o vykonanie komplexného bezpečnostného auditu Objednávateľ oznámi Poskytovateľovi písomne min. 30 kalendárnych dní pred začatím auditu.

2.1.5 Objednávateľ má právo prizvať na posúdenie zavedených procesov a postupov aj externého špecialistu v prípade, ak nie sú v rámci SEPS interné kapacity na dostatočnej úrovni znalostí konkrétneho systému, resp. aplikačného vybavenia.

2.2 Personálna bezpečnosť

2.2.1 Poskytovateľ musí mať zavedené procesy a špecifické ustanovenia, pre zabezpečenie primeranej previerky personálneho pozadia pracovníkov, ktorí sú nasadzovaní na plnenie predmetu zmluvy v SEPS. Toto ustanovenie je povinne auditované u Poskytovateľa, ktorý zabezpečuje dodávku tovarov, prác alebo služieb pre Objednávateľa na kritických systémoch, aplikáciách, resp. má prístup k citlivým informáciám.

2.2.2 Manažér bezpečnosti Poskytovateľa musí zabezpečiť primerané monitorovanie pridelených ICT prostriedkov, prostredníctvom ktorých je zabezpečované plnenie predmetu zmluvy vo vzťahu k Objednávateľovi. O tejto skutočnosti musia byť preukázateľne poučení všetci zamestnanci Poskytovateľa, ktorí sa podieľajú na plnení predmetu zmluvy. Manažér bezpečnosti Poskytovateľa musí mať definovaný formálny proces pre odozvu na porušenie bezpečnostných politík a predpisov.

2.3 Inventár, vlastníctvo a klasifikácia aktív

2.3.1 Poskytovateľ musí mať formalizovaný a zavedený proces riadenia aktív, minimálne v rozsahu:

2.3.2 **Inventár údajov a informácií:** zmluvní partneri musia udržiavať inventár všetkých informačných aktív (vo vzťahu k SEPS). Inventár musí zahŕňať:

2.3.2.1 názov, umiestnenie, uchovávanie a klasifikačný stupeň údajov. Týka sa to informačných aktív ako napr. technické dokumentácie, prevádzkové postupy, databázy ale napr. aj prístupové údaje, konfiguračné údaje systémov atď.

2.3.3 **Inventár fyzických aktív:** zmluvní partneri musia udržiavať inventár fyzických aktív používaných pri plnení predmetu zmluvy voči SEPS.

2.3.3.1 Fyzické aktíva a vybavenie musí mať evidenčné štítky alebo zaznamenané sériové čísla.

2.3.3.2 Každému aktívu musí byť priradený vlastník a musia byť definované požiadavky a podmienky pre primerané používanie aktív.

2.3.4 **Inventár softvéru:** zmluvní partneri musia udržiavať inventár softvéru používaného

pri plnení predmetu zmluvy voči SEPS.

2.4 Ukladanie a narábanie s údajmi, ochrana informácií

2.4.1 Zmluvní partneri musia pri ukladaní údajov, resp. pri nakladaní s nimi dodržiavať minimálne požiadavky spĺňajúce nasledovné odporúčania:

2.4.1.1 Neverejné informácie musia byť uložené zamknuté, chránené heslom/zašifrované.

2.4.1.2 Pri práci s papierovými dokumentmi SEPS je potrebné sa riadiť politikou čistého stola. Tlač citlivých dokumentov SEPS nesmie byť ponechaná bez dozoru.

2.4.1.3 Heslá do systémov a aplikácií SEPS nesmú byť uložené vo formáte nechráneného textu.

2.4.2 Nesmú sa robiť kópie citlivých informácií bez povolenia vlastníka informácii za SEPS.

2.4.3 Údaje a dokumenty SEPS používané Poskytovateľom za účelom plnenia predmetu zmluvy, nesmú byť ukladané alebo replikované u prípadných subdodávateľov bez súhlasu Objednávateľa; súhlas musí dať Objednávateľ ešte pred prenosom údajov subdodávateľovi alebo ktorejkoľvek ďalšej entite mimo Objednávateľa a Poskytovateľa. Manažér Poskytovateľa musí udržiavať zoznam subdodávateľov, ktorí dostávajú údaje, účel prenosu údajov, metódu prenosu a šifrovania/ochrany alebo protokol, že údaje sú prenesené a schvaľovateľ za SEPS (gestor informačného systému za SEPS alebo vedúci odboru bezpečnosti BOZP a OPP za SEPS), ktorí autorizovali prenos s týmito opatreniami.

2.4.4 Poskytovateľ a všetci jeho zamestnanci podieľajúci sa na plnení predmetu zmluvy sú povinní zachovávať mlčanlivosť o všetkých skutočnostiach, s ktorými sa oboznámili počas výkonu prác, služieb alebo dodávke tovarov v zmysle predmetu zmluvy a to ako po dobu trvania zmluvy, tak aj po jej skončení.

2.4.5 Poskytovateľ je oprávnený poskytovať zmluvou dohodnuté činnosti len prostredníctvom zamestnancov, ktorí boli odsúhlasení Objednávateľom.

2.4.6 Pri ukončení alebo vypovedaní zmluvného vzťahu musia zmluvní partneri poskytnúť Objednávateľovi kópie všetkých informácií udržiavaných v rámci zmluvného vzťahu, ako aj všetky záložné a archívne médiá obsahujúce informácie SEPS.

2.4.7 Pri ukončení zmluvného vzťahu musí byť spoločne so zmluvnými partnermi dohodnutý proces zničenia údajov kvôli odstráneniu všetkých informácií SEPS zo systémov a aplikácií zmluvných partnerov. Obdobným spôsobom musia byť zničené aj údaje v tlačenej forme.

2.5 Výmena informácií

2.5.1 Zmluvní partneri musia pri výmene informácií s Objednávateľom dodržiavať nasledovné odporúčania:

2.5.1.1 Email: Citlivé informácie SEPS musia byť pri prenose elektronickou poštou vo forme príloh šifrované.

2.5.1.2 Doručovanie tlačených zásielok: Posielať citlivé tlačené informácie SEPS prostredníctvom kuriéra alebo doporučenou poštou so sledovaním/evidenciou zásielky.

2.5.1.3 Fax: citlivé informácie sa neodporúčajú vymieňať faxom.

2.5.1.4 Telefón: citlivé informácie SEPS nesmú byť diskutované prostredníctvom pevných alebo IP telefónov.

2.5.1.5 Mobilné telefóny: citlivé informácie SEPS nesmú byť diskutované prostredníctvom mobilných telefónov.

2.6 Pravidlá pre dodávateľské Notebooky/PC pripájané do infraštruktúry SEPS

2.6.1 Zmluvní partneri musia mať definovanú politiku pre Primerané použitie ICT prostriedkov.

2.6.2 Zmluvní partneri musia udržiavať bezpečnosť počítačov/notebookov prostredníctvom preukázateľného patch manažmentu a pravidelne aktualizovaného antivirového programu. Pre všetky notebooky/PC s OS Windows pripájaných do siete SEPS sa vyžaduje zapnutie osobného firewall-u.

2.6.3 Údaje SEPS nesmú byť uložené na notebookoch alebo iných prenosných zariadeniach zmluvných partnerov, pokiaľ ich disky nie sú chránené šifrovaním.

2.7 Kontinuita činností

2.7.1 Manažér bezpečnosti Poskytovateľa zodpovedá za aktuálnosť a funkčnosť plánov obnovy

činností súvisiacich s plnením predmetu zmluvy voči Objednávateľovi tak, aby dodávka služieb, prác alebo tovarov vyplývajúcich z predmetu zmluvy neboli ohrozené ani v prípadoch neočakávaných alebo havarijných situácií.

2.7.2 Vedúci odboru bezpečnosti BOZP a OPP SEPS musí zabezpečiť prípravu, udržiavanie a pravidelné testy BCP/DR plánov, ktoré umožnia dostupnosť všetkých kritických služieb vo vzťahu k Objednávateľovi v prípade núdze alebo katastrofy a spĺňajú podmienky minimálnej požadovanej úrovne služieb.

2.7.3 Akýkoľvek stav núdze, havárie alebo inej neočakávanej situácie, ktorá má (môže mať) za následok prerušenie alebo znemožnenie plnenia predmetu zmluvy musí byť bezodkladne nahlásený Osobe oprávnenej rokovať vo veciach zmluvných za SEPS.

2.8 Odozva na incidenty

2.8.1 Manažér bezpečnosti Poskytovateľa musí udržiavať a aktualizovať plán odozvy na bezpečnostné incidenty.

2.8.2 Manažér bezpečnosti Poskytovateľa musí vedúceho odboru bezpečnosti BOZP a OPP SEPS bezodkladne informovať o bezpečnostných incidentoch, ktoré Poskytovateľ zistí pri plnení predmetu zmluvy (jedná sa najmä o incidenty charakteru neautorizovaný prístup, narušenie dôvernosti alebo dostupnosti citlivých údajov, identifikovaný škodlivý kód).

2.8.3 Pokiaľ z predmetu zmluvy pre Poskytovateľa vyplýva povinnosť zabezpečovať primeranú úroveň dôvernosti a/alebo dostupnosti systému alebo údajov v systéme, v oznámení o incidente musia byť popísané navrhované opatrenia ako aj návrh plánu budúcich činností na prevenciu pred podobnými incidentmi v budúcnosti. Manažér bezpečnosti Poskytovateľa a vedúci odboru bezpečnosti BOZP a OPP SEPS musia v čo najkratšom možnom čase dohodnúť postup, resp. vzájomne odsúhlasiť zmeny za účelom odstránenia bezpečnostného incidentu a spôsob realizácie plánu budúcich činností.

2.9 Súlad s predpismi

Ak je ktorékoľvek ustanovenie tejto politiky v konflikte s politikami Poskytovateľa, tento problém musí byť predložený vedúcemu odboru bezpečnosti BOZP a OPP SEPS na preskúmanie a vyriešenie ešte pred podpisom zmluvy.

2.10 Doplňujúce informácie

Ďalšie bezpečnostné požiadavky, najmä špecifické vo vzťahu ku konkrétnym aplikáciám, systémom ako aj ku sieťovej konektivite môžu byť špecifikované Gestorom informačného systému za SEPS priamo v zmluve.

Príloha č. 4

Zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností

podľa § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon o kybernetickej bezpečnosti") v spojení s § 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 NBÚ")

Predmetom tejto Prílohy je úprava podmienok a spôsobu zabezpečenia plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona o kybernetickej bezpečnosti, Vyhlášky NBÚ a ostatných všeobecne záväzných právnych predpisov v oblasti kybernetickej bezpečnosti s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov spoločnosti SEPS počas celej doby trvania zmluvného vzťahu založeného Zmluvou.

Pojmy použité v tejto Prílohe majú význam vymedzený Zákonom o kybernetickej bezpečnosti. Na účely tejto Prílohy je spoločnosť SEPS prevádzkovateľom základnej služby a druhá zmluvná strana je Dodávateľom.

Časť A.
Všeobecné ustanovenia

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti za účelom zabezpečenia kybernetickej bezpečnosti sietí a informačných systémov spoločnosti SEPS, a to na úrovni písomne dohodnutej so SEPS; špecifikácia a rozsah bezpečnostných opatrení, ktoré sa Dodávateľ zaväzuje prijať a dodržiavať po celý čas trvania zmluvného vzťahu založeného Zmluvou je vymedzený v časti B. tejto Prílohy.
2. Konkrétny rozsah činností Dodávateľa vyplýva zo Zmluvy a jej príloh.
3. Dodávateľ vyhlasuje, že sa oboznámil s bezpečnostnou politikou spoločnosti SEPS, tvoriacou osobitnú prílohu k Zmluve, vyjadruje s ňou súhlas a zaväzuje sa ju dôsledne dodržiavať; so zmenou/doplnením bezpečnostnej politiky spoločnosti SEPS, ktorá bude prijímaná formou vzájomne odsúhlaseného písomného dodatku k Zmluve v dostatočnom časovom predstihu pred nadobudnutím jej účinnosti je Dodávateľ povinný sa bezodkladne oboznámiť a dôsledne ju dodržiavať.
4. Každá Zmluvná strana sa zaväzuje chrániť všetky dôverné informácie, ktoré jej boli, alebo budú zo strany druhej Zmluvnej strany poskytnuté, alebo sprístupnené a to najmä, avšak nie len pred akýmkoľvek nezákonným zničením, stratou, zmenou, neoprávneným poskytnutím, alebo sprístupnením. Povinnosť mlčanlivosti upravená v časti E. tejto Prílohy sa aplikuje v prípade, ak v Zmluve, alebo v jej prílohách nie je povinnosť mlčanlivosti, resp. ochrana dôverných informácií upravená inak.
5. Dodávateľ je oprávnený poveriť plnením predmetu Zmluvy s dopadom na kybernetickú bezpečnosť výlučne odborne spôsobilé osoby viazané povinnosťou mlčanlivosti a v súlade s princípom *need-to-know*; zoznam pracovných rolí a osôb s prístupom k informáciám a údajom spoločnosti SEPS je uvedený v časti C. tejto

Prílohy; O zmene v personálnom obsadení je Dodávateľ povinný spoločnosť SEPS bezodkladne písomne informovať.

6. Rozsah, spôsob a možnosti vykonávania **kontrolných činností a auditu** Ustanovenia tohto bodu sa aplikujú v prípade, ak nie je výkon kontrolných činností a auditu v Zmluve upravený inak.
   a. Spoločnosť SEPS je oprávnená po písomnom oznámení doručenom Dodávateľovi v dostatočnom časovom predstihu vykonať u Dodávateľa audit za účelom preverenia účinnosti Dodávateľom prijatých bezpečnostných opatrení a plnenia požiadaviek a povinností v oblasti kybernetickej bezpečnosti. Spoločnosť SEPS je oprávnená vykonať audit sama, alebo prostredníctvom tretej osoby.
   b. Dodávateľ je povinný umožniť vykonanie auditu a spoločnosti SEPS poskytnúť všetku vopred dohodnutú súčinnosť nevyhnutne potrebnú k riadnemu vykonaniu auditu a to najmä, avšak nie len informácie, vysvetlenia, dokumenty a prístupy za účelom preukázania účinnosti prijatých bezpečnostných opatrení a splnenia požiadaviek a povinností v oblasti kybernetickej bezpečnosti; Dodávateľ je povinný za vopred dohodnutých podmienok zabezpečiť prítomnosť svojich zamestnancov a iných osôb poverených plnením povinností v oblasti kybernetickej bezpečnosti.
   c. Spoločnosť SEPS predloží Dodávateľovi záverečnú správu o výsledkoch auditu spolu s opatreniami na nápravu zistených nedostatkov a s Dodávateľom vopred dohodnutými lehotami na ich odstránenie. V prípade, ak Dodávateľ zistené nedostatky v dohodnutej lehote neodstráni a/alebo vykonanie auditu neumožní v rozpore s podmienkami Zmluvy, spoločnosť SEPS je oprávnená od Zmluvy odstúpiť; tým nie je dotknuté právo spoločnosti SEPS na náhradu škody spôsobenej porušením povinností Dodávateľa na úseku kybernetickej bezpečnosti a/alebo neprijatím opatrení na nápravu v súlade s podmienkami Zmluvy.
7. Podmienky a možnosti **zapojenia ďalšieho dodávateľa (subdodávateľa)**
   a. Ak nie je v Zmluve uvedené inak, Dodávateľ nie je oprávnený zapojiť ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie predmetu Zmluvy bez písomného súhlasu spoločnosti SEPS, pričom predmetný súhlas spoločnosti SEPS nebude odoprený bez primeraného dôvodu riadne preukázaného Dodávateľovi. Predchádzajúci súhlas podľa tohto bodu sa nevyžaduje pre zapojenie člena skupiny Dodávateľa (t.j. spriaznené osoby Dodávateľa podľa § 66a Obchodného zákonníka) a/alebo tzv. bežného personálu Dodávateľa, t.j. osoby, ktoré sú so Dodávateľom alebo iným členom jeho skupiny v pracovnom pomere alebo v obchodnom vzťahu (napr. konzultanti v postavení SZČO), na základe ktorého vykonávajú konzultačné činnosti a služby v oblasti IT výhradne alebo pravidelne pre príslušného člena skupiny Dodávateľa. Tým nie je dotknutá povinnosť Dodávateľa podľa bodu 5. tejto časti.
   b. Ak Dodávateľ zapojí ďalšieho dodávateľa, ďalšiemu dodávateľovi je v zmluve alebo v inom právnom úkone povinný uložiť porovnateľné povinnosti týkajúce sa plnenia predmetu Zmluvy s dopadom na kybernetickú bezpečnosť ako sú ustanovené pre Dodávateľa a je povinný zaviazať ho v porovnateľnom rozsahu povinnosťou zachovávať mlčanlivosť; ustanovenia tejto Prílohy o vykonávaní kontrolnej činnosti a auditu platia pre ďalších dodávateľov primerane.

c. Zapojením ďalšieho dodávateľa nie je dotknutá zodpovednosť Dodávateľa za riadne plnenie predmetu Zmluvy, ako ani zodpovednosť za plnenie povinností v oblasti kybernetickej bezpečnosti.

8. **Informačná povinnosť** Dodávateľa a postup pri **riešení kybernetických bezpečnostných incidentov**

a. Dodávateľ sa zaväzuje spoločnosť SEPS informovať o všetkých skutočnostiach, o ktorých je možné rozumne predpokladať, že môžu mať podstatný vplyv na plnenie predmetu Zmluvy v oblasti kybernetickej bezpečnosti bez zbytočného odkladu po tom, ako sa o nich dozvedel. Informácie je Dodávateľ povinný adresovať kontaktným osobám spoločnosti SEPS uvedeným v časti D. tejto Prílohy.

b. Dodávateľ sa zaväzuje spoločnosť SEPS informovať o každom kybernetickom bezpečnostnom incidente (v zmysle definície uvedenej v príslušných ustanoveniach Zákona o kybernetickej bezpečnosti), bez zbytočného odkladu po tom, ako sa o ňom dozvedel, a zároveň po dohode so spoločnosťou SEPS vykonať všetky neodkladné opatrenia, ktorých účelom je zabrániť rozširovaniu kybernetického bezpečnostného incidentu a jeho následkov.

c. Oznámenie o kybernetickom bezpečnostnom incidente (ďalej len „Oznámenie") musí obsahovať všetky podstatné informácie známe Dodávateľovi ku dňu Oznámenia, čo môže zahŕňať najmä nasledovné informácie:

i. opis povahy kybernetického bezpečnostného incidentu a služby, ktorá je kybernetickým bezpečnostným incidentom zasiahnutá, vrátane počtu používateľov základnej služby zasiahnutých kybernetickým bezpečnostným incidentom;

ii. opis priebehu, dĺžky trvania a geografického rozšírenia kybernetického bezpečnostného incidentu;

iii. opis pravdepodobných následkov a vplyvu kybernetického bezpečnostného incidentu na poskytovanú službu, vrátane stupňa narušenia fungovania základnej služby;

iv. opis opatrení prijatých alebo navrhovaných Dodávateľom s cieľom napraviť porušenie kybernetickej bezpečnosti a podľa potreby, opatrení na zmiernenie potenciálnych nepriaznivých dôsledkov kybernetického bezpečnostného incidentu, vrátane preventívnych opatrení.

Oznámenie je Dodávateľ povinný adresovať kontaktným osobám spoločnosti SEPS uvedeným v časti D. tejto Prílohy.

d. Ak do okamihu oznámenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať spoločnosti SEPS neúplné oznámenie, v ktorom túto skutočnosť uvedie; neúplné oznámenie je Dodávateľ povinný bezodkladne po obnovení riadnej prevádzky siete a informačného systému doplniť.

e. Zmluvné strany za zaväzujú postupovať vo vzájomnej súčinnosti a vynaložiť primerané úsilie s cieľom v čo najkratšom možnom čase dohodnúť postup za účelom odstránenia kybernetického bezpečnostného incidentu a jeho následkov, ako aj potrebu prijatia preventívnych opatrení.

f. Zmluvné strany za zaväzujú postupovať vo vzájomnej súčinnosti a vynaložiť primerané úsilie v čase kybernetického bezpečnostného incidentu s cieľom zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní.

g. Zmluvné strany za zaväzujú postupovať vo vzájomnej súčinnosti a vynaložiť primerané úsilie s cieľom zdokumentovať každý kybernetický bezpečnostný incident, jeho hrozbu, následky a opatrenia prijaté na jeho nápravu, ako aj uchovávať primerane dostupnú dokumentáciu o kybernetickom bezpečnostnom incidente.

9. Odplata za plnenie povinností a výkon činností v zmysle tejto Prílohy bude určená dohodou Zmluvných strán v súlade s ustanoveniami Zmluvy.

10. **Sankčný mechanizmus a náhrada škody** pri porušení Zmluvy
    a. Spoločnosť SEPS má nárok na zmluvnú pokutu vo výške 5.000 EUR za každý jednotlivý prípad porušenia povinnosti Dodávateľa stanovenej v tejto Prílohe, maximálne však vo výške 20.000 EUR za obdobie jedného kalendárneho roka; uplatnením alebo zaplatením zmluvnej pokuty nie je dotknutý nárok spoločnosti SEPS na náhradu škody v súlade so Zmluvou a touto Prílohou.
    b. Spoločnosť SEPS má nárok na náhradu zákonných sankcií, ktoré jej budú uložené Národným bezpečnostným úradom alebo iným príslušným orgánom verejnej správy, ak sankcia bude spoločnosti SEPS uložená preukázateľne a výlučne z dôvodu porušenia povinnosti Dodávateľa na úseku kybernetickej bezpečnosti, a to v rámci náhrady škody v súlade so Zmluvou a touto Prílohou.
    c. Zmluvné strany zodpovedajú len za skutočnú škodu spôsobenú druhej Zmluvnej strane, nie za ušlý zisk či nepriame škody či škody spôsobené tretím stranám. Žiadna zo zmluvných strán nezodpovedá za škodu, ktorá vznikla v dôsledku vecne nesprávneho alebo inak chybného zadania, pokynu, informácie, súčinnosti alebo inštrukcie, ktoré prijala od druhej Zmluvnej strany alebo v dôsledku omeškania s poskytnutím čohokoľvek z uvedeného.
    d. Zmluvné strany sa dohodli, že celkový rozsah náhrady škody, na ktorú vznikne spoločnosti SEPS nárok v prípade porušenia povinností Dodávateľa vyplývajúcich z tejto Prílohy, v žiadnom prípade neprevýši sumu 40.000 EUR za obdobie jedného kalendárneho roka. Zmluvné strany v nadväznosti na ustanovenie § 379 Obchodného zákonníka konštatujú, že tento rozsah škody zodpovedá maximálnej výške škody, ktorá je Dodávateľom predvídaná ako možný dôsledok porušenia jeho povinností; škoda spôsobená poškodenej Zmluvnej strane, prevyšujúca výšku predvídateľnej škody podľa tohto odseku sa nenahrádza.

11. **Podmienky a spôsob ukončenia Zmluvy**
    a. V prípade, ak ktorákoľvek Zmluvná strana podstatným spôsobom poruší ktorúkoľvek z povinností vymedzených v tejto Prílohe, druhá Zmluvná strana je oprávnená odstúpiť od Zmluvy z dôvodu podstatného porušenia Zmluvy. Ak nie je v Zmluve uvedené inak, písomné odstúpenie od Zmluvy nadobúda účinnosť dňom jeho doručenia druhej Zmluvnej strane s účinkami odo dňa jeho doručenia (ex nunc). Ak nie je v Zmluve uvedené inak, odstúpenie od Zmluvy sa nedotýka nároku na náhradu spôsobenej škody, ako ani nároku na zmluvnú pokutu, ktorý vznikol v dôsledku porušenia povinnosti, ani nároku na dojednanú odplatu, a to všetko v súlade so Zmluvou a touto Prílohou.
    b. Zánikom zmluvného vzťahu založeného Zmluvou nie je dotknutá povinnosť oboch Zmluvných strán zachovávať mlčanlivosť.

12. Po ukončení zmluvného vzťahu založeného Zmluvou je Dodávateľ povinný v súlade s usmernením spoločnosti SEPS odsúhlaseným oboma Zmluvnými stranami:

a. vrátiť, previesť alebo zničiť všetky podklady a informácie, ku ktorým mal počas trvania zmluvného vzťahu prístup a na požiadanie spoločnosti SEPS je povinný vykonanie prijatých opatrení preukázať,
b. uskutočniť všetky vzájomne dohodnuté kroky a úkony nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby v súlade s Vyhláškou NBÚ, vrátane poskytnutia potrebných licencií, práv a súhlasov zo strany Dodávateľa, a to v rozsahu s obsahom a za podmienok vzájomne dohodnutých Zmluvnými stranami, a
c. predložiť spoločnosti SEPS sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča, ktoré priamo alebo nepriamo súvisia s povinnosťami vyplývajúcimi z tejto Prílohy, zo Zákona o kybernetickej bezpečnosti alebo zo všeobecne záväzného právneho predpisu v oblasti kybernetickej bezpečnosti a ktoré sa týkajú spoločnosti SEPS, a to v rozsahu s obsahom a za podmienok vzájomne dohodnutých Zmluvnými stranami.

Časť B.

Špecifikácia a rozsah bezpečnostných opatrení Dodávateľa

1. Dodávateľ sa zaväzuje prijať, aktualizovať a po celý čas trvania zmluvného vzťahu založeného Zmluvou dodržiavať bezpečnostné opatrenia uvedené v tejto Prílohe alebo inak písomne dohodnuté Zmluvnými stranami v oblasti kybernetickej bezpečnosti s cieľom zabezpečiť kybernetickú bezpečnosť počas celého životného cyklu sietí a informačných systémov spoločnosti SEPS.
2. Vzhľadom na to, že spoločnosť SEPS zaviedla a implementovala normu **STN EN ISO/IEC 27001**, ktorá špecifikuje požiadavky na zostavovanie, implementáciu, prevádzku, monitorovanie, preskúmanie a zlepšovanie systému manažérstva informačnej bezpečnosti, Zmluvné strany sa dohodli, že uvedená norma predstavuje minimálny štandard v oblasti informačnej bezpečnosti, ktorý je Dodávateľ povinný zaviesť a implementovať. Tým nie je dotknutá povinnosť Dodávateľa zaviesť v súlade so Zákonom o kybernetickej bezpečnosti, Vyhláškou NBÚ a ostatnými všeobecne záväznými právnymi predpismi v oblasti kybernetickej bezpečnosti ostatné bezpečnostné opatrenia uvedené v tejto Prílohe alebo inak písomne dohodnuté Zmluvnými stranami s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby spoločnosťou SEPS.
3. Dodávateľ je povinný spoločnosť SEPS bezodkladne písomne informovať o každej zmene špecifikácie a/alebo rozsahu bezpečnostných opatrení uplatňovaných u Dodávateľa s dopadom na kybernetickú bezpečnosť spoločnosti SEPS.
4. Zmluvné strany za zaväzujú postupovať vo vzájomnej súčinnosti a vynaložiť primerané úsilie s cieľom zdokumentovať prijaté bezpečnostné opatrenia v bezpečnostnej dokumentácii vypracovanej v súlade so Zákonom o kybernetickej bezpečnosti a Vyhláškou NBÚ.

Časť C.
Zoznam pracovných rolí/pozícií a zamestnancov Dodávateľa s prístupom k informáciám a údajom spoločnosti SEPS

1. Zoznam pracovných rolí/pozícií:
   Contract manager, IT System developer, IT špecialista, Solution design architect

2. Zoznam zamestnancov

Časť D.
Kontaktné osoby a doručovanie

1. Spoločnosť SEPS určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:

2. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu so spoločnosťou SEPS na úseku kybernetickej bezpečnosti:

3. Zmluvné strany sú povinné vzájomne sa bezodkladne písomne informovať o každej zmene údajov kontaktných osôb, pričom uvedená zmena nepodlieha predchádzajúcemu súhlasu druhej Zmluvnej strany.

4. Ak nie je v Zmluve uvedené inak, všetky oznámenia, hlásenia, pokyny, žiadosti, výzvy a iné úkony v súvislosti s plnením povinností na úseku kybernetickej bezpečnosti (ďalej len „**Písomnosti**") musia byť urobené v písomnej forme. Písomnosti v listinnej podobe sa považujú za doručené za nasledovných podmienok:
   a) v prípade osobného doručovania odovzdaním Písomnosti kontaktnej osobe príslušnej Zmluvnej strany a podpisom takej osoby na doručenke a/alebo kópii doručovanej Písomnosti,
   b) v prípade doručovania prostredníctvom poštového podniku (Slovenskej pošty, a.s. alebo iného doručovateľa – kuriéra) doručením na adresu Zmluvnej strany a v prípade doporučenej zásielky odovzdaním Písomnosti osobe oprávnenej prijímať Písomnosti za túto Zmluvnú stranu a podpisom takej osoby na doručenke, alebo odmietnutím prevzatia Písomnosti, najneskôr však preukázateľným dňom vrátenia nedoručenej Písomnosti späť Zmluvnej strane, ktorá zásielku odosielala, i keď sa druhá Zmluvná strana o obsahu Písomnosti nedozvedela,
   c) pri doručovaní Písomností v elektronickej podobe, t.j. formou zaslania e-mailu na správnu e-mailovú adresu kontaktnej osoby, sa Písomnosť považuje za doručenú okamihom preukázateľného doručenia emailu kontaktnej osobe druhej Zmluvnej strany.

   Písomnosti, ktorých obsah sa týka platnosti, účinnosti, znenia Zmluvy alebo Písomnosti, ktoré obsahujú zásadné zmeny, sa považujú za doručené len ak boli doručené spôsobom podľa bodu 4 písm. a) a b).

Časť E.
Mlčanlivosť

1. Za dôverné informácie sa považujú najmä informácie týkajúce sa (i) plnenia predmetu Zmluvy, (ii) IT infraštruktúry spoločnosti SEPS, (iii) prevádzky komunikačných sietí a informačných systémov spoločnosti SEPS vrátane ich zabezpečenia, (iv) detaily týkajúce sa technických a organizačných opatrení na zabezpečenie integrity a prevádzkyschopnosti sietí a informačných systémov vrátane bezpečnostnej politiky spoločnosti SEPS, (v) osobné údaje, ktoré si Zmluvné strany na základe tejto Zmluvy a v súvislosti s jej plnením poskytnú, (vi) údaje a informácie o spoločnosti SEPS, o spoločnosti Dodávateľa a ich činnostiach, ktoré nie sú verejne dostupné a (vii) iné údaje a informácie poskytnuté druhej Zmluvnej strane, ktoré poskytujúca Zmluvná strana výslovne označí ako dôverné (ďalej len „**Dôverné informácie**").

2. Dôverné informácie poskytnuté, odovzdané, oznámené, sprístupnené a/alebo akýmkoľvek iným spôsobom získané jednou Zmluvnou stranou od druhej Zmluvnej strany na základe a/alebo v akejkoľvek súvislosti s plnením predmetu Zmluvy môžu byť použité výhradne na účely plnenia predmetu Zmluvy. Zmluvné strany sa zaväzujú udržiavať vyššie uvedené Dôverné informácie v prísnej tajnosti, zachovávať o nich mlčanlivosť a chrániť ich pred zneužitím, poškodením, zničením, znehodnotením, stratou a odcudzením, a to i po ukončení zmluvného vzťahu založeného Zmluvou.
3. Zmluvná strana nie je oprávnená bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany Dôverné informácie poskytnúť, odovzdať, oznámiť, sprístupniť, zverejniť, publikovať, rozširovať, vyzradiť ani použiť inak, než na účely plnenia predmetu Zmluvy, a to ani po ukončení zmluvného vzťahu založeného Zmluvou, s výnimkou prípadu ich poskytnutia/odovzdania/oznámenia/sprístupnenia, svojím spriazneným osobám (§ 66a Obchodného zákonníka) a odborným poradcom Zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov, alebo audítorov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti stanovenou alebo uloženou zákonom alebo sú povinní zachovávať mlčanlivosť na základe písomnej dohody so Zmluvnou stranou.
4. Povinnosť Zmluvných strán zachovávať mlčanlivosť o Dôverných informáciách sa nevzťahuje na informácie, ktoré:
   a. boli zverejnené už pred podpisom Zmluvy, čo musí byť preukázateľné na základe poskytnutých podkladov, ktoré túto skutočnosť dokazujú;
   b. boli zistené alebo samostatne vytvorené mimo spolupráce Zmluvných strán založenej Zmluvou, čo musí byť preukázateľné na základe poskytnutých podkladov, ktoré túto skutočnosť dokazujú;
   c. majú byť sprístupnené na základe povinnosti stanovenej zákonom, rozhodnutím súdu, prokuratúry alebo iného oprávneného orgánu verejnej moci, pričom v tomto prípade Zmluvná strana, ktorá je povinná informácie sprístupniť, bezodkladne informuje o sprístupnení informácií druhú Zmluvnú stranu.
5. Zmluvné strany sú povinné zabezpečiť riadne a včasné utajenie Dôverných informácií a zachovávanie povinnosti mlčanlivosti o Dôverných informáciách podľa všeobecne platných, zaužívaných a zachovávaných pravidiel, zásad a zvyklostí pre utajovanie a zachovávanie povinnosti mlčanlivosti o takýchto informáciách.
6. Zmluvné strany sú povinné zabezpečiť riadne a včasné utajenie Dôverných informácií a zachovávanie povinnosti mlčanlivosti o Dôverných informáciách aj u svojich zamestnancov, štatutárnych orgánov, členov štatutárnych orgánov, dozorných orgánov, členov dozorných orgánov, zástupcov, splnomocnencov, subdodávateľov, ako i iných spolupracujúcich tretích osôb, pokiaľ im takéto Dôverné informácie boli poskytnuté, odovzdané, oznámené a/alebo sprístupnené.

Zoznam subdodávateľov

Príloha č.5

č.	Obchodné meno	Sídlo podnikania	IČO	IČ DPH	Predmet subdodávky	Podiel subdodávky z hodnoty zmluvy v EUR		Osoba oprávnená konať za subdodávateľa			
						bez DPH	s DPH	Meno	Priezvisko	Adresa pobytu	Dátum narodenia
1.											
2.											
3.											
4.											
5.											
6.											

Príloha č. 6

Zoznam zodpovedných osôb

Zoznam osôb Objednávateľa, oprávnených komunikovať s Poskytovateľom.

Zoznam osôb Poskytovateľa.

PROTOKOL O VYKONANÍ SLUŽIEB

Číslo:	**Dátum:**

Objednávateľ [1]:
Slovenská elektrizačná prenosová sústava, a.s.
Mlynské nivy 59/A
824 84 Bratislava
IČO: 35 829 141

Poskytovateľ [2]:

Názov Diela (alebo jeho dokončenej časti)/ Vymenovaného systému:
Servisná zmluva na technickú podporu APM dátového koncentrátora.

	Objednávateľa [1]	**Poskytovateľa [2]**
Číslo Zmluvy:		
Číslo Objednávky:		

Obdobie:		**Lokalita:**	

€Tento protokol je dokladom o vykonaní **Technickej podpory** v nasledujúcom členení:

1		
1.1		
2		
3		
4		
4.1		
4.2		
4.3		
4.4		
4.5		
5		

€Prehľad odstránených vád v zmysle bodu č.3:

Dátum uzavretia	**Odstraňovanie vád – špecifikácia prác s krátkym popisom**	**Číslo HD**	**Rozsah prác [čl. hod]**

Služby zdokumentované v rámci tohto protokolu boli poskytovateľom zrealizované v súlade s kvalitatívnymi parametrami služieb definovanými v Prílohe č.1 "Špecifikácia služieb Technickej podpory" predmetnej zmluvy a odberateľ ich preberá bez výhrad.

Zástupcovia Objednávateľa a Poskytovateľa zúčastnení na preberaní vyššie špecifikovaných prác týmto potvrdzujú platnosť protokolu a súhlasia s údajmi v protokole uvedenými:

za Objednávateľa [1]: za Poskytovateľa [2]:

Rozdeľovník 2x 2x