Číslo Zmluvy Objednávateľa: 2023-0259-1189101

Číslo Zmluvy Poskytovateľa: .....

ZMLUVA O POSKYTOVANÍ SLUŽIEB

IS eranet a súvisiacich služieb

uzatvorená podľa ustanovení § 269 ods. 2 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v platnom znení (ďalej len „Zmluva").

I. ZMLUVNÉ STRANY

1.1 Objednávateľ

Slovenská elektrizačná prenosová sústava, a.s.

so sídlom:	Mlynské nivy 59/A, 824 84 Bratislava 26 zapísaná v obchodnom registri Mestského súdu Bratislava III, oddiel Sa, vložka č. 2906/B
zastúpená:	Ing. Jaroslav Vach, MBA, predseda predstavenstva Mgr. Martin Riegel, člen predstavenstva
IČO:	35 829 141
DIČ:	2020261342
IČ DPH:	SK2020261342
bankové spojenie:	TATRA BANKA, a.s., Bratislava
číslo účtu:	2620191900/1100
IBAN:	SK30 1100 0000 0026 2019 1900
Osoby oprávnené rokovať vo veciach:	
zmluvných	Mgr. Martin Riegel, vrchný riaditeľ RI a O Ing. Marek Šimlaštík, špecialista
technických:	Ing. Tomáš Mondik, špecialista Ing. Karol Haluška, špecialista

(ďalej len „Objednávateľ")

1.2 Poskytovateľ

innovis, s.r.o.

so sídlom:	Moldavská cesta 10/B 040 11 Košice
zastúpená:	Ing. Mojmír Prídavok, PhD. konateľ
IČO:	47 894 458
DIČ:	2024139656
IČ DPH:	SK2024139656
bankové spojenie:	Československá obchodná banka, a.s.
číslo účtu:	SK46 7500 0000 0040 2051 2351
Osoby oprávnené rokovať vo veciach:	
zmluvných:	Ing. Mojmír Prídavok, PhD. konateľ
technických:	Ing. Martin Oravec, konzultant

(ďalej len „Poskytovateľ")
(ďalej spoločne len „Zmluvné strany" alebo jednotlivo len „Zmluvná strana")
sa dohodli na uzatvorení tejto Zmluvy:

II. PREAMBULA

2.1. Podkladom pre uzavretie tejto Zmluvy je výberové konanie a ponuka Poskytovateľa ako úspešného uchádzača zo dňa 30.08.2023.

2.2. Zmluva je súčasťou projektu „Implementácia koncepcie centrálneho nákupu a optimalizácia procesov obstarávania", kde jedným z hlavných cieľov je digitalizácia procesov interného obstarávania prostredníctvom informačného systému.

III. VYMEDZENIE POJMOV

3.1. Zmluvné strany sa dohodli, že na účely tejto Zmluvy sa pod vybranými pojmami rozumie nasledovné:

eranet.sk	Internetové rozhranie dostupné cez sieť internet na www.eranet.sk prevádzkované Poskytovateľom, na ktorom je Objednávateľovi a tretím stranám prístupný IS eranet.
ERANET	Označenie informačného systému na riadenie verejných obstarávaní, jeho hardvérových a softvérových súčastí, vrátane databáz, potrebných na prevádzku portálu eranet.sk a poskytovanie ďalších Súvisiacich služieb Poskytovateľom.
IS eranet	Programové rozhranie spoločnosti Poskytovateľom dostupné na eranet.sk umožňujúce riadenie procesov verejných obstarávaní v nasledujúcich moduloch: Plánovanie, Obstarávanie, Kontraktácia, Elektronická aukcia a Hodnotenie dodávateľov.
Plánovanie	Modul IS eranet umožňujúci zber a spracovanie požiadaviek na uskutočnenie verejného obstarávania z rôznych organizačných jednotiek Objednávateľa.
Kvalifikácia dodávateľov	Modul IS eranet umožňujúci riadenie procesu kvalifikácie a registrácie dodávateľov.
Verejné obstarávanie	Modul IS eranet umožňujúci riadenie procesu verejného obstarávania, ktorý je zapísaný do Zoznamu elektronických prostriedkov v súlade so zákonom zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vyhlášky č. 73/2022 Z. z. ktorou sa ustanovujú obsahové náležitosti dotazníka na zápis do zoznamu elektronických prostriedkov na elektronickú komunikáciu vo verejnom obstarávaní.
Interné obstarávanie	Modul IS eranet umožňujúci riadenie procesov interného obstarávania v súlade so zákonom č. 513/1991 Obchodný zákonník a o zmene a doplnení niektorých zákonov v znení neskorších predpisov; a v súlade s internou smernicou Objednávateľa, vrátane elektronickej komunikácie a elektronického príjmu ponúk.
Elektronická aukcia	Modul IS eranet umožňujúci uskutočňovanie elektronických aukcií prostredníctvom virtuálnej aukčnej siene. IS eranet je integrovaný s certifikovanou elektronickou aukciou, ktorá spĺňa požiadavky kladené zákonom č. 343/2015 Z. z. o verejnom

	obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vyhláškou Úradu pre verejné obstarávanie č. 132/2016, ktorou sa ustanovujú podrobnosti o postupe certifikácie systémov na uskutočnenie elektronickej aukcie v znení neskorších predpisov.
Súvisiace služby	Služby poskytované Poskytovateľom podľa výberu Objednávateľa v nasledujúcich rozsahoch: Aktualizácia, Archivácia, Hosting, Záloha, Používateľská podpora a Odborné poradenstvo.
Aktualizácia	Automatické priebežné aktualizácie (najmä opravy, aktualizácie dát, databáz) a bezpečnostné aktualizácie IS eranet, aktualizácia IS eranet v súlade so zmenami platnej legislatívy Slovenskej republiky (implementácia legislatívnych zmien).
Archivácia	Archivácia dát Objednávateľa v IS eranet sa vykonáva vždy ku koncu kalendárneho roka vo forme exportu všetkých dokumentov a dokladov Objednávateľa v IS eranet do jedného súboru, ktorý bude najneskôr do jedného mesiaca po skončení daného kalendárneho roka sprístupnený Objednávateľovi na stiahnutie.
Hosting	Prevádzkovanie IS eranet, vrátane súvisiacich databáz, a údržby a správy dát Objednávateľa na serveroch Poskytovateľa.
Záloha	Automatické zálohovanie dát Objednávateľa vykonávané minimálne raz denne počas posledných 14 kalendárnych dní a raz týždenne počas posledných 12 mesiacov.
Používateľská podpora	Používateľská podpora a asistencia Poskytovateľa Objednávateľovi a ním povereným osobám (Administrátorom) ako aj uchádzačom verejného obstarávania uskutočňovaná emailom alebo telefonicky v pracovných dňoch v čase od 8:00 do 16:00 hod. prostredníctvom kontaktov uvedených na osobitnej subdoméne eranet.sk zriadenej Objednávateľovi v zmysle Prílohy č. 1 tejto Zmluvy.
Odborné poradenstvo	Odborné poradenstvo pri realizácii procesov verejných obstarávaní v zmysle zákona o verejnom obstarávaní poskytované emailom alebo telefonicky Poskytovateľom, v rozsahu a podľa požiadaviek Objednávateľa, v pracovných dňoch v čase od 8:00 do 16:00 hod. prostredníctvom kontaktov uvedených na osobitnej subdoméne eranet.sk zriadenej Objednávateľovi v zmysle Prílohy č. 1 tejto Zmluvy.
Administrátor	Zamestnanec alebo iná osoba poverená Objednávateľom na uskutočňovanie všetkých úkonov týkajúcich sa správy a konfigurácie IS eranet v rámci možností udeleného prístupu Poskytovateľom k IS eranet.
Obstarávateľ	Zamestnanec alebo iná osoba poverená Objednávateľom na uskutočňovanie konkrétnych verejných obstarávaní v IS eranet v prospech a v súlade s potrebami Objednávateľa.
Iný používateľ	Zamestnanec alebo iná osoba poverená Objednávateľom na uskutočňovanie konkrétnych aktivít v IS eranet v prospech

	a v súlade s potrebami Objednávateľa. Napr. pozorovateľ, člen komisie, zadávateľ požiadavky v module Plánovanie, a pod.
Človekodeň	je násobok základnej jednotky práce. Človekodeň je práca jedného človeka po dobu ôsmich hodín (ďalej aj „MD").
Človekohodina	je základná jednotka práce. Človekohodina je práca jedného človeka po dobu jednej hodiny (ďalej tiež „MH").
Servisná požiadavka	požiadavka na Poskytovateľa od Objednávateľa na informáciu, radu a pod. Vznik požiadavky je iniciovaný výpadkom alebo obmedzením funkčnosti IS eranet.
Service Desk	je jednotný kontaktný bod medzi Objednávateľom a Poskytovateľom, ktorí prijíma, riadi a monitoruje Vady, Problémy a Zmenové požiadavky.
Problém	akákoľvek v danom čase neznáma (alebo predpokladaná) príčina vzniku viacerých existujúcich, alebo potenciálne možných Vád.
Vada	je akákoľvek udalosť, ktorá spôsobí neplánovaný výpadok IS eranet alebo obmedzenie jeho funkčnosti a má dopad na biznis alebo podnikové činnosti Objednávateľa.
Workaround	náhradné riešenie – je riešenie Vady/ Problému, ktoré zastrešuje alebo eliminuje jeho dopad.

IV. PREDMET ZMLUVY

4.1. Poskytovateľ touto Zmluvou udeľuje Objednávateľovi oprávnenie používať IS eranet v nasledujúcich moduloch: Plánovanie, Kvalifikácia dodávateľov, Verejné obstarávanie, Interné obstarávanie, Elektronická aukcia a Hodnotenie dodávateľov, vzdialeným prístupom cez internetové rozhranie https://sepsas.eranet.sk/, a zároveň sa zaväzuje poskytnúť Objednávateľovi Súvisiace služby v rozsahu: Aktualizácia, Archivácia, Hosting, Záloha, Používateľská podpora a Odborné poradenstvo, a to na obdobie trvania tejto Zmluvy podľa čl. V Zmluvy a za podmienok uvedených v tejto Zmluve.

4.2. Poskytovateľ sa touto Zmluvou zaväzuje poskytnúť Objednávateľovi podporu pri implementácií IS eranet a ďalšie služby, ktorých detailný popis je uvedený v Prílohe č. 1 – Rozsah poskytovaných služieb a Prílohe č. 2 – Implementačné a integračné služby, ktoré tvoria neoddeliteľnú súčasť tejto Zmluvy.

4.3. Objednávateľ sa zaväzuje Poskytovateľovi uhradiť odmenu vo výške a spôsobom dohodnutým v článku VI tejto Zmluvy.

V. ČAS A MIESTO PLNENIA

5.1. Poskytovateľ sa zaväzuje poskytovať služby v rozsahu podľa Prílohy č. 1 (Rozsah pravidelne poskytovaných služieb) v termíne od 1.1.2024 do 31.12.2027.

5.2. Poskytovateľ sa zaväzuje poskytovať služby v rozsahu podľa Prílohy č. 2 (Implementačné a integračné služby) v súlade s termínmi plnenia míľnikov podľa bodov 5.2.1 až 5.2.3:

5.2.1. Míľnik č. 1 Analýza procesu obstarávania a návrh riešenia v termíne do 2 mesiacov od nadobudnutia účinnosti tejto Zmluvy.

5.2.2. Míľnik č. 2 Implementácia, testovanie, revidovanie nastavenia informačného systému, zaškolenie zamestnancov a nasadenie systému do prevádzky v termíne do 31.12.2023.

5.2.3. Míľnik č. 3 Integrácia na informačné systémy v termíne do 8 mesiacov od nadobudnutia účinnosti tejto Zmluvy.

5.3. Poskytovateľ nie je oprávnený takto stanovený termín plnenia meniť bez dohody s Objednávateľom. Záväzok poskytovať služby v zmysle bodu 5.2 alebo jeho častí je splnený jeho odovzdaním a prevzatím zástupcami oboch Zmluvných strán oprávnenými rokovať vo veciach technických na mieste stanovenom v tejto Zmluve.

5.4. Miestom realizácie a odovzdania je sídlo spoločnosti Slovenská elektrizačná prenosová sústava, a. s., Mlynské nivy 59/A, Bratislava.

VI. CENA A PLATBA ZA POSKYTOVANÉ SLUŽBY

6.1. Cena za poskytovanie služieb v rozsahu podľa čl. V tejto Zmluvy je stanovená dohodou Zmluvných strán podľa § 3 zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov.

Cena je tvorená:

6.1.1. Cenou za pravidelne poskytované služby za kalendárny rok, uvedené v bode 5.1 tejto Zmluvy vo výške 20 000,00 EUR/rok bez DPH, slovom: dvadsaťtisíc EUR/rok bez DPH a

6.1.2. Cenou za služby poskytované v rámci implementačných a integračných služieb podľa bodu 5.2 tejto Zmluvy v celkovej výške 104 737,50 EUR bez DPH, slovom: stoštyritisícsedemstotridsaťsedem EUR bez DPH,

Rozpis cien poskytovaných služieb podľa bodu 6.1 tvorí Prílohu č. 8 tejto Zmluvy.

6.2. K cene bude fakturovaná DPH v zmysle zákona číslo 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej aj ako „zákon o DPH").

6.3. V cene dohodnutej podľa bodu 6.1 tejto Zmluvy sú zahrnuté všetky náklady Poskytovateľa za poskytované služby.

VII. PLATOBNÉ PODMIENKY

7.1. Zmluvné strany sa dohodli na ročných platbách vo výške stanovenej podľa bodu 6.1.1 tejto Zmluvy.

7.2. Cenu za kalendárny rok stanovenú podľa bodu 6.1.1 tejto Zmluvy za poskytovanie služieb v rozsahu podľa bodu 4.1 tejto Zmluvy Objednávateľ uhradí na základe faktúry vystavenej Poskytovateľom a doručenej Objednávateľovi do 15 dní pred začiatkom kalendárneho roka, v ktorom budú predmetné služby poskytované. Poskytovateľ doručí predmetnú faktúru najneskôr 60 dní pred začiatkom kalendárneho roka, v ktorom budú predmetné služby poskytované.

7.3. Zmluvné strany sa dohodli na úhrade ceny stanovenej podľa bodu 6.1.2 tejto Zmluvy prostredníctvom viacerých platieb naviazaných na splnenie jednotlivých míľnikov, pričom právo na zaplatenie časti zmluvnej ceny podľa jednotlivých míľnikov vzniká Poskytovateľovi riadnym odovzdaním a prevzatím záväzku zástupcami oboch Zmluvných strán oprávnenými rokovať vo veciach technických na mieste stanovenom v tejto Zmluve nasledovne:

7.3.1. Míľnik č.1 v rozsahu bodu 5.2.1 10 500,00 EUR bez DPH.

7.3.2. Míľnik č.2 v rozsahu bodu 5.2.2 58 187,50 EUR bez DPH.

7.3.3. Míľnik č.3 v rozsahu bodu 5.2.3 36 050,00 EUR bez DPH.

7.4. Cenu za jednotlivé odovzdané časti v zmysle bodov 7.3.1 až 7.3.3 uhradí Objednávateľ na základe faktúr, ktoré Poskytovateľ vystaví do 15 dní odo dňa vzniku daňovej povinnosti a doručí Objednávateľovi. Dňom vzniku daňovej povinnosti je deň prevzatia časti záväzku formou protokolu o odovzdaní a prevzatí. Poskytovateľ je oprávnený vystaviť faktúru na základe protokolu o odovzdaní a prevzatí podpísaného obidvomi Zmluvnými stranami.

7.5. Faktúra sa považuje za doručenú v listinnej (tlačenej) forme na adresu sídla Objednávateľa, alebo 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.

7.6. Objednávateľ podpisom tejto Zmluvy udeľuje Poskytovateľovi súhlas v zmysle ustanovenia § 71 ods. 1 písm. b) zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len "zákon o DPH"), aby vystavoval a spracúval faktúry v elektronickej forme, za podmienky predchádzajúceho informovania Objednávateľa o používaní elektronického spôsobu 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 v elektronickej forme bude v oznámení uvedená aj e-mailová adresa, z ktorej budú faktúry odosielané.

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

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

7.10. K cene bude fakturovaná DPH podľa zákona o DPH platným v deň vzniku daňovej povinnosti. Faktúra musí obsahovať všetky náležitosti podľa zákona o DPH, označenie čísla tejto Zmluvy podľa evidencie Objednávateľa a číslo bankového účtu v tvare IBAN. Povinnou prílohou faktúry je originál preberacieho protokolu o vykonaných prácach podpísaný za Objednávateľa osobou oprávnenou rokovať vo veciach technických.

7.11. V prípade, že faktúra nebude obsahovať náležitosti uvedené v bode 7.10 tejto Zmluvy, je Objednávateľ oprávnený vrátiť ju Poskytovateľovi. V takom prípade sa preruší plynutie lehoty splatnosti a nová lehota splatnosti začne plynúť doručením opravenej faktúry Objednávateľovi.

7.12. Lehota splatnosti faktúry je 30 dní od jej doručenia Objednávateľovi.

7.13. V prípade, že Objednávateľ cenu uvedenú v odseku 1 tohto článku Zmluvy a vystavenej faktúry nezaplatí riadne a včas, Zmluvné strany sa dohodli, že Poskytovateľ je oprávnený po písomnom upozornení a po uplynutí stanovenej primeranej dodatočnej lehoty znemožniť Objednávateľovi prístup do IS eranet do doby, než bude dohodnutá cena Objednávateľom uhradená. Objednávateľovi neskorším zaplatením a nemožnosťou používania IS eranet nevzniká nárok na predĺženie platnosti a účinnosti Zmluvy podľa trvania dohodnutého v čl. V tejto Zmluvy. Objednávateľ je zároveň povinný uhradiť

Poskytovateľovi poplatok vo výške 300,- EUR (slovom: tristo eur) za obnovenie prístupu do IS eranet. Poskytovateľ nezodpovedá za škodu spôsobenú Objednávateľovi, ktorá vznikla znemožnením prístupu do IS eranet z dôvodu uvedeného v tomto odseku. Zodpovednosť za náhradu škody spôsobenej Poskytovateľovi, tým nie je dotknutá.

7.14. V prípade omeškania Objednávateľa s úhradou zmluvnej ceny na základe predloženej faktúry má Poskytovateľ právo na uplatnenie úroku z omeškania vo výške 1M EURIBOR + 8% p.a. z dlžnej sumy za každý deň omeškania (pri 360 dňovom účtovnom roku). 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.

VIII. BEZPEČNOSŤ PRI PRÁCI A OCHRANA PRED POŽIARMI

8.1. Poskytovateľ zodpovedá za bezpečnosť a ochranu zdravia vlastných zamestnancov a pracovníkov subdodávateľských spoločností a je povinný dodržiavať ustanovenia Všeobecných zmluvných podmienok zabezpečovania BOZP a OPP - Príloha č. 9 tejto Zmluvy.

8.2. Poskytovateľ sa zaväzuje pri realizácii služieb v objektoch Objednávateľa dodržiavať miestne prevádzkové predpisy, dopravné značenie a zásady zabezpečovania BOZP a PO. Poskytovateľ prehlasuje, že sa s obsahom uvedených predpisov oboznámi po podpise tejto Zmluvy pri prvom vstupe do areálu Objednávateľa.

IX. PRÁVA A POVINNOSTI OBJEDNÁVATEĽA

9.1. Objednávateľ sa zaväzuje užívať IS eranet výlučne pre svoje potreby v súlade s jeho určením, na dosiahnutie účelu tejto Zmluvy a za podmienok stanovených touto Zmluvou.

9.2. Objednávateľ sa zaväzuje, že IS eranet bude používať v súlade s platným právom, dobrými mravmi a touto Zmluvou a tiež, že nebude narúšať alebo poškodzovať IS eranet, servery, siete a systémy s ňou spojené, uverejňovať či používať spamy, softvérové vírusy alebo akékoľvek iné kódy, súbory alebo programy, ktoré by mohli prerušiť, obmedziť, ukončiť alebo akokoľvek inak poškodiť prevádzkovanie IS eranet alebo jeho funkčnosť.

9.3. Všetky činnosti Objednávateľa v rozpore s touto Zmluvou, ktoré súčasne tiež môžu mať za následok (hoci aj prípadné) ohrozenie funkčnosti IS eranet, či všetky činnosti Objednávateľa, ktoré by akýmkoľvek spôsobom ohrozovali autorské práva či iné oprávnenia, budú zo strany Poskytovateľa posudzované ako podstatné porušenie tejto Zmluvy a Poskytovateľ je oprávnený Objednávateľa v takejto jeho činnosti obmedziť. Takéto obmedzenie spočíva najmä v zamedzení prístupu k IS eranet, pričom opatrenia smerujúce k obmedzeniu takejto činnosti Objednávateľa je Poskytovateľ oprávnený uplatniť okamžite.

9.4. Objednávateľ sa zaväzuje pre využívanie IS eranet stanoviť Administrátorov, ktorí budú jediní oprávnení spravovať a konfigurovať IS eranet na základe individuálnych prihlasovacích údajov udelených Poskytovateľom.

9.5. Objednávateľ sa zaväzuje dodržiavať podmienky a pravidlá používania IS eranet uvedené v tejto Zmluve, ako aj zabezpečiť dodržiavanie týchto podmienok a pravidiel osobami oprávnenými alebo poverenými Objednávateľom používať IS eranet (najmä Administrátor, Obstarávateľ, Iný používateľ).

9.6. Objednávateľ sa zaväzuje primerane zabezpečiť prístup do IS eranet tak aby nedošlo k jeho zneužitiu, a to najmä, aby nedošlo k neoprávnenému vstupu do IS eranet osobou, ktorá k tomu nie je oprávnená. Objednávateľ je povinný vykonať všetky opatrenia nevyhnutné na zamedzenie úniku prihlasovacích údajov a hesiel IS eranet neoprávneným osobám. Objednávateľ v plnom rozsahu zodpovedá za škodu, ktorá vznikla jemu, Poskytovateľovi alebo tretím osobám v súvislosti s neoprávneným vstupom do IS eranet alebo únikom prihlasovacích údajov.

9.7. Objednávateľ sa zaväzuje vykonávať práva a plniť povinnosti podľa tejto Zmluvy s riadne a včas.

9.8. Objednávateľ súhlasí s tým, aby Poskytovateľ uvádzal názov a logo Objednávateľa, kontaktnú osobu, všeobecný popis poskytnutých služieb, a dobu ich poskytovania ako svoju referenciu a zároveň tieto údaje použil aj vo svojich materiáloch určených na marketingové použitie.

9.9. Objednávateľ sa zaväzuje chrániť IS eranet v zmysle bodov 9.9.1. až 9.9.4.:predchádzajúceho písomného súhlasu Poskytovateľa oprávnený:

9.9.1. Predať, prenajímať, požičiavať alebo iným spôsobom sprístupniť IS eranet tretej osobe (za neoprávnené sprístupnenie sa nepovažuje sprístupnenie Administrátorovi, Obstarávateľovi, Inému používateľovi),

9.9.2. IS eranet rozmnožovať, meniť, prekladať, rekompilovať, reassemblovať a vracať do predchádzajúceho stavu,

9.9.3. Rozmnožovať, zostavovať alebo rozširovať produkty odvodené od IS eranet,

9.9.4. Rozmnožovať, prekladať či meniť akúkoľvek dokumentáciu k IS eranet poskytnutú Poskytovateľom s výnimkou jej použitia pre interné účely resp. účely, pre ktoré bol IS eranet dodaný.

Porušenie týchto záväzkov zo strany Objednávateľa zakladá právo Poskytovateľa od tejto Zmluvy odstúpiť a zamedziť prístup Objednávateľa do IS eranet. Zodpovednosť za náhradu škody spôsobenej Poskytovateľovi, tým nie je dotknutá.

9.10. Objednávateľ sa zaväzuje poskytnúť všetku nevyhnutnú súčinnosť Poskytovateľovi pri plnení predmetu tejto Zmluvy a to najmä pri dodaní IS eranet a jeho implementácií, ako aj ďalšiu súčinnosť, ktorú si Poskytovateľ od Objednávateľa vopred vyžiada aspoň 2 (dva) dni pred nutnosťou jej poskytnutia, pokiaľ nebude z objektívnych dôvodov potrebná dlhšia lehota. Objednávateľ nemá voči Poskytovateľovi nárok na akúkoľvek náhradu nákladov spojených s poskytnutou súčinnosťou. V prípade omeškania Objednávateľa s poskytnutím súčinnosti Poskytovateľovi sa lehoty uvedené v tejto Zmluve, na ktoré má vplyv dané omeškanie Objednávateľa s poskytnutím súčinnosti predlžujú o dobu omeškania Objednávateľa s poskytnutím súčinnosti. Poskytovateľ nezodpovedá za škodu zapríčinenú v dôsledku omeškania Objednávateľa s poskytnutím súčinnosti alebo neposkytnutia súčinnosti zo strany Objednávateľa.

9.11. V prípade, že v rámci plnenia tejto Zmluvy dochádza k spracovaniu osobných údajov Zmluvnými stranami, Zmluvná strana, ktorá vykonáva spracúvanie osobných údajov je povinná dodržiavať ustanovenia 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 a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, za čo aj zodpovedá.

X. PRÁVA A POVINNOSTI POSKYTOVATEĽA

10.1. Poskytovateľ sa zaväzuje, že do termínov definovaných v článku V umožní Objednávateľovi prístup k IS eranet cez osobitnú subdoménu eranet.sk.

10.2. Poskytovateľ sa zaväzuje v súlade s predmetom tejto Zmluvy umožniť Objednávateľovi prístup do IS eranet a poskytnúť Súvisiace služby s odbornou starostlivosťou, riadne a včas, a to za predpokladu poskytnutia potrebnej súčinnosti Objednávateľom a včasného plnenia ďalších záväzkov Objednávateľa. Poskytovateľ je povinný raz ročne zaslať Objednávateľovi prevádzkový report s vyhodnotením poskytovania služby, ktorý bude akceptovaný oboma stranami.

10.3. Umožnením prístupu k IS eranet Objednávateľovi v zmysle ods. 1 tohto článku Zmluvy nastáva riadne a včasné odovzdanie IS eranet Objednávateľovi Poskytovateľom. Odovzdanie podľa predchádzajúcej vety nastáva dňom podpísania akceptačného protokolu zástupcami oboch Zmluvných strán oprávnených rokovať vo veciach technických. Poskytovateľ vyhlasuje, že IS eranet bude Objednávateľ môcť využívať v kvalite, ktorú je možné rozumne očakávať s prihliadnutím na jeho povahu, účel, odmenu za jeho sprístupnenie a podmienky používania v zmysle tejto Zmluvy.

10.4. Poskytovateľ nenesie zodpovednosť za prerušenie poskytovania Súvisiacich služieb, odcudzenie či stratu dát a nemožnosť prístupu do IS eranet zavinené zásahom vyššej moci (požiar, zemetrasenie, a pod.), pokiaľ preukázateľne nebol schopný týmto skutočnostiam zabrániť alebo im predísť.

10.5. Poskytovateľ zabezpečuje, aby IS eranet mal náležitosti požadované platnými právnymi predpismi, nenesie však žiadnu zodpovednosť za správnosť, úplnosť a bezchybnosť údajov vyplnených Objednávateľom, ani žiadne riziká a zodpovednosť za škodu spojenú s jeho používaním.

10.6. Poskytovateľ garantuje 99,5% dostupnosť IS eranet v príslušnom kalendárnom roku. Výnimku tvoria plánované a vopred ohlásené odstávky IS eranet za účelom údržby, opráv alebo Aktualizácie, ktoré budú realizované mimo pracovných dní alebo vo večerných hodinách. Počas nahlásenej neopravenej vady kategórie „Veľmi vysoká" podľa bodu 11.1. je IS eranet považovaný za nedostupný.

10.7. Poskytovateľ nemonitoruje činnosť Objednávateľa v IS eranet ako ani obsah, ktorý doň vkladá. Obsah Objednávateľa Poskytovateľ nevlastní, nie je oprávnený ho upravovať, či akokoľvek inak meniť bez predchádzajúceho súhlasu Objednávateľa.

10.8. Poskytovateľ môže meniť aj bez súhlasu Objednávateľa podobu a štruktúru IS eranet a to najmä pri Aktualizácií, pričom každú zmenu podoby a štruktúry IS eranet musí Poskytovateľ oznámiť Objednávateľovi aspoň 5 dní pred jej zavedením.

10.9. Poskytovateľ nezodpovedá za akýkoľvek obsah (napr. údaje, materiály, podklady, dokumentáciu) vložený Objednávateľom do IS eranet a to najmä za jeho správnosť, úplnosť, bezchybnosť, legálnosť. Poskytovateľ nezodpovedá najmä za porušovanie práv duševného vlastníctva ani iných práv Objednávateľom. Poskytovateľ nie je zodpovedný ani za cudzí obsah (napr. externé webové stránky tretích osôb, odkazy na ne, reklamný obsah) umiestnený Objednávateľom v IS eranet.

10.10. Poskytovateľ podpisom tejto zmluvy vyhlasuje, že :

a) nie je ruský štátny podnik alebo fyzická osoba s pobytom v Rusku,

b) nie je právnická osoba, subjekt alebo orgán usadený v Rusku, právnická osoba, subjekt alebo orgán, ktoré z viac ako 50 % priamo alebo nepriamo vlastní subjekt uvedený v písmene a) tohto odseku,

c) nie je právnická alebo fyzická osoba, subjekt alebo orgán, ktoré konajú v mene alebo na základe pokynov subjektu uvedeného v písmene a) alebo b) tohto odseku.

10.11. Poskytovateľ je povinný oznámiť bez zbytočného odkladu Objednávateľovi akékoľvek zmeny, ktoré majú za následok zmeny v rámci jeho vlastníckej alebo organizačnej štruktúry, ktoré by mali za následok porušenie jeho vyhlásenia v zmysle bodu 10.10, a to kedykoľvek od podpisu tejto zmluvy a počas trvania zmluvného vzťahu.

10.12. V prípade, že v rámci plnenia tejto Zmluvy dochádza k spracovaniu osobných údajov Zmluvnými stranami, Zmluvná strana, ktorá vykonáva spracúvanie osobných údajov je povinná dodržiavať ustanovenia 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 a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, za čo aj zodpovedá.

XI. ZODPOVEDNOSŤ ZA VADY

11.1. Vady zistené po odovzdaní IS eranet Poskytovateľom Objednávateľovi, Objednávateľ ohlási písomne Poskytovateľovi bez zbytočného odkladu. Objednávateľ musí podrobne špecifikovať vadu a určiť prioritu vady. Poskytovateľ je oprávnený po oboznámení sa s Objednávateľovým ohlásením vady zmeniť prioritu vady, pričom rozhodujúce je určenie priority vady Poskytovateľom. Poskytovateľ garantuje dobu odozvy a dobu vykonania opravy v zmysle nižšie uvedenej tabuľky vo väzbe na prioritu vady.

Kategória vady	**Popis vady**	**Doba odozvy**	**Doba vykonania opravy**
Veľmi vysoká	IS eranet nefunguje vôbec po dobu dlhšiu ako 20 minút, a/alebo IS eranet alebo niektorú jeho kľúčovú funkciu alebo modul nie je možné používať a nemožno použiť ani náhradné riešenie (workaround), čo bráni Objednávateľovi v riadnom riadení bežiacich procesov verejných obstarávaní, a/alebo výpadky IS eranet pri jeho štandardnom zaťažení pri bežnom režime práce tri alebo viackrát za deň, a/alebo nie je zabezpečený súlad s aktuálne platnou legislatívou. Podmienkou je, že musí byť garantovaný súlad obsahu systému s aktuálne platným znením zákona vždy ku dňu účinnosti novely zákona o verejnom obstarávaní.	do 3 hodín (v pracovné dni)	do 1 pracovného dňa

Vysoká	Funkčnosť IS eranet je narušená tak, že dochádza k významnému spomaleniu jeho výkonu, a/alebo došlo k dočasnému vyriešeniu kritickej chyby formou náhradného riešenia (workaround), a/alebo dochádza k výpadkom dohodnutej funkcionality alebo modulov IS eranet, zatiaľ čo zostávajúce funkcionality alebo moduly sú aj naďalej funkčné, a/alebo dochádza k takým výpadkom funkcionality alebo modulov IS eranet, ktoré spôsobujú nutnosť Objednávateľa vykonávať činnosti navyše, zložitejšie pristupovať k funkciám alebo iným spôsobom obchádzať vadu, čo prácu s IS eranet spomaľuje a robí ju nepohodlnou.	do 2 pracovných dní	do 7 pracovných dní
Normálna	Akákoľvek vada nespadajúca do ostatných kategórií.	do 3 pracovných dní	do 15 pracovných dní

11.2. Doba odozvy je doba, v ktorej Poskytovateľ zaeviduje hlásenie vady. Doba vykonania opravy je doba, do ktorej je Poskytovateľ povinný vadu odstrániť od jej zaevidovania Poskytovateľom. Pokiaľ z povahy vady vyplýva, že na odstránenie vady je potrebná dlhšia doba, Poskytovateľ je povinný o tom Objednávateľa bezodkladne písomne upovedomiť.

11.3. Ak Zmluvná strana poruší svoje povinnosti alebo akýkoľvek záväzok vyplývajúci z tejto Zmluvy, je povinná nahradiť škodu tým spôsobenú druhej zmluvnej strane v súlade s § 373 a nasl. Obchodného zákonníka, ak v zmluve nie je dohodnuté inak.

11.4. V prípade vzniku škody sa bude nahrádzať iba skutočná škoda a nie ušlý zisk ani náklady vynaložené poškodenou Zmluvnou stranou v dôsledku porušenia povinnosti druhej Zmluvnej strany.

11.5. Zmluvná strana, ktorá porušila svoju povinnosť alebo akýkoľvek záväzok vyplývajúci z tejto Zmluvy, sa môže zbaviť zodpovednosti za škodu ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku vyplývajúceho z tejto Zmluvy došlo v dôsledku okolností vylučujúcich zodpovednosť.

11.6. Okolnosťou vylučujúcou zodpovednosť je prekážka, ktorá nastala nezávisle na vôli povinnej strany a bráni jej v splnení jej povinnosti, ak je nemožné rozumne predpokladať, že by povinná strana túto prekážku alebo jej následky odvrátila alebo prekonala a ďalej, že by v čase vzniku prekážku predvídala, či mohla alebo mala predvídať.

11.7. Ak okolnosti vylučujúce zodpovednosť nastanú, potom je Zmluvná strana, u ktorej táto skutočnosť nastane, povinná bezodkladne informovať druhú Zmluvnú stranu o povahe, začiatku a konci trvania takejto prekážky, ktorá bráni splneniu povinností podľa tejto

Zmluvy. Zmluvné strany sa zaväzujú vyvinúť maximálne úsilie na odvrátenie a prekonanie okolností vylučujúcich zodpovednosť.

11.8. Zodpovednosť však nie je vylúčená v prípade, keď takáto okolnosť vznikla až v čase, keď povinná strana bola v omeškaní s plnením svojej povinnosti, alebo ak predmetná Zmluvná strana nesplní svoju povinnosť bezodkladne informovať druhú Zmluvnú stranu o povahe a začiatku trvania prekážky, alebo ak vznikla z jej hospodárskych pomerov. Účinky vylučujúce zodpovednosť sú obmedzené len na obdobie, kým trvá prekážka, s ktorou sú tieto účinky spojené.

11.9. Ak okolnosti vylučujúce zodpovednosť trvajú 45 (štyridsaťpäť) dní a dlhšie, môže druhá Zmluvná strana písomným oznámením zaslaným povinnej Zmluvnej strane od Zmluvy odstúpiť s účinnosťou od doručenia oznámenia o odstúpení povinnej Zmluvnej strane.

11.10. Proces riešenia vád je popísaný v Prílohe č. 1 tejto Zmluvy.

XII. ÚROKY Z OMEŠKANIA, ZMLUVNÉ POKUTY, NÁHRADA ŠKODY

12.1. V prípade, že Poskytovateľ bude v omeškaní s poskytovanými službami, pokiaľ toto omeškanie nie je zapríčinené vinou Objednávateľa, môže si Objednávateľ uplatniť zmluvnú pokutu vo výške 0,1 % z ceny v zmysle bodu 6.1.za každý deň omeškania, maximálne však v celkovej výške 10 % z ceny v zmysle bodu 6.1.

12.2. Ak Poskytovateľ nezačne s odstraňovaním prípadných vád počas platnosti tejto Zmluvy v lehote dohodnutej podľa bodu 11.1. tejto Zmluvy, môže Objednávateľ uplatniť zmluvnú pokutu vo výške 0,1 % z celkovej zmluvnej ceny za každý kalendárny deň omeškania, maximálne však v celkovej výške 10 % z ceny v zmysle bodu 6.1.

12.3. Ak Poskytovateľ neodstráni prípadné vady počas doby platnosti tejto Zmluvy v lehote dohodnutej podľa bodu 11.1. tejto Zmluvy, môže Objednávateľ uplatniť zmluvnú pokutu vo výške 0,1 % z celkovej zmluvnej ceny za každý kalendárny deň omeškania, maximálne však v celkovej výške 10 % z ceny v zmysle bodu 6.1.

12.4. Za každé jednotlivé porušenie povinnosti podľa článku VIII. tejto Zmluvy je Objednávateľ oprávnený uplatniť si u Poskytovateľa zmluvnú pokutu vo výške uvedenej v Prílohe č.4 tejto Zmluvy.

12.5. Za každé jednotlivé porušenie povinnosti podľa článku XIV. tejto Zmluvy je Objednávateľ oprávnený uplatniť si u Poskytovateľa zmluvnú pokutu vo výške 5 000 EUR (slovom päťtisíc eur).

12.6. Za každé jednotlivé porušenie povinnosti podľa bodu 10.10 tejto Zmluvy je Poskytovateľ povinný zaplatiť zmluvnú pokutu vo výške 5 000 EUR (slovom päťtisíc eur). Dohodou o zmluvnej pokute nie je dotknutý nárok Objednávateľa na náhradu škody vo výške prevyšujúcej zmluvnú pokutu.

12.7. Nárok na zmluvnú pokutu podľa tohto článku tejto Zmluvy je Objednávateľ povinný uplatniť si u Poskytovateľa písomnou formou. Uplatnením zmluvnej pokuty nezaniká Objednávateľovi právo na náhradu škody spôsobenej Poskytovateľom porušením zmluvných povinností. Zmluvná strana je oprávnená požadovať aj náhradu škody prevyšujúcu zmluvnú pokutu.

XIII. OKOLNOSTI VYLUČUJÚCE ZODPOVEDNOSŤ

13.1. Pre účely tejto Zmluvy sa na okolnosti vylučujúce zodpovednosť vzťahuje právna úprava uvedená v § 374 Obchodného zákonníka.

13.2. Okolnosti vylučujúce zodpovednosť sú okolnosti, ktoré nie sú závislé od vôle Zmluvných strán, a ktoré Zmluvné strany nemôžu ovplyvniť, ako napr. vojna, mobilizácia, povstanie, živelné pohromy, teroristický čin a pod.

XIV. OCHRANA DÔVERNÝCH INFORMÁCIÍ

14.1. V tejto Zmluve "dôverné informácie" znamenajú všetky informácie, ktoré sa týkajú alebo môžu týkať predmetu plnenia tejto Zmluvy, 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.

14.2. Ďalšie práva a povinnosti Zmluvných strán vo vzťahu k zabezpečeniu primeranej úrovne dôvernosti, dostupnosti a integrity informácií definuje Príloha č. 6 tejto Zmluvy.

XV. VZÁJOMNÁ KOMUNIKÁCIA

15.1. Komunikácia súvisiaca s touto Zmluvou, môžu byť uskutočnená prostredníctvom pošty (doporučená zásielka) alebo elektronickej pošty, a to aj bez elektronického podpisu.

15.2. V prípade doručovania poštou je adresou pre doručovanie zásielok sídlo jednotlivých Zmluvných strán uvedené v záhlaví tejto Zmluvy. Písomnosť doručovaná poštou sa považuje za doručenú ak ju adresát prevzal, dňom prevzatia adresátom, ak ju odmietol adresát prevziať, dňom odmietnutia prevziať písomnosť. V prípade, ak si adresát písomnosť neprevezme v úložnej lehote na pošte, ak sa písomnosť vráti odosielateľovi s označením pošty „adresát neznámy" alebo „adresát sa odsťahoval" alebo s inou poznámkou podobného významu, za deň doručenia sa považuje deň vrátenia zásielky odosielateľovi, a to aj vtedy, ak sa adresát o tom nedozvie

15.3. V prípade doručovania elektronickou poštou je adresou pre doručovanie elektronickej pošty emailová adresa jednotlivých kontaktných osôb Zmluvných strán uvedená v bode 15.4. tohto článku Zmluvy, ak nebola ohlásená Zmluvnou stranou jej zmena. Elektronická pošta sa považuje za doručenú dňom nasledujúcim po dni jej odoslania na emailovú adresu podľa tohto odseku, aj keď nebola adresátom prečítaná.

15.4. Kontaktné osoby pre vzájomnú komunikáciu sú:

za Objednávateľa: meno a priezvisko: Ing. Tomáš Mondik
pracovné zaradenie: špecialista
telefón a e-mail:
meno a priezvisko: Ing. Karol Haluška
pracovné zaradenie: špecialista

	telefón a e-mail:	
za Poskytovateľa	meno a priezvisko:	Ing. Martin Oravec
	pracovné zaradenie:	konzultant
	telefón a e-mail:	
	meno a priezvisko:	Ing. Mojmír Prídavok, PhD
	pracovné zaradenie:	konateľ
	telefón a e-mail:	

V prípade ak dôjde pri nezmenenom pracovnom zaradení len k zmene konkrétnej fyzickej osoby (vrátane e-mailu a telefónu) v tomto pracovnom zaradení, takáto zmena nepredstavuje zmenu tejto Zmluvy a nie je preto potrebné vyhotoviť dodatok k Zmluve.

XVI. OPRÁVNENIE A POUŽÍVANIE

16.1. Oprávnenie využívať IS eranet a Súvisiace služby podľa tejto Zmluvy je neprenosné a časovo obmedzené na dobu trvania tejto Zmluvy. Objednávateľ môže používať IS eranet len pre svoje potreby a len prostredníctvom svojich zamestnancov alebo Objednávateľom poverených osôb. Objednávateľ nie je oprávnený k prevodu a/alebo prechodu svojich práv k predmetu tejto Zmluvy tretej osobe bez písomného súhlasu Poskytovateľa. Porušenie týchto záväzkov zo strany Objednávateľa zakladá právo Poskytovateľa od tejto Zmluvy odstúpiť a zamedziť prístup Objednávateľa do IS eranet. Zodpovednosť za náhradu škody spôsobenej Poskytovateľovi, tým nie je dotknutá.

XVII. UKONČENIE ZMLUVY

17.1. Túto Zmluvu je možné ukončiť dohodou Zmluvných strán, výpoveďou alebo odstúpením od Zmluvy.

17.2. Za podstatné porušenie tejto Zmluvy v zmysle ustanovení § 344 a nasl. Obchodného zákonníka a teda dôvodom na okamžité odstúpenie Objednávateľa od tejto Zmluvy sa považuje:

17.2.1. Opakované neplnenie povinností Poskytovateľa zakotvených v tejto Zmluve a to ani v dodatočnej lehote na odstránenie nedostatkov stanovenej Objednávateľom v predchádzajúcej písomnej výzve.

17.2.2. 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 § 40 ods. 8 písm. a) a c) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých predpisov.

17.2.3. Porušenie vyhlásenia a povinnosti Poskytovateľa podľa bodu 10.10 a 10.11 tejto Zmluvy.

17.3. Nepodstatným porušením tejto Zmluvy sa rozumie nedodržanie ostatných zmluvných podmienok tejto Zmluvy okrem podmienok uvedených v bode 17.2. Na nepodstatné porušenie tejto Zmluvy Objednávateľ Poskytovateľa písomne upozorní. Po opakovanom porušení tej istej zmluvnej povinnosti je Objednávateľ oprávnený od tejto Zmluvy odstúpiť.

17.4. Ktorákoľvek Zmluvná strana je oprávnená túto Zmluvu vypovedať, a to z akéhokoľvek dôvodu alebo bez udania dôvodu. Výpovedná doba je 6 (šesť) mesiacov a začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej Zmluvnej strane. Zmluvné strany sa dohodli, že túto Zmluvu sú Zmluvné strany oprávnené vypovedať najskôr po 2 (dvoch) rokoch odo dňa účinnosti tejto Zmluvy.

17.5. V prípade vypovedania Zmluvy zo strany Poskytovateľa alebo Objednávateľa pred uplynutím doby, na ktorú už bola Poskytovateľovi uhradená dohodnutá cena, je Poskytovateľ povinný vrátiť pomernú časť uhradenej ceny Objednávateľovi v lehote 14 (štrnástich) dní odo dňa zániku Zmluvy.

17.6. V prípade ukončenia Zmluvy bude mať Objednávateľ bezodplatne aj naďalej prístup k IS eranet, avšak iba za účelom prezerania už realizovaných procesov a úkonov v IS eranet, bez možnosti jeho aktívneho využívania, a to po dobu 10 rokov. V prípade ak má Objednávateľ v zmysle zákona o verejnom obstarávaní povinnosť uchovávať všetky doklady a dokumenty dlhšie obdobie ako 10 rokov, bude táto lehota nahradená lehotou stanovenou v zákone o verejnom obstarávaní; po uplynutí tejto doby dôjde k nenávratnému zrušeniu prístupu k IS eranet a všetkým dokumentom, dokladom, údajom a dátam Objednávateľa. Po uplynutí tejto doby je Poskytovateľ oprávnený všetky tieto doklady, dokumenty, údaje a dáta vymazať, s čím Objednávateľ bezvýhradne súhlasí. Objednávateľ nemá voči Poskytovateľovi žiaden nárok na náhradu škody v dôsledku takéhoto vymazania dokladov, dokumentov, údajov a dát.

17.7. Odstúpením od tejto Zmluvy podľa bodu 17.2.3. nie je dotknuté právo Objednávateľa na náhradu škody.

XVIII. ZÁVEREČNÉ USTANOVENIA

18.1. Táto Zmluva sa uzatvára na dobu určitú do 31.12.2027.

18.2. Táto Zmluva nadobúda platnosť dňom jej podpisu oboma Zmluvnými stranami a účinnosť dňom nasledujúcim po jej zverejnení v centrálnom registri zmlúv (www.crz.gov.sk).

18.3. Túto Zmluvu je možné meniť alebo dopĺňať len dohodou Zmluvných strán písomnými, vzostupne číslovanými a obojstranne podpísanými dodatkami.

18.4. Zmluvné strany sa dohodli, že žiadna z nich nie je oprávnená postúpiť svoje práva a povinnosti vyplývajúce z tejto Zmluvy tretej strane bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany.

18.5. Práva a záväzky vyplývajúce pre Zmluvné strany z tejto Zmluvy prechádzajú na prípadných právnych nástupcov Zmluvných strán. Pred zánikom či rozdelením má zanikajúca či deliaca sa Zmluvná strana povinnosť oznámiť túto skutočnosť druhej Zmluvnej strane.

18.6. 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 tejto 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.

18.7. Táto Zmluva je vypracovaná v štyroch rovnopisoch, z ktorých každá zo Zmluvných strán dostane po dve vyhotovenia.

18.8. Zmluvné strany vyhlasujú, že táto 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.

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

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

18.11. 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.

18.12. Zoznam subdodávateľov podľa Prílohy č. 10 je možné meniť len na základe vzájomnej dohody oboch zmluvných strán formou dodatku k tejto Zmluve, ktorého obsahom bude nový zoznam subdodávateľov.

18.13. 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.

18.14. Nedeliteľnou súčasťou tejto Zmluvy sú tieto prílohy:

Príloha č. 1 – Rozsah poskytovaných služieb

Príloha č. 2 – Implementačné a integračné služby
Príloha č. 3 – Vymedzenie rozsahu a spôsobu plnenia bezpečnostných opatrení
Príloha č. 4 – Bezpečnostné opatrenia laKB dodávateľov SEPS
Príloha č. 5 – Požiadavky na vzdialený prístup
Príloha č. 6 – Všeobecné podmienky zachovania mlčanlivosti
Príloha č. 7 – Proces riadenia zmenových požiadaviek
Príloha č. 8 – Rozpis cien poskytovaných služieb
Príloha č. 9 – Všeobecné zmluvné podmienky zabezpečenia BOZP a OPP
Príloha č. 10 – Zoznam subdodávateľov

V Bratislave dňa .....
Objednávateľ:

.....

Ing. Jaroslav Vach
predseda predstavenstva

Mgr. Martin Riegel
člen predstavenstva

V ..... dňa .....
Poskytovateľ:

.....

Ing. Mojmír Prídavok, PhD
konateľ

ROZSAH POSKYTOVANÝCH SLUŽIEB

1. Elektronický proces plánovania a zberu požiadaviek na obstarávanie

1.1 Zber požiadaviek do ročného plánu obstarávania z gestorských úsekov obstarávateľa,
1.2 Systém umožní zber požiadaviek v rámci ročného plánovania a následné upresnenie špecifikácie požiadaviek ich autormi podľa bodu 1.3,
1.3 Funkcionalita hromadného importu požiadaviek minimálne vo formáte: .xls alebo.xlsx.,
1.4 Formulár na zadanie požiadavky na obstarávanie musí obsahovať najmä: názov požiadavky, klasifikácia CPV alebo vlastná klasifikácia, technická a funkčná špecifikácia, očakávaný termín dodania, predpokladaná hodnota, prijímateľ tovaru/služby, poznámky a prílohy,
1.5 Vstavané komunikačné rozhranie určené na komunikáciu medzi referátom verejného obstarávania a jednotlivými autormi požiadaviek. História komunikácie musí byť vedená pre každú požiadavku samostatne a dostupná po náhľade vlastností danej požiadavky,
1.6 Viackrokové schvaľovanie požiadaviek podľa hierarchie schvaľovania objednávateľa. Systém musí umožňovať nastavenie min. ôsmych úrovní schvaľovania,
1.7 Systémové logy procesu schvaľovania, ktoré budú používateľom systému zobrazované,
1.8 Automatické spočítavanie predpokladaných hodnôt v rámci klasifikácie CPV alebo vlastnej kategorizácie obstarávateľa,
1.9 Generovanie štruktúrovaného ročného plánu verejného a interného obstarávania s možnosťou jeho editácie a schvaľovania. Po prijatí požiadavky na obstarávanie, ktorá nie je zahrnutá v ročnom pláne obstarávania sa ročný plán aktualizuje,
1.10 Export ročného plánu verejného obstarávania vo formáte: .xls, .xlsx, .pdf.,
1.11 Automatické aktualizovanie stavu požiadavky na obstarávanie podľa fázy jej spracovania (v min. rozsahu: v procese schvaľovania/ schválená/ zamietnutá/ v procese VO).

2. Elektronické obstarávanie

2.1 Zadávanie neobmedzeného počtu zákaziek postupmi podľa zákona o verejnom obstarávaní č. 343/2015 Z. z., a internými postupmi Obstarávateľa.
2.2 Spracovanie všetkých etáp verejného a interného obstarávania elektronicky, vrátane komunikácie medzi obstarávateľom a uchádzačom alebo obstarávateľom a členmi komisie.
2.3 Integrovaná prehľadná pracovná plocha používateľa s dostupnosťou aktuálneho prehľadu o zákazkách, ich aktuálneho stavu, prehľad najbližších termínov a úloh z nich vyplývajúcich.
2.4 Možnosť vytvoriť si vlastný harmonogram pre jednotlivé postupy zadávania zákaziek, vrátane nastavenia notifikácii a automatických prepočtov lehôt pre jednotlivé kroky harmonogramu.
2.5 Automatické generovanie nastavených harmonogramov pre jednotlivé postupy zadávania zákaziek, vrátane možnosti úpravy vygenerovaných harmonogramov pričom pri zmene príslušného dátumu (míľnika) musí automaticky editovať všetky ostatné dátumy (míľniky) v súlade s nastavením harmonogramu.

2.6 Automatické notifikácie o blížiacej sa expirácii záväzných termínov podľa nastavenia harmonogramu, vrátane zvýraznenia blížiacich sa záväzných termínov zadávania zákaziek v kalendári na pracovnej ploche.
2.7 Evidencia a úprava katalógu dodávateľov, pričom údaje o dodávateľoch sa budú z katalógu automaticky načítavať do údajov o záujemcoch/ uchádzačoch v rámci realizovaných zákaziek.
2.8 Evidencia záujemcov/uchádzačov/účastníkov zákaziek s automatickým naťahovaním údajov z vlastného katalógu dodávateľov
2.9 Zverejňovanie dokumentov podľa bodu 2.10 ako aj registrovaným záujemcom/uchádzačom/účastníkom zákaziek.
2.10 Systémový profil na zverejňovanie dokumentov v súlade s § 64 ods.4.
2.11 Elektronická komunikácia v rámci organizácie objednávateľa a medzi organizáciou verejného obstarávateľa a záujemcami/ uchádzačmi/ účastníkmi zákaziek. Systém umožňuje preukázateľne zachytiť dátum a čas prečítania správy a zobraziť ho verejnému obstarávateľovi.
2.12 Elektronický príjem žiadostí o dokumentáciu k zákazke/ žiadostí o vysvetlenie/ žiadostí o nápravu.
2.13 Elektronický príjem ponúk podľa § 20.
2.14 Jednokolové a dvojkolové otváranie ponúk. Systém neumožní otvorenie ponúk skôr, ako je dátum otvárania. Po otvorení sa zaznamená dátum a čas otvorenia, ktorý nie je editovateľný.
2.15 Možnosť vytvárania hodnotiacich tabuliek priamo v systéme. Systém umožňuje hodnotenia na úroveň požadovaných dokladov/dokumentov.
2.16 Automatické hodnotenie ponúk podľa vopred nastavených hodnotiacich kritérií, so stanovením poradia uchádzačov. Systém musí podporovať hodnotenie na ekonomicky najvýhodnejšiu ponuku, ktorá je daná:
  2.16.1 Nákladmi životného cyklu (TCO)
  2.16.2 Najnižšou cenou
  2.16.3 Najlepším pomerom ceny a kvality
2.17 Automatický prepočet mimoriadne nízkej cenovej ponuky uchádzačov, v prípade ak sa vyhodnocujú aspoň 3 cenové ponuky.
2.18 Nástroj na vytváranie, archivovanie a editáciu šablón dokumentov podľa zákona č. 343/2015 Z. z. Systém musí disponovať vlastnou sadou systémových šablón dokumentov vytváraných podľa zákona č. 343/2015 Z. z. s automatickým vypĺňaním údajov dostupných v systéme (v rozsahu podľa platnej legislatívy) s možnosťou ich úpravy. Pre všetky podporované postupy podľa bodu 2.1 sa požadujú šablóny uvádzané v rámci verejného obstarávania. Aplikovať aj pre interné obstarávanie.

Obstarávateľ vyžaduje šablóny dokumentov v min. rozsahu:

  2.18.1 Súťažné podklady
  2.18.2 Zápisnice z otvárania a vyhodnotenie ponúk
  2.18.3 Zápisnice zo splnenia podmienok účasti
  2.18.4 Informácie o výsledku
  2.18.5 Dokumentácie pre členov komisie
  2.18.6 Správa podľa § 24 ods. 3
  2.18.7 Zoznamy záujemcov, uchádzačov, členov komisie
  2.18.8 Obálka a uznesenie do orgánov spoločnosti

2.19 Do systémových šablón uvedených v bode 2.18 sa budú automaticky naťahovať údaje dostupné v systéme v min. rozsahu:
- 2.19.1 Údaje definované v Oznámení o vyhlásení verejného obstarávania/ Výzve na predkladanie ponúk
- 2.19.2 Zoznamy záujemcov, uchádzačov, členov komisie
- 2.19.3 Poradie uchádzačov a ich návrhy na plnenie kritérií
- 2.19.4 Podpisové tabuľky pre členov komisie

2.20 Export systémom generovaných dokumentov podľa bodu 2.18 a 2.19 do formátov .doc/docx, .pdf.

2.21 Generovanie protokolov z elektronickej komunikácie, elektronického príjmu ponúk a zverejňovania. Protokoly budú needitovateľnými logmi zo systému, ktoré sa budú týkať akejkoľvek elektronickej komunikácie v systéme, vrátane doručenia ponúk.

2.22 Integrácia na ISZÚ prevádzkovaného Úradom pre verejné obstarávania SR. Systém musí umožňovať prenos informácií do nasledujúcich formulárov ISZÚ.
- 2.22.1 Oznámenie o vyhlásení verejného obstarávania
- 2.22.2 Výzva na predkladanie ponúk
- 2.22.3 Oznámenie podľa § 166 zákona č. 343/2015 Z. z.
- 2.22.4 Oznámenie o výsledku verejného obstarávania
- 2.22.5 Referencie

Počet polí, do ktorých sa údaje prenášajú bude tvoriť minimálne 70% z celkového počtu každého formulára.

2.23 Definovanie minimálne nasledujúcich rolí, ktoré musia byť delegovateľné iným používateľom pomocou administrátorských nastavení:
- 2.23.1 používateľ administrujúci konkrétny postup zadávania zákazky
- 2.23.2 člen komisie na prípravu zákazky (vidí a administruje len prípravu)
- 2.23.3 člen komisie na vyhodnotenie (vidí a administruje proces hodnotenia)
- 2.23.4 pozorovateľ (vidí celú zákazku bez možnosti administrovania).

2.24 Reporting - vytváranie štatistík a reportov. Systém automaticky dopĺňa údaje do preddefinovaných reportov v min. rozsahu:
- 2.24.1 Dátum vyhlásenia verejného obstarávania a označenia VVO, v ktorom bolo verejné obstarávanie vyhlásené
- 2.24.2 Dátumy otvárania ponúk/ ponúk časť „Ostatné"/ponúk časť „Kritériá"
- 2.24.3 Dátum podpisu a ukončenia zmluvy
- 2.24.4 Počet prijatých ponúk / účastníkov aukcie
- 2.24.5 Predpokladaná hodnota zákazky/ Zazmluvnená hodnota / Úspora.

2.25 Systém musí zaznamenávať všetky vykonané aktivity jednotlivých používateľov prostredníctvom needitovateľných logov.

3. Podpora

3.1 Zabezpečenie bezpečnosti a plynulosti prevádzky informačného systému s dostupnosťou minimálne 99,5%.

3.2 Zabezpečenie bezplatného súladu s aktuálne platnou legislatívou. Musí byť garantovaný súlad obsahu systému s aktuálne platným znením zákona vždy ku dňu účinnosti novely zákona o verejnom obstarávaní. Rozpor medzi obsahom systému a aktuálne platným znením zákona o verejnom obstarávaní je považovaný za vadu kategórie „Veľmi vysoká".

3.3 Zálohovanie dát
- 3.3.1 Zálohovanie sa rozdeľuje na dve logické časti:

3.3.1.1 Prvou je záloha platformy resp. celého virtuálneho servera, ktorá sa vykonáva raz týždenne. Takáto záloha je pripravená na restore / obnovu v priebehu niekoľkých desiatok minút. Záloha dát sa vykonáva denne. Dáta a nastavenia sú aktuálne ku dňu poslednej zálohy,

3.3.1.2 Druhou časťou backup procesu je záloha zákazníckych databáz a aplikačných logov. Databázy obsahujú aktuálne dáta potrebné ku kompletnej obnove požadovanej služby. Logy obsahujú informácie o všetkých úkonoch/zmenách vykonaných priamo v systéme IS eranet. Záloha produkčných databáz a logov prebieha každý pracovný deň v nočných hodinách. Predmetné zálohy dát budú exportované a sprístupnené Objednávateľovi vopred dohodnutým spôsobom minimálne raz za kalendárny rok.

3.3.2 Pri vytváraní sú zálohy šifrované a kopírované na dve samostatné, vzájomne nezávislé úložiská. Jedna záloha je vo forme full backup zálohy. Táto záloha je zároveň chránená voči prepisovaniu, je zapnuté verzionovanie a možnosť obnovy vymazanej zálohy (ak medzi vymazaním a potrebou obnovy neprešlo viac ako 3 dni). Druhá záloha je vykonávaná ako rozdielová a nie je zabezpečená voči vymazaniu/prepisovaniu.

3.4 Nahlasovanie požiadaviek na Service Desk

3.4.1 Objednávateľ nahlasuje požiadavky na Vady, Servisné požiadavky a Zmenové požiadavky prostredníctvom Service Desku, v ktorom sú tieto požiadavky evidované a riadené pracovníkmi Poskytovateľa.

3.4.2 Poskytovateľ garantuje dobu odozvy a dobu vykonania opravy v zmysle tabuľky uvedenej v Zmluve v čl. 11 a v bode 11.1 vo väzbe na prioritu vady.

3.5 Riešenie Vád/ Problémov

3.5.1 V rámci manažmentu Vád/Problémov bude Poskytovateľ vykonávať minimálne tieto aktivity:

3.5.1.1 - Prijatie a potvrdenie nahlásenia Vady/Problému

3.5.1.2 - Investigácia a diagnostika

Parameter	Maximálne trvanie/ objem	Kontakt
Service Desk/ Telefonická podpora	Od 8:00 hod. – do 16:00 hod. počas pracovných dní	+421 948 877 665
Service Desk/ Emailová podpora	Od 8:00 hod. – do 16:00 hod. počas pracovných dní	podpora@eranet.sk

3.5.1.3 - Informácia o zahájení riešenia

3.5.1.4 - Informácia o postupe riešenia

3.5.1.5 - Riešenie a oprava

3.5.1.6 - Informácia o ukončení riešenia

3.5.2 Poskytovateľ bude v súčinnosti s Objednávateľom vykonávať riadenie Problémov s cieľom eliminovať a redukovať výskyt Vád určením príčin ich vzniku. Poskytovateľ v rámci dodania riešenia Vady poskytne Objednávateľovi aj identifikáciu príčiny Vady.

3.5.3 Prijatie Vady/ Problému - akákoľvek Vada/Problém predložený Poskytovateľovi bude obsahovať minimálne tieto atribúty:

3.5.3.1 Kontaktná osoba Zákazníka,

3.5.3.2 Popis Vady/Problému (vrátane relevantných dostupných príloh ako napríklad „print screens, log files"),

3.5.3.3 Replikačný scenár (popis spôsobu, ako Vada/Problém replikovať v danom prostredí), ak je Vada/Problém replikovateľný, resp. ak je možné ho popísať,

3.5.3.4 Priorita Vady/Problému,

3.5.3.5 Dátum a čas predloženia.

3.5.4 Prijatie Vady/Problému

3.5.4.1 Poskytovateľ preberie Vadu/Problém prostredníctvom Service Desku a poskytne Objednávateľovi potvrdenie o jej prevzatí.

3.5.4.2 Poskytovateľ reaguje podľa termínov stanovených v zmysle parametrov uvedených v tejto Zmluve na základe uvedenej úrovne priority Vady/Problému. Každá reakcia na predloženú Vadu/Problém bude spĺňať minimálne nasledovné atribúty:

3.5.4.2.1 ID (ak bolo poskytnuté Objednávateľom, rovnaké ako pôvodné),

3.5.4.2.2 Dátum a čas vyrozumenia,

3.5.4.2.3 Informácia o stave spracovania Vady/Problému.

3.5.5 Investigácia a diagnostika Vady

V prípade, ak sa počas analýzy ukáže, že príčina Vady je v aplikácii tretích strán resp. v infraštruktúre Objednávateľa alebo tretej strany (napr. databáza, aplikačný server alebo iná súčasť, ktorá je podmienkou funkčnosti IS eranet), je Poskytovateľom po schválení zo strany Objednávateľa vygenerovaná požiadavka na systémové riešenie. V prípade, že je servis aplikácií tretích strán krytý zmluvným vzťahom medzi Objednávateľom a treťou stranou, bude na strane Objednávateľa určený zodpovedný zástupca, ktorý bude sprostredkovať komunikáciu medzi Poskytovateľom a treťou stranou až do úplného odstránenia Vady. Poskytovateľ je aj tak v tomto prípade povinný poskytnúť Objednávateľovi nevyhnutnú súčinnosť. V rámci nevyhnutnej súčinnosti budú poskytnuté zo strany Poskytovateľa všetky dostupné informácie k Vade týkajúce sa IS eranet.

3.5.6 Riešenie a oprava Vady/Problému

3.5.6.1 Vada/Problém sa považuje za odstránený pokiaľ IS eranet sa stane pre Objednávateľa opätovne dostupný a plne funkčný v zmysle požiadaviek uvedených v tejto Zmluve.

3.5.6.2 Neakceptované (odmietnuté) riešenie bude ďalej spracovávané Poskytovateľom s použitím rovnakého procesu ako pre zaobchádzanie s novými Vadami/Problémami, ale pri zachovaní pôvodného ID Vady/Problému a pri pokračovaní plynutia času od prvotného predloženia Vady/Problému.

3.5.7 Zamietnutie Vady/Problému

Poskytovateľ je oprávnený zamietnuť nahlásenú Vadu/Problém v prípade, že nie je pokrytý touto Zmluvou.

3.6 Performance parametre IS eranet

Poskytovateľ definuje kľúčové performance parametre IS eranet, definujúce minimálne parametre, ktoré musí systém plniť počas trvania tejto Zmluvy, pričom Poskytovateľ sa zaväzuje vykonávať všetky aktivity na systéme tak, aby boli dodržané performance parametre produktu.

Parameter	Maximálne trvanie/ objem
Doba dostupnosti	- Dostupnosť: 99,50 % - Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní. - Nedostupnosť IS eranet sa počíta od reálneho času celkového výpadku počas prevádzkových hodín alebo, ak nie

	je možné potvrdiť reálny čas, od nahlásenia incidentu Objednávateľom v čase dostupnosti Service Desku Poskytovateľa (t.j. nahlásenie incidentu na L3 v čase od 8:00 hod. - do 16:00 hod. počas pracovných dní). - Do dostupnosti IS eranet nie sú započítavané vopred ohlásené servisné okná a plánované odstávky IS eranet

Prevádzkové časy, servisné okná a plánované odstávky

Parameter	Maximálne trvanie/ objem
Prevádzkové hodiny	Od 6:00 hod. – do 18:00 hod. počas pracovných dní
Servisné okná a plánované odstávky	Od 19:00 hod. – do 5:00 hod. počas pracovných dní Od 00:00 hod. – do 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov Realizácia servisných zásahov (servisné okná) je vždy vopred ohlásená a mimo prevádzkových hodín (pracovného času).

Implementačné a integračné služby

1. Implementácia systému a ďalšie požiadavky.

1.1 Implementácia šablón

1.1.1 Zapracovanie nových automaticky generovaných šablón k IO
- kontrola a analýza zaslaných šablón pre IO,
- formátovanie šablón v rámci IS eranet,
- v každej časti zákazky možnosť generovať preddefinované šablóny, do ktorých budú doplnené údaje na základe zákazky,
- kontrola aktuálnych hashov pre doťahovanie dát zo zákazky,
- pridanie nových hashov pre doťahovanie dát zo zákazky.

1.1.2 Možnosť nastaviť pätu a hlavičku generovaných dokumentov + číslovanie strán
- možnosť separátnej päty a hlavičky dokumentov,
- pre každý dokument separátny výber,
- preddefinované hlavičky a päty na základe šablóny,
- možnosť upravovať šablóny pre pätu a hlavičku dokumentu,
- možnosť zvoliť automatické číslovanie strán.

1.1.3 Úprava / doplnenie atribútov v zákazke (interný postup – IO)
- úprava / doplnenie atribútov v zákazke pre interné obstarávanie na základe požiadaviek.

1.1.4 Protokol (šablóna) generovaná po schválení požiadaviek (do 33 tis., nad 33 tis. a rámcová dohoda)
- dopracovanie šablón generovaných v rámci požiadaviek na základe vzoru,
- doťahovanie všetkých údajov vyplnených v požiadavkách.

1.2 Implementácia schvaľovania a ďalšie požiadavky

1.2.1 Implementácia procesu interného obstarávania
- úpravy harmonogramov pre súťaže na základe interných procesov s možnosťou notifikovania používateľov,
- úpravy preddefinovaných požiadaviek na ponuku,
- všeobecné úlohy pri implementácii procesu interného obstarávania.

1.2.2 Zapracovanie požiadavky - Požiadavka IO (do 33 tis. a nad 33 tis.)
- analýza parametrov pre požiadavky IO na základe interných dokumentov,
- zapracovanie nového modulu – požiadavky IO,
- možnosť zadefinovať povinné parametre požiadavky,
- implementácia nových typov požiadavky (do 33 tis. a nad 33 tis.),
- zapracovanie nových atribútov na základe vzoru požiadavky,
- úprava schvaľovacieho procesu požiadaviek IO na základe interného schvaľovania z možnosťou schválenia priamo v emaile.

1.2.3 Zapracovanie požiadavky - Rámcová dohoda
- analýza parametrov pre požiadavku – Rámcová dohoda,
- zapracovanie nového modulu – požiadavky RD,
- implementácia nového typu požiadavky,
- zapracovanie nových atribútov na základe vzoru požiadavky,

- úprava schvaľovacieho procesu požiadavky IO na základe interného schvaľovania z možnosťou schválenia priamo v emaile.

1.3 Hodnotenie dodávateľov

1.3.1 Hodnotenie dodávateľov po dodávke predmetu zákazky

- dopracovanie nového modulu - Hodnotenie dodávateľov po dodávke predmetu zákazky,
- možnosť separátneho hodnotenia dodávateľa po dodaní predmetu zákazky,
- postup hodnotenia dodávateľa na základe internej smernice,
- zapracované hodnotiace hárky pre hodnotenie dodávateľa podľa druhu zákazky (tovar, služba, stavebná práca),
- automatické prepočty % pre výsledné hodnotenie dodávateľa,
- automatické notifikácie pre používateľov v procese hodnotenia,
- história hodnotenia dodávateľa,
- automatické prepočty hodnotenia dodávateľa pre nasledujúce obdobie na základe min obdobia,
- prehľadná tabuľka hodnotenia dodávateľa,
- filtrovanie dodávateľa pri zasielaní výzvy na základe hodnotenia,
- odfiltrovanie dodávateľov, ktorí získali stav „nevyhovujúci“,
- delegovanie hodnotenia - možnosť hodnotenia vybranou osobou,
- všetky funkcionality na základe internej smernice hodnotenia dodávateľa po dodávke predmetu zákazky.

1.4 Modul štatistiky

- dopracovanie novo pridaných parametrov z požiadaviek / zo zákaziek do modulu štatistiky pre možnosť generovania prehľadných štatistík,
- možnosť nastavenia preddefinovaných šablón vybraných parametrov pre zostavenie štatistiky,
- exportovanie štatistík do excel súboru,
- možnosť nastaviť automatické generovanie štatistik vo vopred zadefinovanom čase.

1.5 Úvodné školenie používateľov systému určených Objednávateľom

- zabezpečenie úvodného predstavenia a školenia hlavných užívateľov informačného systému,
- vypracovanie manuálov a postupov pre používateľov systému.

1.6 Prvotné nastavenie systému v rozsahu

- organizačná štruktúra a prístupy do systému,
- zaslanie notifikačných mailov pre subjekty zaradené v zozname dodávateľov,

2. Integrácie na ďalšie systémy

2.1 Integrácia na IS SAP (modul MM)

- na základe typu žiadanky (žiadanka v hodnote od 3300€ do 3300 € / žiadanka nad 33000€ / žiadanka vytvorená na základe rámcovej dohody) možnosť vytvoriť priamo zo systému IS eranet POBJ v SAP MM,
- vytvorenie POBJ v SAP MM na základe údajov vyplnených v IS eranet,
- synchronizácia číselníkov jednotlivých parametrov SAP – IS eranet (automatická + manuálna synchronizácia),
- zobrazenie prehľadu objednávky (na základe typu žiadanky) vopred zadefinovaným používateľom,

- možnosť pre vopred zadefinované osoby doplnenia údajov objednávky (na základe číselníkov zo SAP MM) v IS eranet a následné odoslanie objednávky do modulu POBJ v SAP MM.
- integrácia bude realizovaná prostredníctvom integračnej platformy Objednávateľa na základe Zmluvnými stranami odsúhlasenej špecifikácie dodanej Poskytovateľom.

2.2 Integrácia na spisovú službu– registratúru
- automaticky generované referenčné číslo zákazky vo vopred stanovenom formáte,
- nový atribút referenčne číslo – možné editovať manuálne zodpovednou osobou,
- možnosť vyhľadávania / filtrovania v prehľade zákaziek podľa novo pridaných referenčných čísiel,
- pre každý novo pridaný dokument zadefinované presné referenčne číslo vo vopred stanovenom formáte (rozdielne označenie interných dokumentov / dokumentov od dodávateľov),
- automatické generovanie protokolov po ukončení zákazky,
- po ukončení zákazky zablokovanie možnosti editovania (editovanie povolené len na základe povolenia administrátora/vopred zadefinovanej osoby v systéme),
- vymazávanie zákaziek zo systému na základe žiadosti o vyradenie od SEPS.
- integrácia bude realizovaná prostredníctvom integračnej platformy Objednávateľa na základe Zmluvnými stranami odsúhlasenej špecifikácie dodanej Poskytovateľom.

2.3 Integrácia na verejné registre (RPVS, ORSR, Zoznam hospodárskych subjektov ÚVO, Finstat)

2.3.1 Register partnerov verejného sektora
- používatelia majú možnosť priamo v IS eranet overiť zápis dodávateľa v RPVS,
- v rámci prehľadu dodávateľa zobrazený prehľad aktuálnych údajov dodávateľa z RPVS,
- zobrazenie základných informácii z RPVS,
- informácie o oprávnených osobách z RPVS,
- informácie o konečných užívateľových výhod z RPVS,
- zobrazenie dátumov overenia konečných užívateľoch výhod z RPVS.

2.3.2 Obchodný register
- prehľadná karta údajov dodávateľa kde má používateľ zobrazené informácie o dodávateľovi v IS eranet z Obchodného registra,
- nastavená automatická validácia údajov spoločnosti vyplnených pri registrácii oproti údajom dotiahnutých z OR, kedy bude používateľ informovaný v prípade ak by mal dodávateľ rôzne údaje uvedené v IS eranet a OR.

2.3.3 Zoznam hospodárskych subjektov
- používatelia majú možnosť priamo v IS eranet overiť zápis dodávateľa v ZHS pre preukázanie spôsobilosti na uzatváranie zmlúv alebo rámcových dohôd vo verejnom obstarávaní z hľadiska splnenia podmienok účasti týkajúcich sa osobného postavenia,
- prehľadná karta údajov dodávateľa na základe údajov dodávateľa uvedených v Zozname hospodárskych subjektov,
- zobrazenie základných informácii dodávateľa uvedených v ZHS priamo v IS eranet,
- registračné čísla a platnosti zápisu dodávateľa v ZHS priamo v IS eranet.

2.3.4 Finstat

- prehľadná karta ekonomických údajov na základe dát z Finstat kedy si používateľ vie priamo v IS eranet pozrieť široké spektrum finančných ukazovateľov a informácii o finančnej kondícií dodávateľa,
- zobrazenie základných údajov dodávateľa,
- grafické znázornenie jednotlivých dôležitých udalostí (napr. či má dodávateľ dlhy a nedoplatky, pohľadávky voči štátu, či je dodávateľ konkurze reštrukturalizácií atď.),
- grafické znázornenie ziskov / tržieb/ celkových výnosov dodávateľa.

2.4 Modul dodávatelia

2.4.1 Modul dodávatelia – prehľad údajov z jednotlivých systémov pre jednoduchú analýzu dodávateľa

- v rámci „Modulu dodávateľov" pridaná separátna sekcia prehľadu dodávateľa na základe údajov z jednotlivých systémov (integrácia - Finstat / RPVS / Obchodný register / Zoznam hospodárskych subjektov),
- údaje prehľadne zobrazené na jednotlivých kartách „Prehľadu dodávateľa" so zobrazenými aktuálnymi informáciami z jednotlivých systémov.

2.4.2 Zobrazenie údajov prehľadu dodávateľa v zákazke

- novo pridaná prehľadná karta informácii o uchádzačoch priamo v rámci zákazky bez nutnosti vyhľadávania dodávateľov (systém automaticky zobrazí informácie o jednotlivých uchádzačoch v danej zákazke na separátnej karte),
- zobrazenie údajov v prehľadnej tabuľke s rýchlou identifikáciou údajov dodávateľov s možnosťou zobrazenia detailných informácii z jednotlivých systémov.

Vymedzenie rozsahu a spôsobu plnenia bezpečnostných opatrení (požadovaných vyhláškou č. 362/2018 Z. z.)

Oblasť	Referencia na vyhlášku č. 362/2018 Z. z.	Špecifikácia legislatívnej požiadavky	Spôsob plnenia bezpečnostného opatrenia	Požadovaná dokumentácia
a)	§ 5 písm. a)	Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej **zásada určenia manažéra kybernetickej bezpečnosti**, ktorý: 1. má možnosť predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby, 2. zabezpečuje aplikáciu bezpečnostných opatrení v systéme riadenia kybernetickej bezpečnosti, 3. je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a 4. spĺňa znalostné štandardy na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu.	Rola manažéra kybernetickej bezpečnosti v prostredí spoločnosti je určená s definovanými kompetenciami.	
a)	§ 5 písm. b)	Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej **zásada najnižších privilégií**, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh.	Zásada najnižších privilégií a požiadavka na jej dodržiavanie je definovaná v riadiacej dokumentácii organizácie.	
a)	§ 5 písm. c)	Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej **zásada oddeľovania zodpovedností**, podľa ktorej žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity	Zásada oddeľovania zodpovedností a požiadavka na jej dodržiavanie je definovaná v riadiacej dokumentácii organizácie.	
a)	§ 5 písm. d)	Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej **zásada dodržiavania a vykonávania nezávislého hodnotenia**, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrenie rizík.	Kontrolnú zložku a úlohu nezávislého hodnotenia opatrení kybernetickej bezpečnosti v prostredí SEPS plní interný audit.	
a)	§ 5 písm. e)	Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej **zásada jasného vymedzenia právomoci, povinnosti a zodpovednosti**, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností.	Právomoci, povinnosti a zodpovednosti sú vymedzené v popise pracovnej pozície, pracovnej zmluve, príp. prostredníctvom špecifických poverení.	

b)	§ 6 ods. 1	Riadenie aktív, hrozieb a rizík je proces spojený s finančnými, zmluvnými a inventarizačnými funkciami na podporu riadenia životného cyklu informačných technológií a konfiguračných položiek. Účelom riadenia aktív, hrozieb a rizík je zabezpečiť ochranu aktív podľa ich hodnoty.	V spoločnosti je zavedený proces riadenia aktí. Aktivity realizované v súvislosti s kybernetickou bezpečnosťou sú zosúladené s týmito korporátnymi procesmi.	
b)	§ 6 ods. 2	Všetky aktíva súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami sú identifikované a inventár týchto aktív je centrálne zaznamenaný a riadený.	Zoznam komponentov implementovaného riešenia (CMDB konfiguračných položiek) dodať aj v elektronickej forme.	Inventárny zoznam aktív
b)	§ 6 ods. 3	Riadenie aktív pozostáva z identifikácie a evidencie všetkých a) aktív, od ktorých závisí poskytovanie základnej služby, b) podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie, c) zodpovedných osôb za identifikáciu a evidenciu aktív a d) vlastníkov aktív.	Organizácia vedie evidenciu sietí a informačných systémov a inventárny zoznam aktív v rozsahu požadovanom legislatívou.	
b)	§ 6 ods. 4	Rovnaká ochrana sa neuplatňuje pre všetky druhy aktív. Na tento účel sa aktíva klasifikujú a kategorizujú postupom podľa § 4.	V spoločnosti je zavedená klasifikácia informácií a kategorizácia sietí a informačných systémov zohľadňuje požiadavky platnej legislatívy.	
b)	§ 6 ods. 5	Ukončením pracovného pomeru alebo iného obdobného pracovného vzťahu zamestnancov prevádzkovateľa základnej služby a zamestnancov tretích strán sa zadokumentovaným spôsobom vracajú späť všetky zverené aktíva.	Postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného sú súčasťou postupov riadenia ľudských zdrojov. Používateľ pri ukončení pracovného pomeru alebo obdobného pracovného vzťahu odovzdá jemu zverené aktíva spoločnosti v súlade s pokynmi poskytovateľa.	

b)	§ 6 ods. 6	Riadenie rizík pozostáva z a) identifikácie zraniteľností, b) identifikácie hrozieb, c) identifikácie a analýzy rizík s ohľadom na aktívum, d) určenia vlastníka rizika, e) implementácie organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením, f) analýzy funkčného dopadu a g) pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.	V procese riadenia rizík, vrátane riadenia bezpečnostných rizík, resp. rizík kybernetickej bezpečnosti, sú náležitým spôsobom zohľadnené požiadavky platnej legislatívy.	
b)	§ 6 ods. 7	Identifikácia rizika sa vykonáva na základe princípu najhoršieho scenára, ktorý môže nastať aj pri nízkej pravdepodobnosti. Na určenie úrovne identifikovaného rizika sa vopred nastaví súbor pravidiel, ktoré umožnia na základe štandardných a opakovateľných postupov určiť merateľné a objektívne úrovne rizika pre najhoršie scenáre.	Identifikácia rizika sa vykonáva na základe princípu najhoršieho scenára, ktorý môže nastať aj pri nízkej pravdepodobnosti. Kritériá hodnotenia rizík sú vopred stanovené.	
b)	§ 6 ods. 8	Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva.	Pri analýze rizík je hodnotená pravdepodobnosť vzniku a potenciálny dopad vzniku škodlivej udalosti z hľadiska narušenia dôvernosti, integrity alebo dostupnosti.	
b)	§ 6 ods. 9	Identifikácia hrozieb je založená na identifikácii aktív a ich vlastníkov a identifikácii zraniteľností potenciálne pôsobiacich na tieto aktíva.	V procese riadenia rizík, vrátane riadenia bezpečnostných rizík, resp. rizík kybernetickej bezpečnosti, sú náležitým spôsobom zohľadnené požiadavky platnej legislatívy.	
b)	§ 6 ods. 10	Pre potreby analýzy rizík sa zoznam hrozieb združuje do jednotlivých skupín tak, že je možné tento zoznam použiť univerzálne pre väčšinu aktív. Pre jednotlivé aktíva sú hodnotené len hrozby relevantné pre konkrétne aktívum. Hrozby sa rozdeľujú podľa ich pôvodu do kategórií najmenej ako a) úmyselné hrozby pre všetky úmySEPSlné aktivity zamerané na aktíva, b) náhodné hrozby pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť aktíva, c) hrozby spôsobené vplyvom prostredia pre všetky udalosti, ktoré vznikajú nezávisle od ľudskej činnosti.	V procese riadenia rizík, vrátane riadenia bezpečnostných rizík, resp. rizík kybernetickej bezpečnosti, sú náležitým spôsobom zohľadnené požiadavky platnej legislatívy. Katalóg hrozieb zohľadňuje požiadavky legislatívy.	

b)	§ 6 ods. 11	Súčasťou riadenia aktív, hrozieb a rizík je aj **analýza funkčného dopadu**, ktorá pozostáva z hodnotenia dopadu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby a spôsobiť ohrozenie alebo narušenie kontinuity jeho poskytovanej základnej služby.	V procese riadenia rizík, vrátane riadenia bezpečnostných rizík, resp. rizík kybernetickej bezpečnosti, sú náležitým spôsobom zohľadnené požiadavky platnej legislatívy.	
c)	§ 7 písm. a)	Personálna bezpečnosť pozostáva najmenej z **postupov pri zaradení osoby do niektorých z bezpečnostných rolí, presunu práv, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu.**	Typové pracovné pozície sú hodnotené z pohľadu ich vplyvu na kybernetickú bezpečnosť (stanovenie bezpečnostných rolí). Postupy zaradenia osoby do niektorých z bezpečnostných rolí sú súčasťou postupov riadenia ľudských zdrojov.	
c)	§ 7 písm. b)	Personálna bezpečnosť pozostáva najmenej zo zavedenia **plánu rozvoja bezpečnostného povedomia a vzdelávania** spočívajúceho v oboznámení používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov s bezpečnostnými politikami a v pravidelnom zvyšovaní ich bezpečnostného povedomia počas trvania pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu	V SEPS sú zavedené nástupné a periodické školenia (e-learning, interaktívne školenia), informácie na intranete, bezpečnostné posolstvá, oznamy a upozornenia používateľov na nové hrozby v oblasti kybernetickej bezpečnosti.	
c)	§ 7 písm. c)	Personálna bezpečnosť pozostáva najmenej z **kontroly dodržiavania bezpečnostných politík** zo strany zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov.	Kontrola dodržiavania bezpečnostných politík je súčasťou výkonu činností jednotlivých organizačných zložiek podľa organizačného poriadku spoločnosti.	
c)	§ 7 písm. d)	Personálna bezpečnosť pozostáva najmenej z **hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia** zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov	Nástupné a periodické školenia v SEPS sú ukončené testom. Pri výskyte bezpečnostného incidentu, resp. pri jeho hodnotení, je analyzovaný aj vplyv ľudského faktora. Plánované je zahrnutie oblasti informačnej a kybernetickej bezpečnosti do prieskumu kultúry bezpečnosti.	

c)	§ 7 písm. e)	Personálna bezpečnosť pozostáva najmenej z **určenia pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky** zo strany používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,	Pravidlá a postupy riešenia prípadov porušenia bezpečnostnej politiky sú z hľadiska obmedzenia logického prístupu do sietí a informačných systémov spoločnosti stanovené.	
c)	§ 7 písm. f)	Personálna bezpečnosť pozostáva najmenej z **postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu** s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí umožňujúcich presun práv, povinností a zodpovedností na inú novú osobu	Postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného sú súčasťou postupov riadenia ľudských zdrojov.	
c)	§ 7 písm. g)	Personálna bezpečnosť pozostáva najmenej z postupov pri porušení bezpečnostných politík spočívajúcich v **oprávnení obmedziť alebo odňať prístupové oprávnenia a privilégiá.**	Oprávnenie žiadať o obmedzenie alebo odňatie prístupových oprávnení v prípade porušenia platných bezpečnostných politík spoločnosti je súčasťou xxxx.	
c)	§ 7 písm. h)	Personálna bezpečnosť pozostáva najmenej z **vykonania poučenia o manipulácii s informáciami pre osoby, ktoré vykonávajú činnosť alebo sa oboznamujú s informáciami podľa osobitného predpisu.**	Pre umožnením prístupu osôb k informáciám chráneným podľa osobitného predpisu je vykonané ich poučenie v zmysle požiadaviek osobitného predpisu, a ak je to požadované, aj zabezpečenie vyhlásenia o mlčanlivosti.	
d)	§ 8 ods. 1	Na riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov sa pri uzatvorení zmluvy s treťou stranou podľa § 19 ods. 2 zákona analyzujú **riziká dodávateľských služieb, akvizície, vývoja a údržby informačných systémov** spôsobom podľa § 6.	Analýza rizík dodávateľských služieb, akvizície, vývoja a údržby informačných systémov je súčasťou analýzy rizík kybernetickej bezpečnosti. Identifikácia a hodnotenie rizík súvisiacich s konkrétnym dodávateľom sú vykonávané v procese výberu dodávateľa, resp. v procese preverovania protistrán.	

d)	§ 8 ods. 2	Zmluva s treťou stranou obsahuje najmenej: a) obdobie trvania zmluvy, b) ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi, c) ustanovenie o povinnosti chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby tretej strane, d) ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou, e) konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi, f) konkrétny rozsah činnosti tretej strany, g) zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona, h) ustanovenie o rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby v tretej strane, i) vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa, j) ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti, k) ustanovenia o spôsobe a forme hláSEPSnia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie, l) ustanovenie o spôsobe a forme hláSEPSnia všetkých informácií majúcich vplyv na zmluvu, m) ustanovenie o sankčných mechanizmoch pri porušení zmluvy, n) ustanovenia o podmienkach a spôsobe ukončenia zmluvy, o) záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup prevádzkovateľovi základnej služby, p) záväzok tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu	Základné požiadavky na kybernetickú bezpečnosť sú zahrnuté v riadiacej dokumentácii pre oblasť kybernetickej bezpečnosti a uplatňujú sa pri podpisovaní zmlúv s treťou stranou.	

d)	§ 8 ods. 3	Zmluva s treťou stranou obsahuje **bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona.**	Základné požiadavky na kybernetickú bezpečnosť sú zahrnuté v riadiacej dokumentácii pre oblasť kybernetickej bezpečnosti a uplatňujú sa pri podpisovaní zmlúv s treťou stranou.	
d)	§ 8 ods. 4	Vývoj a akvizícia siete a informačného systému základnej služby sa uskutočňuje s ohľadom na **zaistenie kompatibility s existujúcimi sieťami a informačnými systémami** a **zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii.**		
d)	§ 8 ods. 5	**Evidencia všetkých uzatvorených zmlúv s treťou stranou** je súčasťou bezpečnostnej dokumentácie podľa § 2 ods. 1 písm. c).	Dodávateľ vedie evidenciu uzatvorených zmlú s tretími stranami.	
e)	§ 9 písm. a)	Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom **nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí.**	Dodávateľ je povinný bezodkladne informovať o akejkoľvek známej bezpečnostnej zraniteľnosti dodaného riešenia (aplikácie alebo jej časti) a poskytnúť max. súčinnosť pri jej odstránení (hot fix, workaround, patch, update/upgrade).	
e)	§ 9 písm. b)	Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom **nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí.**	Dodávateľ je povinný bezodkladne informovať o akejkoľvek známej bezpečnostnej zraniteľnosti dodaného riešenia (aplikácie alebo jej časti) a poskytnúť max. súčinnosť pri jej odstránení (hot fix, workaround, patch, update/upgrade).	

e)	§ 9 písm. c)	Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom **využitia verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov,**	Dodávateľ je povinný bezodkladne informovať o akejkoľvek známej bezpečnostnej zraniteľnosti dodaného riešenia (aplikácie alebo jej časti) a poskytnúť max. súčinnosť pri jej odstránení (hot fix, workaround, patch, update/upgrade). Dodávateľ poskytne odkaz na stránky výrobcu, kde sú publikované informácie o zraniteľnostiach programových a technických prostriedkov. Doplniť špecifické riziká (zraniteľnosti) systému.	
f)	§ 10 písm. a)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej **riadením prístupov používateľov k sieťam a informačným systémom podľa § 12.**	Organizácia má zavedené riadenie bezpečnosti sietí a informačných systémov na úrovni riadenia prístupov používateľov.	
f)	§ 10 písm. b)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom	Dodávateľ pri návrhu riešenia zohladní požiadavku na mikrosegmentáciu siete (maximálne oddelenie komponentov siete do samostatných VLAN prepojených prostredníctvom firewallov). Topologické schémy riešenia požadujeme dodať v elektronickej forme vrátane knižníc komponentov siete. Osobitne požadujeme označiť prepojenia do externých sietí a prepojenia medzi segmentami sietí.	Schéma sieťovej architektúry zohľadňujúcej požiadavky na mikrosegmentáciu s uvedením miest prepojení sietí/segmentov a pripojenia voči externým sieťam.

f)	§ 10 písm. c)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií.	Súčasťou dodávky riešenia musí byť aj návrh topológie, aby bolo zabezpečené, že každý segment = zóna = časť (PLC, operatorske stanice, HMI, servery, servisné stanice) plní iba služby = funkcie = komunikačné protokoly, požadované technológiou. Každý aktívny sieťový prvok musí umožňovať integráciu so SIEM, IDS, alebo ADS a formou odosielania napr. Netflow, IPFIX, syslog, L2 zariadenia musia podporovať multi port mirroring.	
f)	§ 10 písm. d)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prostredníctvom bezpečnostných opatrení na **bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup**, napríklad bezpečným spôsobom s **použitím dvojfaktorovej autentizácie** alebo použitím kryptografických prostriedkov	Ak je požadovaný vzdialený prístup, realizovať ho striktne prostredníctvom infraštruktúry ICT s použitím dvojfaktorovej autentizácie. V zmluve/objednávke je nevyhnutné ošetriť podmienky pre vzdialený prístup.	
f)	§ 10 písm. e)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej tým, že sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.	Súčasťou dodávky riešenia musí byť aj návrh topológie, aby bolo zabezpečené, že každý segment = zóna = časť (PLC, operatorske stanice, HMI, servery, servisné stanice) plní iba služby = funkcie = komunikačné protokoly, požadované technológiou. Každý aktívny sieťový prvok musí umožňovať integráciu so SIEM, IDS, alebo ADS a formou odosielania napr. Netflow, IPFIX, syslog, L2 zariadenia musia podporovať multi port mirroring.	

f)	§ 10 písm. f)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej **spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.**	Prepoje do externých sietí musia byť riadené firewallom s aktivovaným systémom IDS/IPS.	
f)	§ 10 písm. g)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej **prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcov.**	Všetky servre (HW, SW) dodané v rámci riešenia musia spĺňať výrobcom odporúčané možnosti hardeningu. Súčasťou musí byť detailný popis povolených služieb, protokolov, portov... aj s ich odôvodnením.	
f)	§ 10 písm. h)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej **udržiavaním zoznamu všetkých vstupno-výstupných bodov na hranici siete** v aktuálnom stave.	Súčasťou dodávky riešenia SaIS musí byť aj návrh topológie, aby bolo zabezpečené, že každý vstupno-výstupný bod na hranici siete bude zdokumentovaný. Topologické schémy riešenia požadujeme dodať v elektronickej forme vrátane knižníc komponentov siete. Osobitne požadujeme označiť prepojenia do externých sietí a prepojenia medzi segmentami sietí.	
f)	§ 10 písm. i)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej **použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.**	Každý aktívny sieťový prvok tvoriaci sieť alebo informačný systém musí umožňovať integráciu so SIEM, IDS, alebo ADS, formou odosielania napr. Netflow, IPFIX, syslog, L2 zariadenia musia podporovať multi port mirroring.	

f)	§ 10 písm. j)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prostredníctvom **blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby**, ak to nastavenie informačného systému umožňuje.	Zabezpečiť, aby komunikácia prebiehala len v rámci segmentov siete a výhradne s prvkami, pre ktorých riadenie je zariadenie určené (napr. servisné PC, HMI, ...). Doložiť popis riešenia. Možné riešenia napr. host file, antivír, lokálny firewall,... Firewally oddelujúce jednotlivé zóny/segmenty musia komunikáciu kontrolovať aj voči black list zoznamom.	
f)	§ 10 písm. k)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej **neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty.**	Na zariadenia je aplikovaný princíp - všetko je zakázané, povolené je len to, čo je nevyhnutné. Hardening = zodolnenie komponentov tým, že sa zablokujú porty na úrovni BIOS. Povinnosť autorizovať USB zariadenia. Koncové porty v rámci infraštruktúry musia byť obmedzené len na jednoznačný identifikátor / objekt stanice. Funkcionality (skripty, ovládače, možnosti subsystémov a súborových systémov), ktoré nie sú nevyhnutné pre prevádzku, musia byť zakázané. Musí byť zakázaná funkcionalita „Autoplay“, resp. „Autorun“ pre všetky externé médiá.	

f)	§ 10 písm. l)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prostredníctvom **systému monitorovania bezpečnosti, ktorý** je nakonfigurovaný tak, že **zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.**	Spôsob monitorovania musí obsahovať minimálne ADS (anomaly detection system) a pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu monitorovaciemu systému SIEM (multi port mirroring, NetFlow, IPFIX, syslog...). Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	
f)	§ 10 písm. m)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej implementovaním **systému detekcie prienikov alebo systému prevencie prienikov** na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.	Spôsob monitorovania musí obsahovať minimálne ADS (anomaly detection system) a pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostného monitorovaciemu systému (multi port mirroring, TAP, NetFlow,...). Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	
f)	§ 10 písm. n)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prostredníctvom **smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.**	Ak je požadovaná používateľská komunikácia mimo spoločnosť, realizovať ju striktne prostredníctvom infraštruktúry ICT s použitím ICT proxy serverov (napr. mail gateway, web gateway).	

f)	§ 10 písm. o)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej prostredníctvom vyžiadania **použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.**	Ak je požadovaný vzdialený prístup, realizovať ho striktne prostredníctvom infraštruktúry ICT s použitím dvojfaktorovej autentizácie. V zmluve/objednávke je nevyhnutné ošetriť podmienky pre vzdialený prístup.	
f)	§ 10 písm. p)	Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej vykonávaním pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo **zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti**.	Ak bude na pripojenie do siete alebo informačného systému používané zariadenie dodávateľa, popísať spôsob zabezpečenia jeho ochrany a posúdenie súladu s požiadavkami legislatívy. Pred nadviazaním vzdialeného pripojenia do ICS kategórie II. a III., požadujeme preukázať, že zariadenie je pravidelne aktualizované a je chránené AV softvérom. napr. doložiť záznam o preskúmaní počítača bezpečnostnou aplikáciou, ktorá poskytne informácie ako nainštalované ovládače, programy, opravné balíky, sieťové pripojenia či údaje z databázy Registry, ktoré môžu pomôcť zistiť príčiny podozrivého správania sa systému či už vplyvom nekompatibility alebo infekcie škodlivého kódu.	
g)	§ 11 písm. a)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na riadenie zmien.**	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na riadenie zmien, zohľadňujúce požiadavky SEPS a.s..	Postupy riadenia zmien
g)	§ 11 písm. b)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na riadenie záplat a aktualizácií.**	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na aplikáciu záplat a aktualizácií.	Postupy na aplikáciu záplat a aktualizácií

g)	§ 11 písm. c)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na riadenie kapacít.**	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na riadenie kapacít (dostatočné dimenzovanie diskového priestoru, výpočtového výkonu procesorov, operačnej pamäte RAM, ...). Eliminovať zraniteľnosť zariadenia na kritický bod zlyhania (Single Point of Failure) vo vhodnej forme (napr. redundancia), resp. aj dimenzovaním riešenia a fyzických parametrov so zohľadnením plánovania kapacít.	
g)	§ 11 písm. d)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na pravidelné zálohovanie a testovanie obnovy informácií zo záloh.**	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na pravidelné zálohovanie a testovanie obnovy informácií zo záloh	Postupy zálohovania na obnovu siete a informačného systému
g)	§ 11 písm. e)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na ochranu pred škodlivým kódom**.	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na ochranu pred škodlivým kódom. Tam kde je to možné sa musia aplikovať technické riešenia na ochranu pred škodlivým kódom.	Postupy na ochranu pred škodlivým kódom
g)	§ 11 písm. f)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na inštaláciu softvéru v sieťach a informačných systémoch.**	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na inštaláciu (opravy, parametrizáciu, ...) softvéru v sieťach a informačných systémoch (vrátane bezpečnostných pravidiel)	Postupy na inštaláciu softvéru v sieťach a informačných systémoch
g)	§ 11 písm. g)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na inštaláciu zariadení v sieťach a informačných systémoch.**	Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na inštaláciu (opravy, parametrizáciu, ...) zariadení v sieťach a informačných systémoch (vrátane bezpečnostných pravidiel)	Postupy na inštaláciu zariadení v sieťach a informačných systémoch

g)	§ 11 písm. h)	Riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených **pravidiel a postupov na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov.**	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.
h)	§ 12 ods. 1	Riadenie prístupov osôb k sieti a informačnému systému je založené na **zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa**. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.	Pravidlá riadenia prístupu k sieti a informačnému systému sú stanovené v riadiacej dokumentácii organizácie.	
			Špecifikovať spôsob autentizácie, a spôsob ochrany autentizačných informácií v systéme. Podmienkou je zákaz používania prihlasovacích údajov v čitateľnej forme v	

h)	§ 12 ods. 2	Riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.	skriptoch, zmena výrobcom nastavených účtov a hesiel. Nastaviť systémové vynucovanie politiky hesiel (min. vynútenie komplexnosti, času platnosti, možnosť zablokovania po x nesprávnych pokusoch). Možnosť pripojenia prvkov Sietí a IS ku ktorým sa prihlasujú užívatelia alebo služby, na centrálne autentifikačné a autorizačné adresáre (min. Active Directory, Radius). V prípade, ak aktuálne v sieti alebo informačnom systéme neexistuje systém pre centrálne riadenie identít (napr.AD) tak musí byť súčasťou dodávaného riešenia.	
h)	§ 12 ods. 3 písm. a)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej vypracovanie **zásad riadenia prístupu k informáciám**.	Zásady riadenia prístupu k informáciám sú stanovené v tejto riadiacej dokumentácii organizácie.	
h)	§ 12 ods. 3 písm. b)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **riadenie prístupu používateľov.**	Pravidlá riadenia prístupu k sieti a informačnému systému sú stanovené v riadiacej dokumentácii organizácie.	
h)	§ 12 ods. 3 písm. c)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **zodpovednosť používateľov.**	Zodpovednosť používateľov v súvislosti s ich prístupom do sietí a informačných systémom spoločnosti je stanovená v riadiacej dokumentácii organizácie.	

h)	§ 12 ods. 3 písm. d)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **riadenie prístupu k sieťam.**	Súčasťou dodávky riešenia Sietí a IS musí byť špecifikácia riadenia prístupu v systéme. Všetky prvky Sietí a IS musia mať nastavené pevné IP adresy, mať vypnuté DHCP pričom rozsah použiteľných adries poskytne SEPS. Všetky aktívne sieťové prvky Sietí a IS musia podporovať protokol IEEE 802.1x. V návrhu riešenia nepoužiť za žiadnych okolností WiFi a Bluetooth zariadenia, vrátane vylúčenia použitia napr. bezdrôtovej myši, klávesnice a pod.	
h)	§ 12 ods. 3 písm. e)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **prístup k operačnému systému a jeho službám.**	Natívne administrátorské účty musia byť zakázané, musia byť vytvorené samostatné privilegované účty s administrátorskými právami pre konkrétnych správcov systému. Odovzdať detailný zoznam všetkých administrátorských a užívateľských prístupov, vrátane hesiel s možnosťou ich zmeny. Odovzdať detailný popis a zdôvodnenie vytvorenia jednotlivých prístupov, vrátane systémových. Samostatne musí byť označený účet pod ktorým beží aplikácia (podprogram, utilita...). Mimo vymenovaných prístupov nesmú byť v systéme vytvorené žiadne iné, skryté prístupy! Dodávané riešenie Sietí a IS musí zahŕňať aj implementáciu politiky čistej obrazovky (v systémoch, v ktorých to prevádzkové podmienky	

h)	§ 12 ods. 3 písm. f)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **prístup k aplikáciám.**	Natívne administrátorské účty musia byť zakázané, musia byť vytvorené samostatné privilegované účty s administrátorskými právami pre konkrétnych správcov systému. Odovzdať detailný zoznam všetkých administrátorských a užívateľských prístupov, vrátane hesiel s možnosťou ich zmeny. Odovzdať detailný popis a zdôvodnenie vytvorenia jednotlivých prístupov, vrátane systémových. Samostatne musí byť označený účet pod ktorým beží aplikácia (podprogram, utilita...). Mimo vymenovaných prístupov nesmú byť v systéme vytvorené žiadne iné, skryté prístupy!	
h)	§ 12 ods. 3 písm. g)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **monitorovanie prístupu a používania informačného systému.**	Prístupy do systému musia byť zaznamenávané v logoch. Povinné logovanie na úrovni OS a aplikácie s následným odosielaním záznamov do centrálneho systému na zber a vyhodnocovanie logov.	Rozsah požadovaného logovania je definovaný v SM 01/2023
h)	§ 12 ods. 3 písm. h)	Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej **riadenie vzdialeného prístupu.**	Ak je požadovaný vzdialený prístup, realizovať ho striktne prostredníctvom infraštruktúry ICT s použitím dvojfaktorovej autentizácie	
h)	§ 12 ods. 4 písm. a)	V rámci riadenia prístupov k sieťam sa každému používateľovi siete a informačného systému prideľuje **jednoznačný identifikátor na autentizáciu na vstup do siete a informačného systému.**	Požaduje aby mal každý používateľ pridelený jednoznačný identifikátor. Nie sú povolené skupinové prístupy.	

h)	§ 12 ods. 4 písm. b)	V rámci riadenia prístupov k sieťam sa zabezpečuje **riadenie jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov**.	Prístup k Sieťam a Informačným systémom musí byť riadený prostredníctvom centrálneho systému na riadenie identít (napr. AD).	
h)	§ 12 ods. 4 písm. c)	V rámci riadenia prístupov k sieťam sa využíva **nástroj na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).**	Prístup k Sieťam a Informačným systémom musí byť riadený prostredníctvom centrálneho systému na riadenie identít (napr. AD). Všetky dodané komponenty tvoriace Sieť alebo informačný systém musia mať definované roly na riadenie prístupových oprávnení so zohľadním pravidla "need to know" a "segregation of duties"	
h)	§ 12 ods. 4 písm. d)	V rámci riadenia prístupov k sieťam sa v pravidelných intervaloch vykonáva **kontrola prístupových účtov a prístupových oprávnení** na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov.	V organizácii sa vykonáva periodická kontrola prístupových účtov a prístupových oprávnení v rámci interných procesov a štandardov.	
h)	§ 12 ods. 4 písm. e)	V rámci riadenia prístupov k sieťam sa určí osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a **vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému** v zmysle príslušnej bezpečnostnej politiky.	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.

i)	§ 13 ods. 1	Dôvernosť, integrita, dostupnosť a hodnovernosť údajov v rámci sietí a informačných systémov, prostredníctvom ktorých je poskytovaná základná služba, sa zabezpečuje pomocou kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy, pričom sa určia pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov.	Ak to technológia siete alebo informačného systému umožňuje, komunikácia medzi klientami a aplikačným serverom musí byť vždy kryptovaná podľa aktuálnych kryptovacích štandardov (HTTPS, SFTP, LDAPS). Služby, ktoré budú publikované musia používať zabezpečený sieťový protokol (https, ftps, sftp, ...). Konfiguračné prístupy musia byť zabezpečené šifrovanými protokolmi (ssh, ...).	
i)	§ 13 ods. 2	Systém správy kryptografických kľúčov a certifikátov je zabezpečený počas celého životného cyklu kryptografických kľúčov a certifikátov. Správa kryptografických kľúčov a certifikátov zahŕňa najmenej: a) bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi, b) generovanie pseudonáhodných čísel a kľúčov, zriadenie, distribúciu, vkladanie, zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zneplatnenie certifikátov, c) umožnenie kontroly a auditu	Správa kľúčov je zabezpečená v sulade s politikami správy kryptografických identifikátorov SEPS a.s.	
j)	§ 14 ods. 1 písm. a)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej z prípravy a **vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov.**	Proces riešenia kybernetických bezpečnostných incidentov je definovaný v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 1 písm. b)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej z **monitorovania a analyzovania udalostí v sieťach a informačných systémoch.**	Dodávateľ poskytne zoznam kľúčových ukazovateľov, ktoré sú kritické z pohľadu analýzy vzniknutých kybernetických incidentov.	
j)	§ 14 ods. 1 písm. c)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej z **detekcie kybernetických bezpečnostných incidentov.**	Dodávateľ poskytne indikátory bezpečnostných incidentov pre dané riešenie.	

j)	§ 14 ods. 1 písm. d)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej zo **zberu relevantných informácií o kybernetických bezpečnostných incidentoch. => § 14 ods. 6**	Dodávateľ popíše rozsah možných atribútov a informácii pre vyšetrovanie a riešenie kybernetických incidentov, pre dané riešenie. (Súčasťou evidencie sú aj informácie identifikujúce kybernetický bezpečnostný incident ako napríklad lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia.)	
j)	§ 14 ods. 1 písm. e)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej z **vyhodnocovania kybernetických bezpečnostných incidentov.**	Dodávateľ poskytne indikátory bezpečnostných incidentov pre dané riešenie a odporúčaný spôsob ich vyhodnotenia.	
j)	§ 14 ods. 1 písm. f)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej z **riešenia zistených kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov.**	Dodávateľ poskytne odporúčaný postup reakcie na kybernetické bezpečnostné incidenty.	
j)	§ 14 ods. 1 písm. g)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmenej z **vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatia opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov.**	n/a	
j)	§ 14 ods. 2 písm. a)	Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmenej **postup pri internom nahlasovaní kybernetických bezpečnostných incidentov.**	Proces riešenia kybernetických bezpečnostných incidentov, vrátane interného nahlasovania KBI, je špecifikovaný v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 2 písm. b)	Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmenej postup pri hláSEPSní kybernetických bezpečnostných incidentov podľa § 24 ods. 1 zákona.	Proces riešenia kybernetických bezpečnostných incidentov, vrátane hlásenia významných KBI na NBÚ, je špecifikovaný v riadiacej dokumentácii organizácie.	

j)	§ 14 ods. 2 písm. c)	Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmenej **postup pri riešení jednotlivých typov kybernetických bezpečnostných incidentov a spôsob ich vyhodnocovania.**	Dodávateľ poskytne odporúčaný postup reakcie na kybernetické bezpečnostné incidenty.	Postup pri riešení jednotlivých typov kybernetických bezpečnostných incidentov a spôsob ich vyhodnocovania
j)	§ 14 ods. 2 písm. d)	Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmenej **spôsob evidencie kybernetických bezpečnostných incidentov a použitých riešení.**	Rámec riešenia kybernetických bezpečnostných incidentov, vrátane spôsobu evidencie KBI a použitých riešení, je stanovený v riadiacej dokumentácii organizácie. Evidencia závažných KBI, hlásených do jednotného informačného systému kybernetickej bezpečnosti.	
j)	§ 14 ods. 3	Proces detekcie kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.**	Nástroj na detekciu kybernetických bezpečnostných incidentov musí obsahovať minimálne ADS (anomaly detection system) a pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostného monitorovaciemu systému (multi port mirroring, TAP, NetFlow,...). Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	

j)	§ 14 ods. 4 písm. a)	Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí,** ktorý umožňuje **zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch.**	Nástroj na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí (napr. ADS - anomaly detection system, SIEM) musí pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostnému monitorovaciemu systému prostredníctvom napr. zrkadlenia dátových tokov prostredníctvom multi port mirroringu alebo TAP-ov a pod. . Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	
j)	§ 14 ods. 4 písm. b)	Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí,** ktorý umožňuje **vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetický bezpečnostným incidentom.**	Nástroj na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí (napr. ADS - anomaly detection system, SIEM) musí pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostnému monitorovaciemu systému prostredníctvom napr. zrkadlenia dátových tokov prostredníctvom multi port mirroringu alebo TAP-ov a pod. . Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	

j)	§ 14 ods. 4 písm. c)	Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí,** ktorý umožňuje **vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov.**	Nástroj na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí (napr. ADS - anomaly detection system, SIEM) musí pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostnému monitorovaciemu systému prostredníctvom napr. zrkadlenia dátových tokov prostredníctvom multi port mirroringu alebo TAP-ov a pod. . Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	
j)	§ 14 ods. 4 písm. d)	Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí,** ktorý umožňuje **revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.**	Nástroj na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí (napr. ADS - anomaly detection system, SIEM) musí pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostnému monitorovaciemu systému prostredníctvom napr. zrkadlenia dátových tokov prostredníctvom multi port mirroringu alebo TAP-ov a pod. . Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu.	

j)	§ 14 ods. 5 písm. a)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **pridelenia zodpovednosti a určenia postupov na zvládanie kybernetických bezpečnostných incidentov**.	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 5 písm. b)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **zavedenia procesu získavania a uchovávania podkladov potrebných na analýzu kybernetickej bezpečnostnej udalosti a kybernetického bezpečnostného incidentu.**	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 5 písm. c)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **prijímania opatrení na odvrátenie alebo zmiernenie dopadu kybernetického bezpečnostného incidentu.**	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 5 písm. d)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **zavedenia procesu nahlasovania kybernetických bezpečnostných incidentov.**	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 5 písm. e)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **vedenia záznamov o kybernetických bezpečnostných incidentoch vrátane použitých riešení.**	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 5 písm. f)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom **prešetrovania a určenia príčin vzniku kybernetického bezpečnostného incidentu aktualizáciou bezpečnostnej politiky a prijatia primeraných bezpečnostných opatrení zamedzujúcich jeho opakovanému výskytu.**	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v riadiacej dokumentácii organizácie.	
j)	§ 14 ods. 5 písm. g)	Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom určenia osoby zodpovednej za nahlasovanie a odovzdávanie hláSEPSní o kybernetických bezpečnostných incidentoch do jednotného informačného systému kybernetickej bezpečnosti, ktoré nastali alebo sa prejavili v rámci siete alebo informačného systému základnej služby.	Proces riešenia kybernetických bezpečnostných incidentov, vrátane určenia osoby zodpovednej za nahlasovanie KBI a odovzdávanie hláSEPSní o KBI do jednotného informačného systému kybernetickej bezpečnosti (prevádzkovaného NBÚ), je popísaný v riadiacej dokumentácii organizácie.	

j)	§ 14 ods. 6	**Súčasťou evidencie kybernetických bezpečnostných incidentov sa na zabezpečenie dôkazu alebo dôkazného prostriedku evidujú aj informácie identifikujúce kybernetický bezpečnostný incident** ako napríklad lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia.	Proces riešenia kybernetických bezpečnostných incidentov je stanovený v xxxx. Referencia na § 14 ods. 1 písm. d)	
k)	§ 15 ods. 1	Monitorovanie bezpečnosti sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu a) centrálnych sieťových prvkov a serverov, b) služieb prístupných do externých sietí a c) kritických interných serverov a služieb.	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.
k)	§ 15 ods. 2 písm. a)	Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej **aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených.**	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.

k)	§ 15 ods. 2 písm. b)	Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej **iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy.**	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.
k)	§ 15 ods. 2 písm. c)	Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej **pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla.**	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.
k)	§ 15 ods. 2 písm. d)	Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej automatické varovné alebo chybové hlásenia systémov.	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.

k)	§ 15 ods. 2 písm. e)	Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej **detegované podozrivé alebo škodlivé aktivity.**	Spôsob monitorovania musí obsahovať minimálne ADS (anomaly detection system) a pokrývať celé prostredie takým spôsobom, aby nespôsobil spoločnú príčinu incidentu. V prípade jednotlivých Sietí a IS musia byť tieto schopné poskytnúť informácie centrálnemu bezpečnostného monitorovaciemu systému (multi port mirroring, TAP, NetFlow,...). Informácie musia umožniť vyšetrenie kybernetického bezpečnostného incidentu. Dodávateľ poskytne zoznam kľúčových ukazovateľov, ktoré sú kritické z pohľadu analýzy vzniknutých kybernetických incidentov.	
k)	§ 15 ods. 2 písm. f)	Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.	Vytvárané prevádzkové a bezpečnostné záznamy musia spĺňať možnosť ukladania so zachovaním integrity. Všetky komponenty tvoriace sieť alebo informačný systém musia umožňovať zaznamenávanie a odosielanie prevádzkových a bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...	Postupy na zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov je definovaný v SM 01/2023 - Monitorovanie systémov.
k)	§ 15 ods. 3 písm. a)	Prevádzkové záznamy sú zabezpečené najmenej tak, že **sú čitateľné výlučne osobám povereným ich analýzou.**	Prevádzkové záznamy sú zabezpečené najmenej tak, že sú čitateľné výlučne osobám povereným ich analýzou.	
k)	§ 15 ods. 3 písm. b)	Prevádzkové záznamy sú zabezpečené najmenej tak, že **zamedzujú možnosti prepísania alebo vymazania záznamu**.	Prevádzkové záznamy sú zabezpečené najmenej tak, že zamedzujú možnosti prepísania alebo vymazania záznamu.	

k)	§ 15 ods. 3 písm. c)	Prevádzkové záznamy sú zabezpečené najmenej tak, že **záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete.**	Napr. formou SNMP verzia 3, samostatná VLAN, servisné porty, softvéroví agenti, ... Riešenie Sietí a IS musí podporovať zasielanie (presmerovanie) logov na centrálne úložisko logov.	
k)	§ 15 ods. 3 písm. d)	Prevádzkové záznamy sú zabezpečené najmenej tak, že **sú uchovávané po dobu zodpovedajúcu kategórii informačného systému**.	Dodávateľ zabezpečí uchovávanie záznamov po dobu podľa požiadaviek SEPS a.s. (SM 01/2023)	
k)	§ 15 ods. 4	Za monitorovanie prevádzkových záznamov, ich vyhodnocovanie a vykonanie nahlásenia podozrivej aktivity je zodpovedný na to poverený zamestnanec prevádzkovateľa základnej služby alebo zamestnanec tretej strany, ak je jej táto činnosť zverená.	V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS), musí zabezpečiť monitorovanie prevádzkových záznamov a ich vyhodnocovanie. V prípade prevádzkovania riešenia v rámci infraštruktúry SEPS a.s., musí dodržiavať postupy a predpisy SEPS a.s.	
k)	§ 15 ods. 5	Zhoda sietí a informačných systémov základnej služby s požiadavkami na zabezpečenie kybernetickej bezpečnosti týchto sietí a informačných systémov, monitorovanie účinnosti bezpečnostných opatrení a vyhodnotenie aktuálnosti bezpečnostnej dokumentácie sa zisťuje prostredníctvom **auditu kybernetickej bezpečnosti.**	SEPS preverujú účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. vykonaním auditu kybernetickej bezpečnosti.	
l)	§ 16 ods. 1 písm. a)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom umiestnenia siete a informačného systému v takom priestore, že sieť a informačný systém alebo aspoň ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „**zabezpečený priestor**“).	Pre Siete a IS kat. II. minimálne kľúčový režim, pre kat. III. musia byť zariadenia umiestnené v uzamykateľných rackoch s vyvedením signalizácie do centrálneho monitorovacieho systému. V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS), ochranu zabezpečuje dodávateľ. V prípade prevádzkovania riešenia v rámci infraštruktúry SEPS a.s., musí dodržiavať postupy a predpisy SEPS a.s.	

l)	§ 16 ods. 1 písm. b)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom **ochrany zabezpečeného priestoru** fyzickými prostriedkami, najmä stenami, mechanickými zábrannými prostriedkami, technickými zabezpečovacími prostriedkami, napríklad zariadeniami elektrickej zabezpečovacej signalizácie, systémami na kontrolu vstupu, kamerovými systémami.	Pre SaIS kat. II. minimálne kľúčový režim, pre kat. III. musia byť zariadenia umiestnené v uzamykateľných rackoch s vyvedením signalizácie do centrálneho monitorovacieho systému. V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS), ochranu zabezpečuje dodávateľ. V prípade prevádzkovania riešenia v rámci infraštruktúry SEPS a.s., musí dodržiavať postupy a predpisy SEPS a.s.	
l)	§ 16 ods. 1 písm. c)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom zaručenia, že sa **v okolí zabezpečeného priestoru nevyskytujú zariadenia, ktoré môžu ohroziť sieť a informačný systém umiestnený v tomto zabezpečenom priestore, najmä kanalizácia, vodovod, horľavé alebo iné obdobné materiály.**	Pri návrhu riešenia Sietí a IS, resp. umiestnenia jeho komponentov v priestoroch prevádzky, je potrebné zohľadniť aj požiadavku, aby neboli v blízkosti zariadení vedené inžinierske siete, resp. neboli umiestnené horľavé alebo iné obdobné materiály.	
l)	§ 16 ods. 1 písm. d)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom vypracovania, implementácie a kontroly dodržiavania **pravidiel na prácu v zabezpečenom priestore.**	V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS), pravidlá na prácu v zabezpečenom priestore zabezpečuje dodávateľ. V prípade prevádzkovania riešenia v rámci infraštruktúry SEPS a.s., musí dodržiavať postupy a predpisy SEPS a.s.	
l)	§ 16 ods. 1 písm. e)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom **zabezpečenia ochrany pred výpadkom zdroja elektrickej energie tých častí siete a informačného systému, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, že taký výpadok nenastane.**	V prípade kategórie Sietí a IS II. a III. je nutné ošetriť zraniteľnosť zariadenia na kritický bod zlyhania (Single Point of Failure) vo forme redundantných zdrojov napájania na všetkých úrovniach infraštruktúry.	

l)	§ 16 ods. 1 písm. f)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom **zaručenia, že existujú záložné kapacity siete a informačného systému, zabezpečujúce dostupnosť, funkčnosť alebo náhradu siete a informačného systému, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru.**	V prípade kategórie Sietí a IS II. a III. sú kladené požiadavky na vysokú dostupnosť (resp. obnovu) riešenia. Tam kde je to technicky možné, je potrebné implementovať záložné riešenie Sietí a IS v záložnom zabezpečenom priestore.	
l)	§ 16 ods. 1 písm. g)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom **zaručenia, že prevádzka, používanie a manažment siete a informačného systému je v súlade vnútornými predpismi a zmluvnými záväzkami.**	xxxx stanovuje požiadavku, aby prevádzka, používanie a manažment siete a informačného systému boli v súlade vnútornými predpismi a zmluvnými záväzkami.	
l)	§ 16 ods. 1 písm. h)	Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom **politiky, ktorá zakazuje nechávanie fyzických dokumentov bez dozoru a prikazuje uzamykanie počítača pred opustením pracoviska.**	Požiadavky politiky čistého stola a politiky čistej obrazovky sú definované v riadiacej dokumentácii organizácie.	
l)	§ 16 ods. 2 písm. a)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na údržbu, uchovávanie a evidenciu technických komponentov sietí a informačných systémov a zariadení sietí a informačných systémov.**	Prevádzková dokumentácia + dokumentácia skutočného vyhotovenia + zoznam aktív	Pravidlá na údržbu, uchovávanie a evidenciu technických komponentov sietí a informačných systémov a zariadení sietí a informačných systémov
l)	§ 16 ods. 2 písm. b)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na používanie zariadení sietí a informačných systémov na iné účely, ako sú určené.**	Požiadavky na zabezpečenie fyzickej ochrany aktív sú určené v xxxx; špecifické požiadavky sú definované pre ICT a OT v príslušnej procesnej dokumentácii.	
l)	§ 16 ods. 2 písm. c)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na používanie sietí a informačných systémov mimo zabezpečených priestorov.**	Požiadavky na zabezpečenie fyzickej ochrany aktív sú určené v riadiacej dokumentácii organizácie.	

l)	§ 16 ods. 2 písm. d)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na vymazávanie, vyraďovanie a likvidovanie zariadení sietí a informačných systémov a všetkých typov relevantných záloh.**	Požiadavky na zabezpečenie fyzickej ochrany aktív sú určené v riadiacej dokumentácii organizácie; špecifické požiadavky sú definované pre ICT a OT v príslušnej procesnej dokumentácii. Pravidlá a požiadavky na bezpečnú likvidáciu údajov sú v organizácii stanovené.	
l)	§ 16 ods. 2 písm. e)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na fyzický prenos technických komponentov sietí a informačných systémov alebo zariadení sietí a informačných systémov mimo zabezpečených priestorov.**	Požiadavky na zabezpečenie fyzickej ochrany aktív sú určené v riadiacej dokumentácii organizácie.	
l)	§ 16 ods. 2 písm. f)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na narábanie s dokumentáciou systému a pamäťovými médiami tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.**	Požiadavky na zabezpečenie fyzickej ochrany aktív sú určené v riadiacej dokumentácii organizácie; špecifické požiadavky sú definované pre ICT a OT v príslušnej procesnej dokumentácii. Pravidlá a požiadavky na bezpečnú likvidáciu údajov sú v organizácii stanovené.	
l)	§ 16 ods. 2 písm. g)	Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania **pravidiel na dimenzovanie a fyzické parametre sietí a hardvéru, ktoré priamo alebo nepriamo ovplyvňujú najväčšiu prípustnú dobu výpadku siete a informačného systému.**	Požiadavky na zabezpečenie fyzickej ochrany aktív sú určené v xxxx; špecifické požiadavky sú definované pre ICT a OT v príslušnej procesnej dokumentácii. Pozn.: súčasť riadenia kapacít.	
m)	§ 17 ods. 1	Prevádzkovateľ základnej služby určí **požiadavky na zabezpečenie kontinuity riadenia kybernetickej bezpečnosti** pri vzniku kybernetického bezpečnostného incidentu.	Požiadavky na zabezpečenie kontinuity riadenia kybernetickej bezpečnosti v prípade vzniku kybernetického bezpečnostného incidentu sú stanovené v riadiacej dokumentácii organizácie.	

m)	§ 17 ods. 2 písm. a)	Riadenie kontinuity procesov pozostáva najmenej z vypracovania **stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu** na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu na základnú službu.	Stratégia BCP/DRP spoločnosti (vrátane stanovenia štruktúry dokumentácie pre oblasť kontinuity činností) je definovaná v riadiacej dokumentácii organizácie.	
m)	§ 17 ods. 2 písm. b)	Riadenie kontinuity procesov pozostáva najmenej z **vyčlenenia adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činností.**	Požiadavky na vyčlenenie adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činností sú v organizácii stanovené.	
m)	§ 17 ods. 2 písm. c)	Riadenie kontinuity procesov pozostáva najmenej z **určenia komunikačného plánu na plnenie havarijných plánov a plánov obnovy** spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti na plnenie havarijných plánov a plánov obnovy po kybernetickom bezpečnostnom incidente.	Pravidlá komunikácie v krízových situáciách sú v organizácii stanovené ; špecifické požiadavky z hľadiska oznamovania kybernetických bezpečnostných incidentov sú stanovené v riadiacej dokumentácii organizácie.	
m)	§ 17 ods. 2 písm. d)	Riadenie kontinuity procesov pozostáva najmenej z **určenia cieľovej doby obnovy** jednotlivých procesov, siete a informačných systémov a aplikácií, a to **najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb**.		
m)	§ 17 ods. 2 písm. e)	Riadenie kontinuity procesov pozostáva najmenej z **určenia cieľového bodu obnovy** jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä **určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby**.		
m)	§ 17 ods. 2 písm. f)	Riadenie kontinuity procesov pozostáva najmenej z **testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov** základnej služby.	Pravidlá pre testovanie jednotlivých plánov v oblasti riadenia kontinuity sú stanovené v riadiacej dokumentácii organizácie.	
m)	§ 17 ods. 2 písm. g)	Riadenie kontinuity procesov pozostáva najmenej z **určenia plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu.**	Dodávateľ vypracúva postupy zálohovania a plány obnovy údajov zo záloh.	Plány záloh a havarijnej obnovy

m)	§ 17 ods. 3 písm. a)	**Postupy zálohovania na obnovu siete a informačného systému** po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu **obsahujú najmenej frekvenciu a rozsah jej dokumentovania a schvaľovania.**	Rozsah a frekvenciu zálohovania odporúča dodávateľ riešenia Sietí a IS.	Postupy zálohovania na obnovu siete a informačného systému
m)	§ 17 ods. 3 písm. b)	**Postupy zálohovania na obnovu siete a informačného systému** po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej **určenie osoby zodpovednej za zálohovanie.**	Dodávateľ riešenia Sietí a IS určí osobu zodpovednú za zálohovanie len v prípade, ak zabezpečuje túto činnosť. Inak túto osobu určí SEPS.	
m)	§ 17 ods. 3 písm. c)	**Postupy zálohovania na obnovu siete a informačného systému** po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej **časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní.**		
m)	§ 17 ods. 3 písm. d)	**Postupy zálohovania na obnovu siete a informačného systému** po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej požiadavku **umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom.**	Dodávateľ zabezpečí uchovávanie záloh v zabezpečenom prostredí s riadeným prístupom, ak vykonáva túto činnosť.	
m)	§ 17 ods. 3 písm. e)	**Postupy zálohovania na obnovu siete a informačného systému** po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej požiadavku **zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené.**	Dodávateľ zabezpečí kryptografickú ochranu záloh s údajmi klasifikovanými ako chránené, alebo vyššieho stupňa.	
m)	§ 17 ods. 3 písm. f)	**Postupy zálohovania na obnovu siete a informačného systému** po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej požiadavku na **vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.**	Prvotné testovanie obnovy zo záloh vykoná dodávateľ. V prípade, že činnosť zálohovania vykonáva dodávateľ musí vykonať aj pravidelné preverenie záloh a testovanie obnovy min. 1 x ročne.	

Bezpečnostné opatrenia na informačnú a kybernetickú bezpečnosť pre dodávateľov SEPS

Pre potreby tejto prílohy sa pod zmluvou rozumie okrem písomne uzatvorenej zmluvy aj vystavenie objednávky.

Časť 1.

Zákonné bezpečnostné opatrenia

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.

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 na čo najvyššej možnej úrovni; špecifikácia a rozsah bezpečnostných opatrení, ktoré sa Dodávateľ zaväzuje prijať a dodržiavať po celý čas trvania zmluvného vzťahu založeného Zmluvou je vymedzený v časti 2. tejto Prílohy.
2. Konkrétny rozsah činností Dodávateľa vyplýva zo Zmluvy a jej príloh.
3. Dodávateľ vyhlasuje, že sa oboznámil s bezpečnostnou politikou spoločnosti SEPS, zverejnenou na webovom sídle spoločnosti SEPS, vyjadruje s ňou súhlas a zaväzuje sa ju dôsledne dodržiavať; so zmenou/doplnením bezpečnostnej politiky spoločnosti SEPS je Dodávateľ povinný sa bezodkladne oboznámiť a dôsledne ju dodržiavať.
4. Dodávateľ sa zaväzuje chrániť všetky informácie, ktoré mu boli, alebo budú zo strany spoločnosti SEPS poskytnuté, alebo sprístupnené a to najmä, avšak nie len pred náhodným alebo nezákonným zničením, stratou, zmenou, neoprávneným poskytnutím, alebo sprístupnením. Povinnosť dodržať mlčanlivosť sa zabezpečuje podpísaním osobitného dokumentu „Dohoda o mlčanlivosti". Tento dokument je povinný ako pre zmluvný vzťah, tak aj pre objednávku.
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 3. 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 predchádzajúcom písomnom oznámení adresovanom Dodávateľovi 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 súčinnosť 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 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 lehotami na ich odstránenie. V prípade, ak Dodávateľ zistené nedostatky v stanovenej lehote neodstráni a/alebo vykonanie auditu neumožní, 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.

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;

b. Ak Dodávateľ zapojí ďalšieho dodávateľa, ďalšiemu dodávateľovi je v zmluve alebo v inom právnom úkone povinný uložiť rovnaké povinnosti týkajúce sa plnenia predmetu Zmluvy s dopadom na kybernetickú bezpečnosť ako sú ustanovené pre Dodávateľa a je povinný zaviazať ho v rovnakom 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, ktoré môžu mať vplyv na plnenie predmetu Zmluvy s dôrazom na zabezpečenie kybernetickej bezpečnosti. Informácie je Dodávateľ povinný adresovať kontaktným osobám spoločnosti SEPS uvedeným v časti 3. tejto Prílohy.

b. Dodávateľ sa zaväzuje spoločnosť SEPS bezodkladne informovať o každom kybernetickom bezpečnostnom incidente, o jeho hrozbe, ako aj o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti o ktorých sa 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 predovšetkým:

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

ii. detailný 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 3. 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 sú povinné v čo najkratšom možnom čase dohodnúť postup za účelom odstránenia kybernetického bezpečnostného incidentu a jeho následkov, ako aj potrebu prijatia preventívnych opatrení.

f. Dodávateľ je povinný v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní.

g. Dodávateľ sa zaväzuje zdokumentovať každý kybernetický bezpečnostný incident, jeho hrozbu, následky a opatrenia prijaté na jeho nápravu. Dokumentáciu o kybernetickom bezpečnostnom incidente je Dodávateľ povinný uchovávať a na vyžiadanie poskytnúť spoločnosti SEPS.

9. Ak nie je v zmluve uvedené inak, odplata za plnenie povinností a výkon činností v zmysle tejto Prílohy je zahrnutá v odplate dohodnutej v Zmluve a Dodávateľ nemá nárok na náhradu akýchkoľvek nákladov alebo výdavkov týkajúcich sa alebo súvisiacich s plnením povinností a výkonom činnosti v zmysle tejto Prílohy.

10. **Sankčný mechanizmus** 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, v Zákone o kybernetickej bezpečnosti, alebo vo všeobecne záväznom právnom predpise v oblasti kybernetickej bezpečnosti a v prípade porušenia povinnosti, ktoré podľa povahy porušenej povinnosti nemožno dodatočne napraviť alebo zvrátiť, má spoločnosť SEPS nárok na zmluvnú pokutu vo výške 5.000 EUR za každý jednotlivý prípad porušenia uvedenej povinnosti; uplatnením alebo zaplatením zmluvnej pokuty nie je dotknutý nárok spoločnosti SEPS na náhradu celej spôsobenej škody.

b. Spoločnosť SEPS má nárok na náhradu akýchkoľvek sankcií, ktoré jej budú uložené Národným bezpečnostným úradom alebo iným príslušným orgánom verejnej správy, ak sankcia bude spoločnosti SEPS uložená z dôvodu porušenia povinnosti Dodávateľa na úseku kybernetickej bezpečnosti. Náhradou podľa predchádzajúcej vety nie je dotknuté právo spoločnosti SEPS na náhradu celej škody spôsobenej porušením povinnosti Dodávateľa, pre ktorú bola spoločnosti SEPS sankcia uložená, ako ani na nárok na zmluvnú pokutu.

11. **Podmienky a spôsob ukončenia Zmluvy**

a. V prípade, ak Dodávateľ poruší ktorúkoľvek z povinností vymedzených v tejto Prílohe, v Zákone o kybernetickej bezpečnosti alebo vo všeobecne záväznom právnom predpise v oblasti kybernetickej bezpečnosti, spoločnosť SEPS 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 celej spôsobenej škody, ako ani nároku na zmluvnú pokutu, ktorý vznikol v dôsledku porušenia povinnosti.

b. Zánikom zmluvného vzťahu založeného Zmluvou nie je dotknutá povinnosť Dodávateľa zachovávať mlčanlivosť.

12. Po ukončení zmluvného vzťahu založeného Zmluvou je Dodávateľ povinný v súlade s usmernením spoločnosti SEPS

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. udeliť, poskytnúť, previesť alebo spoločnosti SEPS postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby; táto povinnosť ostáva v platnosti 10 rokov po ukončení zmluvného vzťahu, 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.

Časť 2.

Rozsah bezpečnostných opatrení

1. Dodávateľ sa zaväzuje prijať, aktualizovať a po celý čas trvania zmluvného vzťahu založeného Zmluvou dodržiavať bezpečnostné opatrenia v oblasti informačnej a kybernetickej bezpečnosti s cieľom zabezpečiť kybernetickú bezpečnosť počas celého životného cyklu sietí a informačných systémov spoločnosti SEPS.
2. Dodávateľ sa zaväzuje zaviesť opatrenia v oblasti informačnej a kybernetickej bezpečnosti v súlade so Zákonom o kybernetickej bezpečnosti č. 69/2022 Z.z., Vyhláškou NBÚ č. 362/2018 Z.z. a ostatnými všeobecne záväznými právnymi predpismi v oblasti kybernetickej bezpečnosti s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby spoločnosťou SEPS.
3. Vzhľadom na to, že spoločnosť SEPS zaviedla a implementovala certifikačný štandard **ISO 27001**, ktorá špecifikuje požiadavky na zostavovanie, implementáciu, prevádzku, monitorovanie, preskúmanie a zlepšovanie systému manažérstva informačnej bezpečnosti, Zmluvné strany sa dohodli, že norma **ISO/IEC 27001: 2022 Information security, cybersecurity and privacy – Information security controls aj s prílohou**, predstavuje minimálny štandard v oblasti informačnej bezpečnosti, ktorý je Dodávateľ povinný zaviesť a implementovať.
4. Dodávateľ sa zaväzuje dodržiavať nižšie uvedené opatrenia informačnej a kybernetickej bezpečnosti.

Organizácia informačnej a kybernetickej bezpečnosti v SEPS

Garant zmluvy: zamestnanec SEPS, ktorý iniciuje za stranu SEPS uzatvorenie zmluvy s dodávateľom a je poverený rokovať s dodávateľom o zmluvných podmienkach. Koordinuje aj osoby oprávnené rokovať o veciach technických. Je zodpovedný za celý životný cyklus zmluvy s dodávateľom – príprava, finalizácia, podpis, monitoring, vyhodnotenie a ukončenie zmluvného vzťahu.

Vlastník aktíva : zamestnanec SEPS, ktorý zodpovedá za životný cyklus prideleného aktíva. Je zodpovedný za špecifikáciu technických a procesno-aplikačných požiadaviek spoločnosti SEPS na aktívum a za správne vykonanie opatrení spojených s bezpečnostnými požiadavkami.

Manažér kybernetickej bezpečnosti : je najvyšší predstaviteľ informačnej a kybernetickej bezpečnosti v SEPS (pre oblasť ISMS podľa normy ISO/IEC 27001 je táto pozícia definovaná ako CISO). Náplň činnosti MKB stanovuje zákon 69/2018 a vyhláška NBÚ 362/2018. Vo vzťahu k dodávateľom 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 MKB oprávnený vykonať u dodávateľa bezpečnostný audit v rozsahu definovanom medzinárodným štandardom ISO 27001. MKB musí úzko spolupracovať s Manažérom bezpečnosti dodávateľa na udržiavaní primeranej odozvy na bezpečnostné incidenty/výsledky auditov a poskytnúť aktualizácie akýchkoľvek prebiehajúcich zmien bezpečnostných postupov a politík objednávateľa.

Manažér informačných rizík (MIR) : je rola, ktorá je zodpovedná za proces riadenia informačných rizík v SEPS. Okrem riadenia procesu je zodpovedný za identifikovanie, posúdenie, ohodnotenie a ošetrenie identifikovaných rizík, v tomto prípade rizík, ktoré sa týkajú dodávateľov.

Manažér bezpečnosti IT/OT (MBITOT) : je rola, ktorá je zodpovedná za vykonávanie a dodržiavanie bezpečnostných pravidiel pri prevádzke systémov a aplikácií v SEPS.

Manažér dodávateľa: Manažér dodávateľa je osoba dodávateľa definovaná v zmluve ako osoba oprávnená

rokovať vo veciach technických, v anglických pomenovaniach je rola známa ako „Delivery manager". Zodpovednosťou manažéra dodávateľa je organizovanie a koordinovanie technickej a technologickej časti dodávky/dodávok a 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.

Manažér bezpečnosti dodávateľa: Manažér bezpečnosti dodávateľa zodpovedá za dodržiavanie bezpečnostných pravidiel a politík objednávateľa. Manažér bezpečnosti dodávateľa spolupracuje pri bezpečnostných auditoch vykonaných MKB alebo ním povereným externým subjektom u dodávateľa a je zodpovedný za implementáciu primeraných organizačných, technických alebo personálnych opatrení za účelom zníženia rizík identifikovaných bezpečnostným auditom. Manažér bezpečnosti dodávateľa je ďalej zodpovedný za priebežnú aktualizáciu a riadenie rizík súvisiacich s dodávanými prácami, službami alebo tovarmi s potenciálnym dopadom na objednávateľa. Manažéra bezpečnosti dodávateľa určí manažér dodávateľa. V prípade, že dodávateľ nemá vytvorenú funkciu manažéra bezpečnosti dodávateľa, túto rolu/funkciu prevezme manažér dodávateľa sám.

1 Všeobecné bezpečnostné požiadavky a pravidlá pre dodávateľov

1.1 Preskúmanie procesov informačnej a kybernetickej bezpečnosti u dodávateľa

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

1.1.2 Manažér bezpečnosti dodávateľa musí preskúmať spolu s MKB (príp. MIR) všetky riziká identifikované prostredníctvom preverenia infraštruktúry a auditov.

1.1.3 Dodávateľ 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 alebo KB v SEPS.

1.1.4 Okrem auditov zmluvných dohôd/záväzkov vo vzťahu k SEPS, musí dodávateľ 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 organizačnej, fyzickej, personálnej a technologickej bezpečnosti v súlade s ISO/IEC 27001: 2022 a ISO/IEC 27002: 2022. Žiadosť o vykonanie komplexného bezpečnostného auditu objednávateľ oznámi dodávateľovi písomne min. 30 kalendárnych dní pred začatím auditu.

1.1.5 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.

1.2 Organizačná bezpečnosť – organizačné opatrenia

1.2.1 **Inventár, vlastníctvo a klasifikácia aktív**

1.2.1.1 Dodávateľ musí mať formalizovaný a zavedený proces riadenia aktív, minimálne v rozsahu:

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

1.2.2.1 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.

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

1.2.3.1 ICT aktíva a ich príslušenstvo musí mať evidenčné štítky alebo zaznamenané sériové čísla.

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

1.2.4 **Softvérové aktíva:** zmluvní partneri musia udržiavať softvérové aktíva používané pri plnení predmetu

zmluvy voči SEPS v aktuálnom stave.

1.2.5 **Ukladanie a narábanie s údajmi, ochrana informácií**

1.2.5.1 Zmluvní partneri musia pri práci s informáciami, resp. pri nakladaní s nimi dodržiavať minimálne požiadavky spĺňajúce nasledovné odporúčania:

1.2.5.2 Informácie v SEPS sa klasifikujú.

1.2.5.3 Na prístup k interným, chráneným a prísne chráneným informáciám je bezpodmienečne nutné, aby dodávateľ podpísal so SEPS dohodu o mlčanlivosti. Povinnosť uzatvoriť dohodu o mlčanlivosti sa vzťahuje aj na dodávateľov, ktorým je vystavená objednávka na poskytovaný tovar alebo služby;

1.2.5.4 Neverejné informácie (interné, chránené a prísne chránené) musia byť uložené zamknuté, chránené heslom/zašifrované.

1.2.5.5 Pri práci s papierovými dokumentmi SEPS je potrebné sa riadiť politikou čistého stola. Tlač citlivých, chránených alebo prísne chránených dokumentov SEPS nesmie byť ponechaná bez dozoru.

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

1.2.5.7 Nesmú sa robiť kópie citlivých, chránených alebo prísne chránených informácií bez povolenia vlastníka informácii za SEPS.

1.2.5.8 Údaje a dokumenty SEPS používané dodávateľom 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 dodávateľa. Manažér dodávateľa 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 MKB za SEPS), ktorí autorizovali prenos s týmito opatreniami.

1.2.5.9 Dodávateľ 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.

1.2.5.10 Dodávateľ je oprávnený poskytovať zmluvou dohodnuté činnosti len prostredníctvom zamestnancov, ktorí boli odsúhlasení objednávateľom.

1.2.5.11 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.

1.2.5.12 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.

1.2.5.13 Všetky ostatné spôsoby narábania s informáciami v SEPS sa riadia smernicou 04/2022 Klasifikácia informácií v SEPS.

1.2.6 **Výmena informácií**

1.2.6.1 Zmluvní alebo iní externí partneri musia pri výmene informácií s objednávateľom dodržiavať nasledovné odporúčania:

1.2.6.2 Elektronická komunikácia: Citlivé a prísne chránené informácie SEPS musia byť pri prenose elektronickou poštou vo forme príloh šifrované, chránené šifrované byť nemusia, ale je možné vymieňať ich len medzi oprávnenými osobami.

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

1.2.7 **Pravidlá pre dodávateľské Notebooky/PC pripájané do infraštruktúry SEPS**

1.2.7.1 Zmluvní partneri musia mať definovanú politiku pre primerané použitie ICT aktív.

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

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

1.3 Personálna bezpečnosť – personálne opatrenia

1.3.1 Dodávateľ 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 dodávateľa, ktorý zabezpečuje dodávku tovarov, prác alebo služieb pre objednávateľa na kritických systémoch, aplikáciách, resp. má prístup k citlivým informáciám.

1.3.2 Manažér dodávateľa 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 dodávateľa, ktorí sa podieľajú na plnení predmetu zmluvy. Manažér dodávateľa musí mať definovaný formálny proces pre odozvu na porušenie bezpečnostných politík a predpisov.

1.4 Fyzická bezpečnosť – opatrenia fyzickej bezpečnosti

1.4.1 Vo všetkých areáloch a objektoch SEPS je zakázané vyhotovovať fotografické a video záznamy. Výnimku v tomto smere majú technické kamerové systémy na implementovanie požiadaviek fyzickej bezpečnosti, ktoré sú vo vlastníctve SEPS

1.4.2 Fyzickú ochranu na niektorých objektoch SEPS zabezpečuje súkromná bezpečnostná služba, ktorá vykonáva zabránenie vjazdu motorových vozidiel a vstupu neoprávneným a nepovolaným osobám do objektov a areálov SEPS

1.4.3 Je zakázané neautorizované vynášanie majetku SEPS

1.4.4 Pri vzniku bezpečnostného incidentu sa informujú riadiace orgány SEPS, ktoré zabezpečia nadväzné činnosti v súvislosti s fyzickou bezpečnosťou.

1.4.5 Všetky návštevy v SEPS sú evidované strážnou službou a návštevy sú sprevádzané zamestnancom SEPS.

1.5 Riadenie prevádzky – technologické opatrenia

1.5.1 Kontinuita činností

1.5.1.1 Manažér bezpečnosti dodávateľa 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. Manažér bezpečnosti dodávateľa informuje o existencii a kvalite kontinuity plánov dodávateľa manažéra kontinuity v SEPS.

1.5.1.2 Manažér kontinuity v SEPS a spolupráci s MKB SEPS musia zabezpečiť prípravu, udržiavanie a pravidelné testy SEPS BCP/DRP plánov, ktoré umožnia dostupnosť všetkých kritických služieb vo vzťahu k objednávateľovi v prípade núdze alebo katastrofy a spĺňajú podmienky minimálnej požadovanej úrovne služieb.

1.5.1.3 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 .

1.5.2 Odozva na incidenty

1.5.2.1 Manažér bezpečnosti dodávateľa musí udržiavať a aktualizovať plán odozvy na bezpečnostné incidenty.

1.5.2.2 Manažér bezpečnosti dodávateľa musí SEPS MKB bezodkladne informovať o bezpečnostných incidentoch, ktoré dodávateľ zistí pri plnení predmetu zmluvy (jedná sa najmä o incidenty charakteru neautorizovaný prístup, narušenie dôvernosti alebo dostupnosti citlivých údajov, identifikovaný škodlivý kód).

1.5.2.3 Pokiaľ z predmetu zmluvy pre dodávateľa 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 dodávateľa a SEPS MKB musia v čo najkratšom možnom čase dohodnúť postup, resp. vzájomne odsúhlasiť zmeny za účelom odstránenia bezpečnostného incidentu

a spôsob realizácie plánu budúcich činností.

1.5.3 **Súlad s predpismi**

Ak je ktorékoľvek ustanovenie tejto politiky v konflikte s politikami dodávateľa, tento problém musí byť predložený SEPS MKB a garantovi zmluvy v SEPS na preskúmanie a vyriešenie ešte pred podpisom zmluvy.

1.6 Doplňujúce informácie

Ďalšie bezpečnostné požiadavky, najmä špecifické vo vzťahu ku konkrétnym aplikáciám, systémom ako aj ku sieťovej konektivite môžu byť špecifikované vlastníkom informačného systému v SEPS

Dodávateľ je povinný spoločnosť SEPS bezodkladne písomne informovať o každej zmene špecifikácie a/alebo rozsahu bezpečnostných opatrení s dopadom na kybernetickú bezpečnosť spoločnosti SEPS. V prípade pochybností platí, že zmena bezpečnostných opatrení má dopad na kybernetickú bezpečnosť spoločnosti SEPS.

Prijaté bezpečnostné opatrenia je Dodávateľ povinný zdokumentovať v bezpečnostnej dokumentácii vypracovanej v súlade so Zákonom o kybernetickej bezpečnosti a Vyhláškou NBÚ; bezpečnostnú dokumentáciu je Dodávateľ povinný priebežne aktualizovať a o každej zmene bezpečnostnej dokumentácie je povinný spoločnosť SEPS bezodkladne písomne informovať.

Časť 3.
Zoznam pracovných rolí/pozícií a zamestnancov Dodávateľa s prístupom k informáciám a údajom spoločnosti SEPS a doručovanie informácií druhej strane

Meno a priezvisko	Pracovná rola / pozícia	E-mail	Tel. číslo
Mojmír Prídavok	konateľ		
Róbert Hanzen	riaditeľ IT		
Martin Oravec	konzultant		

Kontaktné osoby a doručovanie

1. Spoločnosť SEPS určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom na v oblasti informačnej a kybernetickej bezpečnosti:
   Meno, priezvisko:
   Telefónne číslo:

2. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu so spoločnosťou SEPS v oblasti informačnej a kybernetickej bezpečnosti:
   Meno, priezvisko:
   Telefónne číslo:

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).

Záväzné požiadavky na zabezpečenie vzdialeného prístupu k prostriedkom a technológiám ICT, Slovenskej elektrizačnej prenosovej sústavy, a.s.

Zhotoviteľ/Poskytovateľ/Dodávateľ sa zaväzuje, že pri výkone činností predmetu plnenia Zmluvy prostredníctvom vzdialeného prístupu bude dodržiavať nasledovné podmienky a pravidlá:

1. Oprávnená osoba zodpovedná za veci zmluvné Zhotoviteľa/Poskytovateľa/Dodávateľa zašle najneskôr do 20 dní pred požadovaným termínom zriadenia VPN prístupu prostredníctvom emailu oprávnenej osobe Objednávateľa zodpovednej za veci zmluvné nasledovné informácie:
   a) zoznam osôb oprávnených vzdialene pristupovať k ICT prostriedkom SEPS (Meno, Priezvisko, pracovné zaradenie, email, telefonický kontakt),
   b) IP adresu, z ktorej sa bude pristupovať k infraštruktúre SEPS

   V prípade zmeny/doplnenia kontaktov vzdialeného prístupu sa proces opakuje.
2. Vzdialený prístup bude využívať výlučne na realizáciu prác súvisiacich s predmetom plnenia Zmluvy.
3. Zhotoviteľ/Poskytovateľ/Dodávateľ nesmie prístupové údaje (napr. meno, heslo, token...) poskytnúť iným osobám, než sú jeho zamestnanci, ktorých zoznam doručil do SEPS (zoznam osôb oprávnených vzdialene pristupovať k ICT),
4. požiada oprávnenú osobu SEPS o bezodkladné zablokovanie svojho prístupového účtu v prípade výskytu akejkoľvek udalosti, v dôsledku ktorej by mohlo dôjsť k zneužitiu zriadeného vzdialeného prístupu,
5. pri vzniku bezpečnostnej udalosti, v dôsledku ktorej mohlo prísť ku narušeniu dôvernosti, integrity, alebo dostupnosti dát alebo došlo k bezpečnostnému incidentu na infraštruktúre Zhotoviteľa/Poskytovateľa/Dodávateľa počas výkonu predmetu plnenia, neodkladne informovať Objednávateľa prostredníctvom e-mailovej adresy bezpecnost@sepsas.sk ,
6. upozorní oprávnenú osobu Objednávateľa na zistené nedostatky alebo technické problémy, ktoré sa vyskytnú počas vzdialeného prístupu,
7. poskytne súčinnosť pri riešení incidentov týkajúcich sa vzdialeného prístupu,
8. pre vzdialené pripojenie k ICT SEPS bude Zhotoviteľ/Poskytovateľ/Dodávateľ používať výhradne výpočtovú techniku, ktorá má aplikované všetky aktuálne bezpečnostné záplaty, pre daný operačný systém a ktorá má nainštalovaný antimalvérový systém aktualizovaný ku dňu pripojenia,
9. na vzdialené pripojenie k ICT SEPS nebude využívať výpočtovú techniku, ktorá obsahuje alebo obsahovala počítačový vírus alebo škodlivý softvér, o ktorom bol Zhotoviteľ/Poskytovateľ/Dodávateľ notifikovaný antivírusovým softvérom a ktorý nebol odborne odstránený.
10. Zhotoviteľ/Poskytovateľ/Dodávateľ nesmie počas využívania vzdialeného prístupu opustiť pripojenú výpočtovú techniku, dovoliť iným osobám prístup k tejto technike, alebo sledovanie jej aktívnej obrazovky,
11. bezvýhradne akceptuje, že všetky činnosti ktoré bude vykonávať v prostredí ICT SEPS budú monitorované a zaznamenávané.
12. Zhotoviteľ/Poskytovateľ/Dodávateľ sa zaväzuje zachovávať mlčanlivosť o informáciách získaných v súvislosti s predmetom plnenia.
13. Zhotoviteľ/Poskytovateľ/Dodávateľ sa zaväzuje, že Objednávateľovi uhradí akékoľvek škody ktoré mu vzniknú ako dôsledok narušenia integrity, dôvernosti, alebo dostupnosti informačných systémov SEPS, ku ktorým príde počas vzdialeného pripojenia do siete SEPS, alebo následne, ako dôsledok takéhoto pripojenia.

Všeobecné podmienky zachovania mlčanlivosti

1. Tieto všeobecné podmienky zachovania mlčanlivosti (ďalej len „Podmienky zachovania mlčanlivosti" alebo „Príloha") tvoria neoddeliteľnú súčasť Zmluvy, a spoločnosť Slovenská elektrizačná prenosová sústava, a.s. (ďalej len „spoločnosť SEPS") ich vyžaduje ako prílohu samotnej Zmluvy, s ohľadom na skutočnosť, že:

- SEPS poskytne Prijímateľovi všetky informácie a dáta (vymedzené v bode 3. tejto Prílohy), potrebné na realizáciu predmetu Zmluvy a za účelom uvedeným v predmete Zmluvy,
- informácie poskytnuté v zmysle Zmluvy môžu byť súčasťou kritickej infraštruktúry a ich špecifikácia môže obsahovať citlivé informácie o prenosovej sústave Slovenskej republiky, ktorých únik môže predstavovať bezpečnostné riziko, a preto spoločnosť SEPS vyžaduje ochranu pred únikom informácií.

2. Napriek prípadnému rozdielnemu označeniu zmluvných strán podľa Zmluvy tieto Podmienky zachovania mlčanlivosti zodpovedajú stavu, že spoločnosť SEPS má postavenie Poskytovateľa a druhá zmluvná strana má postavenie Prijímateľa.
3. Zmluvné strany sa dohodli, že informácie, špecifikácie a iné údaje bez ohľadu na to, či majú technický, bezpečnostný, odborný, obchodný, prevádzkový, informačný alebo iný charakter, ktoré Poskytovateľ sprístupní Prijímateľovi, sú dôverné (ďalej len „**Dôverné informácie**").
4. Prijímateľ berie na vedomie, že Poskytovateľ ani iná osoba konajúca v mene Poskytovateľa nedáva týmto žiadne vyhlásenie alebo záruku, či už výslovnú alebo implikovanú, týkajúcu sa presnosti, spoľahlivosti alebo úplnosti akejkoľvek Dôvernej informácie.
5. Prijímateľ je povinný zachovávať mlčanlivosť o Dôverných informáciách, ibaže by z Podmienok zachovania mlčanlivosti alebo Zmluvy alebo z ustanovení príslušných všeobecne záväzných právnych predpisov vyplývalo inak.
6. Prijímateľ sa zaväzuje, že:
   (a) všetky Dôverné informácie získané od SEPS neposkytne žiadnej tretej strane;
   (b) nezverejní, nebude obchodovať a ani akýmkoľvek iným spôsobom neposkytne akejkoľvek tretej osobe akýkoľvek údaj týkajúci sa Dôverných informácií;
   (c) nebude Dôverné informácie a/alebo ich nosiče využívať na iný účel než je uvedený v Zmluve a/alebo spôsobom, ktorým by poškodzoval Poskytovateľa.
7. Prijímateľ sa zaväzuje informovať Poskytovateľa okamžite po zistení neoprávnenej manipulácie s Dôvernými informáciami Prijímateľom alebo inou osobou, alebo o inom porušení práv a povinností v zmysle tejto prílohy.
8. Povinnosť zachovávať mlčanlivosť o Dôverných informáciách sa nevzťahuje na:
   (a) informácie, ktoré sú už v deň podpisu Zmluvy verejne známe, alebo ktoré je možné v deň podpisu Zmluvy získať z bežne dostupných informačných zdrojov;
   (b) informácie, ktoré sa stanú po podpise Zmluvy verejne známymi, alebo ktoré bude možné po tomto dni získať z bežne dostupných informačných zdrojov inak než porušením povinnosti Prijímateľa zachovávať mlčanlivosť na základe Zmluvy a tejto prílohy;
   (c) informácie, ktoré nie sú verejne známe a ktoré Prijímateľ získal alebo získa v súlade so všeobecne záväzným právnym predpisom od tretej osoby, ak súčasne tretia osoba poskytnutím týchto informácií Prijímateľovi neporušila všeobecne záväzný právny predpis;

(d) prípady, keď na základe zákona vznikne Prijímateľovi povinnosť poskytnúť Dôverné informácie. Prijímateľ je povinný informovať Poskytovateľa o vzniku povinnosti poskytnúť Dôverné informácie na základe zákona a o spôsobe a rozsahu, akým, resp. v akom ju plnil.

9. Prijímateľ sa zaväzuje zaviazať záväzkom mlčanlivosti v rovnakom rozsahu svojich riadiacich pracovníkov, zamestnancov, právnych a finančných poradcov, subdodávateľov, prípadne iné osoby, ktorým sprístupnil alebo poskytol Dôverné informácie v súlade so Zmluvou a touto prílohou a chrániť Dôverné informácie na dostatočnej úrovni, minimálne však na úrovni ako chráni svoje vlastné dôverné informácie a obchodné tajomstvo.
10. Prijímateľ sa zaväzuje k preukázateľnému poučeniu z povinnosti mlčanlivosti všetkých svojich zamestnancov (ako aj subdodávateľov), ktorí sa zúčastnia na poskytovaní zmluvných služieb, o všetkých skutočnostiach, s ktorými sa oboznámia pri výkone prác, služieb alebo dodávok tovarov podľa zmluvy, a to ako po dobu trvania Zmluvy, tak aj po jej skončení. Záznam o poučení musí obsahovať minimálne presný dátum a miesto poučenia, kto poučenie vykonal, mená a priezviská poučených zamestnancov, ako aj ich podpis potvrdzujúci, že poučeniu porozumeli.
11. Prijímateľ je oprávnený vytvárať len presný počet výtlačkov akejkoľvek dokumentácie, ktorú požaduje Poskytovateľ. Prijímateľ zodpovedá za to, že nedôjde k zneužitiu, strate, úniku alebo odcudzeniu informácií a dokumentov získaných a spracovaných počas plnenia predmetu zmluvy. Pre zabezpečenie tejto povinnosti Prijímateľ príjme primerané organizačné, personálne a technické opatrenia. V prípade, že Prijímateľ zistí porušenie týchto zodpovedností, je povinný o tom bezodkladne písomne informovať osobu Poskytovateľa oprávnenú konať vo veciach zmluvných.
12. Prijímateľ je povinný po ukončení zmluvného vzťahu odovzdať všetky informácie a dokumenty získané v súvislosti s plnením predmetu zmluvy Poskytovateľovi.
13. Pre potreby masmédií môžu poskytovať informácie iba poverení zástupcovia Objednávateľa.
14. Predchádzajúcimi ustanoveniami nie je obmedzené právo na ochranu obchodného tajomstva v zmysle ust. § 17 a nasl. Obchodného zákonníka.
15. Prijímateľ je povinný v prípade porušenia povinnosti mlčanlivosti podľa tejto Prílohy uhradiť Poskytovateľovi zmluvnú pokutu vo výške 10.000,- EUR (slovom desaťtisíc eur) za každé jednotlivé porušenie.
16. Zmluvná pokuta podľa bodu 14. tejto Prílohy je splatná na základe vystavenej faktúry s lehotou splatnosti 15 dní odo dňa jej vystavenia. Uhradením zmluvnej pokuty zostáva povinnosť nahradiť vzniknutú škodu v plnej výške nedotknutá.
17. Prijímateľ vyhlasuje, že zmluvná pokuta uvedená v bodoch 14. a 15. tejto Prílohy je dohodnutá v súlade s dobrými mravmi a zásadami poctivého obchodného styku, s ohľadom na obchodné zvyklosti zachovávané v danej podnikateľskej oblasti a je primeraná vzhľadom na podnikateľské riziko, ktoré znáša Poskytovateľ v prípade, ak by Prijímateľ alebo ktorákoľvek z osôb uvedených v bode 10. tejto prílohy porušili ustanovené povinnosti.
18. Ustanovenia o zachovaní mlčanlivosti zostávajú v platnosti 10 (slovom desať) rokov po ukončení Zmluvy.

Proces riadenia zmenových požiadaviek

1. Predmetom tejto služby sú tie požiadavky Objednávateľa, ktoré nie sú klasifikované ako Vady/Problémy alebo Servisné požiadavky.
2. V rámci manažmentu a dodávky Zmenových požiadaviek Poskytovateľ vykoná minimálne tieto aktivity:

2.1 Analýza požiadavky na Zmenovú požiadavku z pohľadu časovej a finančnej náročnosti
2.2 Spracovanie návrhu riešenia
2.3 Realizácia a otestovanie riešenia Zmenovej požiadavky internými postupmi Poskytovateľa
2.4 Dodávka Zmenovej požiadavky

3. Zákazník predloží požiadavku na Zmenovú požiadavku minimálne s nasledovnými atribútmi:

3.1 Identifikačné číslo (ID)
3.2 Meno zodpovednej osoby Objednávateľa
3.3 Popis požadovanej Zmenovej požiadavky
3.4 Dátum a čas predloženia

4. Poskytovateľ po obdržaní písomnej (emailom) požiadavky Objednávateľa spracuje podľa dohodnutej úrovne parametrov tejto Zmluvy návrh riešenia požiadavky na Zmenovú požiadavku a odhadovanú prácnosť v MD.
5. Návrh riešenia požiadavky na Zmenovú požiadavku musí obsahovať nasledujúce náležitosti:

5.1 Cieľ zadania - jedná sa o stručnú sumarizáciu zadania.
5.2 Popis zadania - ide o analytický výstup z požiadaviek Objednávateľa. Jedná sa o podrobnú špecifikáciu zadania Zmenovej požiadavky na dostatočne detailnej úrovni umožňujúcej začatie realizačných prác.
5.3 Nároky na súčinnosť Objednávateľa – je určená vecná a časová súčinnosť, ktorú bude Poskytovateľ požadovať od Objednávateľa v súvislosti s realizáciou Zmenovej požiadavky.
5.4 Kalkulácia - predstavuje rozpis času potrebného na realizáciu Zmenovej požiadavky.

6. Po písomnom (emailom) schválení návrhu riešenia Drobnej zmeny oprávnenými zástupcami oboch zmluvných strán, vykoná Poskytovateľ jej realizáciu v dohodnutých termínoch.
7. Lehoty dodania a dodacích podmienok Zmenových požiadaviek budú konkrétne stanovené dohodou v príslušných písomných (emailom) Objednávkach. Poskytovateľ má právo s predchádzajúcim súhlasom Objednávateľa Zmenovú požiadavku dodať v termíne kratšom, než je uvedený v Objednávke. Odovzdanie Zmenovej požiadavky na akceptačné testovanie bude potvrdené odovzdávacím protokolom v písomnej (emailovej) forme zodpovednou osobou Objednávateľa. Zmenová požiadavka bude vždy pre potreby tejto Zmluvy pokladaná zo strany Poskytovateľa za odovzdanú, ak Objednávateľ z dôvodov na strane Objednávateľa, v lehote 10 pracovných dní od dňa jej doručenia Objednávateľovi nepotvrdí odovzdávací protokol.
8. Zmenová požiadavka bude spravidla, ak v schválenom návrhu riešenia Zmenovej požiadavky nie je stanovené inak alebo ak sa zodpovedné osoby Zmluvných strán nedohodnú inak, najprv testovaná internými postupmi Poskytovateľa, potom bude odovzdaná Objednávateľovi k otestovaniu.

9. Všetky Vady/Problémy zistené v priebehu akceptačných testov je Objednávateľ povinný oznamovať Poskytovateľovi bez zbytočného odkladu a to vopred dohodnutou formou na Service Desk. Zákazníkom nahlásené Vady/Problémy je Poskytovateľ povinný odstrániť v termíne dohodnutom medzi zodpovedným zástupcom Objednávateľa a zodpovedným zástupcom Poskytovateľa. V priebehu akceptačných testov zodpovedné osoby Objednávateľa a Poskytovateľa priebežne prerokúvajú spôsoby a termíny riešenia nahlásených Vád/Problémov.
10. Akceptácia Zmenovej požiadavky bude uskutočnená po úspešných akceptačných testoch, ak nie je v schválenom návrhu riešenia určené inak. Podmienkou akceptácie je, že daná Zmenová požiadavka spĺňa akceptačné kritériá. Akceptácia Zmenovej požiadavky bude potvrdená akceptačným protokolom v písomnej (emailovej) forme zodpovednou osobou Objednávateľa.
11. Zmenová požiadavka vytvorená podľa Objednávateľom schváleného návrhu riešenia bude vždy považovaná za akceptovanú, ak je Zmenová požiadavka riadne odovzdaná a Objednávateľ prekročí termín ukončenia akceptačných testov uvedených v schválenom návrhu riešenia o viac ako 10 pracovných dní a zároveň sú splnené akceptačné kritéria a Objednávateľ neohlási Poskytovateľovi žiadne Vady/Problémy, ktoré by spôsobili nesplnenie podmienky akceptácie.
12. Výsledná cena za realizáciu Zmenovej požiadavky je vypočítaná ako súčin rozpisu času potrebného na realizáciu Zmenovej požiadavky, poskytnutý Poskytovateľom vo forme kalkulácie pri návrhu riešenia a fixnou sadzbou za 1 MD prác, ktorý bol Zmluvnými stranami dohodnutý vo výške 350,00 € (slovom: tristopäťdesiat eur).
13. Poskytovateľ je oprávnený fakturovať cenu za realizáciu Zmenových požiadaviek po poskytnutí príslušných služieb a ich akceptácii Objednávateľom. Poskytovateľ sa zaväzuje vystaviť príslušné faktúry za objednané služby Zmenových požiadaviek do 15 dní od ich riadneho poskytnutia a akceptácie Zmenových požiadaviek.

p.č.	Miľník č.	Názov položky	cena za MD/rok	počet MD/rok	suma bez DPH spolu (v EUR)
1.		Ročný poplatok za prístup do IS	20 000,00 €	4	80 000,00 €
2.	1.	Analýza procesu obstarávania a návrh riešenia	350,00 €	30	10 500,00 €
3.	2.	Implementácia "interné obstarávanie"	350,00 €	9	3 150,00 €
4.	2.	Hodnotenie dodávateľov	350,00 €	56	19 600,00 €
5.	2.	Zapracovanie šablón	350,00 €	9,5	3 325,00 €
6.	2.	Digitalizácia požiadaviek na obstarávanie	350,00 €	61,25	21 437,50 €
7.	2.	Reporting - štatistika	350,00 €	20	7 000,00 €
8.	2.	Vstupné školenia a aktualizácia internej dokumentácie	350,00 €	3	1 050,00 €
9.	2.	Modul dodávateľ	350,00 €	7,5	2 625,00 €
10.	3.	Registratúra	350,00 €	28	9 800,00 €
11.	3.	Integrácia na SAP	350,00 €	40	14 000,00 €
12.	3.	Integrácia na finstat	350,00 €	25	8 750,00 €
13.	3.	Integrácia na OR SR	350,00 €	2,5	875,00 €
14.	3.	Integrácia na UVO-zoznam hospodárskych subjektov	350,00 €	5	1 750,00 €
15.	3.	Integrácia na RPVS	350,00 €	2,5	875,00 €
			Spolu:	299,25	184 737,50 €

Ročný poplatok	80 000,00 €
Miľník č. 1	10 500,00 €
Miľník č. 2	58 187,50 €
Miľník č. 3	36 050,00 €

Všeobecné zmluvné podmienky zabezpečovania BOZP a OPP

1. Zhotoviteľ 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 zhotoviteľa

   Meno a priezvisko: Róbert Hanzen

   Funkcia: *Riaditeľ IT*

   a technika požiarnej ochrany zhotoviteľa

   Meno a priezvisko: Ing. Antónia Hupková

   Číslo osvedčenia: KRHZ-KE-OPP-352-001/2018

   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. Zhotoviteľ 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. Zhotoviteľ 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 zhotoviteľa zdržujú v objektoch a priestoroch SEPS, hore uvedeným technikom požiarnej ochrany. Zhotoviteľ 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. Zhotoviteľ 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. Zhotoviteľ 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. Zhotoviteľ 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. Zhotoviteľ 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 zhotoviteľ 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 zhotoviteľ povinný ihneď ohlásiť a následne písomne oznámiť aj objednávateľovi s cieľom zabezpečenia objektívneho vyšetrenia.
10. Zhotoviteľ 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. Zhotoviteľ je povinný zabezpečiť jednotné oblečenie a viditeľné označenie svojich zamestnancov názvom - logom firmy, ako aj zamestnancov svojich subdodávateľov a spolupôsobiacich fyzických osôb - podnikateľov.
12. Zhotoviteľ 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 zhotoviteľ na požiadanie predložiť zodpovednému zástupcovi objednávateľa.
13. Zhotoviteľ je povinný písomne požiadať objednávateľa o povolenie vjazdu vozidiel s uvedením typu, EČV a účelu vjazdu vozidla. V objektoch objednávateľa sú vozidlá zhotoviteľa 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 zhotoviteľ 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 zhotoviteľa 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 zhotoviteľa spôsobené nerešpektovaním dopravného značenia a parkovaním na vyhradených miestach pre vozidlá hasičského a záchranného zboru alebo rýchlej zdravotnej služby.
17. Zhotoviteľ je povinný na preukázateľne (zápisnične) prevzatom stavenisku (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. Zistené skutočnosti, odporujúce predpisom bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi, je povinný ihneď po zistení, zaznamenať do **stavebného (montážneho)** denníka.
18. Povinnosťou zhotoviteľa je preukázateľne upozorniť objednávateľa na riziká, vyplývajúce z činností pre splnenie predmetu zmluvy, ktoré bude na pracoviskách a v priestoroch objednávateľa vykonávať.
19. Zamestnanci zhotoviteľa 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, zhotoviteľ 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. Zhotoviteľ 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. Zhotoviteľ 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 zhotoviteľa resp. jeho spolupôsobiacich dodávateľov bude týmto odobraté oprávnenie pre vstup do objektu objednávateľa bez dopadu na plnenie zmluvných záväzkov zhotoviteľa.
22. Pri výkone pracovných činností sú zmluvné strany povinné rešpektovať vzájomné pripomienky, uvedené v stavebnom resp. montážnom denníku z oblasti bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi.
23. **Za nedodržanie zmluvných podmienok BOZP a OPP je zhotoviteľ povinný uhradiť zmluvnú pokutu vo výške 2000,- €.** V prípade, ak objednávateľ zistí, že zamestnanci zhotoviteľa 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 zhotoviteľovi vznikol nárok na náhradu prípadnej škody alebo nabehnutých nákladov.
24. Uložením zmluvnej pokuty nie je zhotoviteľ zbavený zodpovednosti za nedostatky v oblasti BOZP a OPP zistené kontrolnými orgánmi, ktoré boli spôsobené činnosťou zhotoviteľa. Ak bude na základe zisteného porušenia právnych predpisov činnosťou zhotoviteľa uložená pokuta objednávateľovi, zhotoviteľ uhradí uloženú pokutu v plnej výške.

    Zápis o poučení zodpovedného zamestnanca a požiarneho technika zhotoviteľa poverenýmzamestnancom SEPS, je neoddeliteľnou súčasťou uzatvorenej zmluvy o dielo alebo vydanej objednávky na výkon prác.

Zoznam subdodávateľov

Príloha č.10

.	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.											