Slovenská elektrizačná prenosová sústava

číslo zmluvy Objednávateľa: 2024-0156-1176520

číslo zmluvy Zhotoviteľa:

ZMLUVA O DIELO

uzavretá podľa §536 a nasl. zákona. č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „Obchodný zákonník")

(ďalej len „Zmluva")

I. ZMLUVNÉ STRANY

1.1 Objednávateľ: **Slovenská elektrizačná prenosová sústava, a.s.**
Mlynské nivy 59/A
824 84 Bratislava

Zapísaný: Obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka č. 2906/B

IČO: 35 829 141
DIČ: 2020261342
IČ DPH: SK2020261342

Bankové spojenie: TATRA BANKA, a. s. Bratislava
Číslo účtu: 2620191900/1100
IBAN: SK301100 0000 0026 2019 1900
SWIFT: TATRSKBX

Menom spoločnosti koná: Ing. Martin Magáth, predseda predstavenstva
Ing. Miloš Bikár, PhD., podpredseda predstavenstva

Osoby oprávnené rokovať vo veciach:
zmluvných: Ing. Marián Sabol, výkonný riaditeľ sekcie investícií PaSC
technických: Ing. Tibor Szabo, výkonný riaditeľ sekcie bezpečnosti
Bc. Peter Kazimír, vedúci odboru telekomunikácií
Ing. Bohumil Markech, vedúci odboru investícií ICT

(ďalej aj ako „Objednávateľ" alebo „SEPS")

1.2 Zhotoviteľ: **SOITRON, s.r.o.**
Plynárenská 5, 829 75 Bratislava

Zapísaný: v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sro, vložka č. 37618/B
IČO: 35 955 678
DIČ: 2022066937
IČ DPH: SK2022066937

Bankové spojenie: Tatra banka, a. s.
Číslo účtu: 2625832658/1100
IBAN: SK40 1100 0000 0026 2583 2658
SWIFT: TATRSKBX

Menom spoločnosti koná: Ing. Marián Skákala, výkonný riaditeľ a konateľ spoločnosti
Ing. Ondrej Smolár, konateľ spoločnosti

Osoby oprávnené rokovať vo veciach:
zmluvných: Ing. Tibor Bálint, obchodný zástupca spoločnosti
technických: Ing. Peter Benko, Product Manager

(ďalej aj ako „Zhotoviteľ")

(ďalej spoločne aj ako „Zmluvné strany" alebo jednotlivo aj ako „Zmluvná strana")

II. PREAMBULA

2.1 Podkladom pre uzatvorenie tejto Zmluvy je výberové konanie a ponuka Zhotoviteľa ako úspešného uchádzača zo dňa 27.5.2024.

III. PREDMET ZMLUVY

3.1 Zhotoviteľ sa zaväzuje pre Objednávateľa zhotoviť dielo „Zvýšenie zabezpečenia DWDM - MPLS bezpečnostný monitoring" (ďalej len „dielo").

3.2 Predmetom diela je dodávka, konfigurácia, inštalácia zariadení pre zvýšenie zabezpečenia DWDM - MPLS bezpečnostný monitoring:

3.2.1 Návrhu technickej architektúry riešenia (HLD/LLD dizajn) v zmysle požiadaviek uvedených v Prílohe č. 1 „Špecifikácia predmetu plnenia", Prílohe č. 2 „Technická špecifikácia predmetu zákazky" a v Prílohe č. 3 „Tabuľky technických špecifikácií".

3.2.2 Dodávky potrebného HW a SW vrátane podpory výrobcu na obdobie 2 rokov (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 3.2.1) a všetkých potrebných hardvérových a softvérových licencií pre dodávané riešenie.

3.2.3 Konfigurácia zariadení, inštalácia zariadení, inštalácie všetkých dodaných komponentov a potrebného inštalačného materiálu (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 3.2.1).

3.2.4 Inštalácia a konfigurácia SW (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 3.2.1.

3.2.5 Realizácia testovacích scenárov a Disaster recovery plán (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 3.2.1).

3.2.6 Dokumentácie skutočného vyhotovenia, prevádzková dokumentácia.

3.2.7 Príručky administrátora, tabuľky elektrických a tepelných výkonov.

3.2.8 Oboznámenie obsluhy a administrátorov.

3.3 Rozsah predmetu plnenia sa zhotoviteľ zaväzuje vyhotoviť v zmysle Prílohy č. 1 až Prílohy č. 4 a Prílohy č. 6 až Prílohy č. 10 tejto Zmluvy.

3.4 Objednávateľ sa zaväzuje riadne zhotovené dielo prevziať osobami Objednávateľa oprávnenými rokovať vo veciach technických a zaplatiť Zhotoviteľovi dohodnutú zmluvnú cenu.

IV. ČAS A MIESTO PLNENIA

4.1 Zhotoviteľ sa zaväzuje zhotoviť a odovzdať dielo v častiach a vo fakturačných míľnikoch do 7 mesiacov od nadobudnutia účinnosti tejto Zmluvy.

4.1.1 Míľnik č. 1 v rozsahu bodov 3.2.1 do 2 mesiacov od nadobudnutia účinnosti tejto Zmluvy.

4.1.2 Míľnik č. 2 v rozsahu bodov 3.2.2 až 3.2.8 do 7 mesiacov od nadobudnutia účinnosti tejto Zmluvy.

4.2 Zhotoviteľ nie je oprávnený takto stanovené termíny plnenia meniť bez dohody s Objednávateľom. Záväzok zhotoviť dielo alebo jeho časť je splnený jeho odovzdaním a prevzatím zástupcami oboch Zmluvných strán oprávnenými rokovať vo veciach technických na mieste stanovenom v tejto Zmluve.

4.3 Pred dohodnutým termínom môže Zhotoviteľ odovzdať časť diela len so súhlasom osôb Objednávateľa oprávnených rokovať vo veciach zmluvných a technických.

4.4 Miestom realizácie a odovzdania diela je sídlo spoločnosti Slovenská elektrizačná prenosová sústava, a.s., administratívna budova SED Žilina.

V. CENA

5.1 Cena za zhotovenie diela v rozsahu článku III. tejto Zmluvy je stanovená dohodou Zmluvných strán podľa § 3 zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov. Kalkulácia ceny diela je v Prílohe č. 4 tejto Zmluvy.

5.2 Cena za zhotovenie celého diela podľa článku III. je 208 970 EUR.
(slovom: dvestoosemtisícdeväťstosedemdesiat EUR) bez DPH.

5.3 K cene bude uplatnená DPH v zmysle zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej aj ako „zákon o DPH"), platným v deň vzniku daňovej povinnosti.

5.4 V cene dohodnutej podľa bodu 5.2 tejto Zmluvy sú zahrnuté všetky náklady Zhotoviteľa pre zhotovenie diela.

VI. PLATOBNÉ PODMIENKY

6.1 Objednávateľ sa zaväzuje zaplatiť zmluvnú cenu uvedenú v bode 5.2 tejto Zmluvy, ak Zhotoviteľ dodá časti diela a dielo riadne a včas.

6.2 Právo na zaplatenie zmluvnej ceny vzniká Zhotoviteľovi riadnym zhotovením a odovzdaním častí diela definovaných v článku IV. osobám Objednávateľa oprávneným rokovať vo veciach technických, formou písomného protokolu o odovzdaní a prevzatí časti diela nasledovne:

6.2.1	Míľnik č. 1 v rozsahu bodu 4.1.1 tejto Zmluvy	9 600,00	EUR bez DPH
6.2.2	Míľnik č. 2 v rozsahu bodu 4.1.2 tejto Zmluvy	199 370,00	EUR bez DPH

6.3 Zhotoviteľ je oprávnený vystaviť faktúru na základe protokolu o odovzdaní a prevzatí časti diela podpísaného osobami Objednávateľa a Zhotoviteľa oprávnenými rokovať vo veciach technických a zmluvných.

6.4 Protokol o odovzdaní a prevzatí časti diela v zmysle bodu 6.3 tejto Zmluvy, ktorého presná forma a rozsah bude vzájomne dohodnutá (návrh protokolu predloží Zhotoviteľ osobe Objednávateľa oprávnenej rokovať vo veciach technických najneskôr 14 dní pred termínom splnenia časti diela), vypracuje Zhotoviteľ a predloží ho na odsúhlasenie Objednávateľovi. Prílohou protokolu o odovzdaní a prevzatí časti diela bude osobami Objednávateľa oprávnenými rokovať vo veciach technických odsúhlasený súpis skutočne dodaného rozsahu v členení podľa Prílohy č. 4 tejto Zmluvy preukazujúci rozsah odovzdávanej časti diela.

6.5 Cenu za jednotlivé časti diela uhradí Objednávateľ na základe faktúr, ktoré Zhotoviteľ vystaví do 15 dní odo dňa vzniku daňovej povinnosti a doručí Objednávateľovi. Dňom vzniku daňovej povinnosti je deň prevzatia časti diela Objednávateľom formou podpísania protokolu o odovzdaní a prevzatí časti diela. Zhotoviteľ je oprávnený vystaviť faktúru na základe protokolu o odovzdaní a prevzatí časti diela podpísaného obidvomi Zmluvnými stranami.

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

6.7 Faktúra musí obsahovať všetky náležitosti podľa zákona o DPH, označenie čísla Zmluvy podľa evidencie Objednávateľa a číslo bankového účtu v tvare IBAN a kód štatistickej klasifikácie produktov podľa činnosti (CPA). Súčasťou faktúry je originál protokolu o odovzdaní a prevzatí časti diela podpísaný obidvoma Zmluvnými stranami.

6.8 V prípade, že faktúra nebude obsahovať náležitosti uvedené v bode 6.7 tejto Zmluvy, Objednávateľ je oprávnený vrátiť ju Zhotoviteľovi na doplnenie. V takom prípade sa preruší plynutie lehoty splatnosti a nová lehota splatnosti začne plynúť doručením opravenej faktúry Objednávateľovi.

6.9 Lehota splatnosti faktúr je **30 dní** od ich doručenia Objednávateľovi.

6.10 Objednávateľ podpisom tejto Zmluvy udeľuje Zhotoviteľovi súhlas v zmysle ustanovenia § 71 ods. 1 písm. b) zákona o DPH, aby vystavoval a spracúval faktúry v elektronickej forme, za podmienky predchádzajúceho informovania Objednávateľa o používaní elektronického spôsobu fakturácie v zmysle bodu 6.11 Zmluvy.

6.11 Do 10 dní od nadobudnutia účinnosti tejto Zmluvy, je Zhotoviteľ povinný písomne oznámiť Objednávateľovi, či bude pri fakturácii podľa tohto zmluvného vzťahu používať elektronickú formu alebo listinnú (tlačenú) formu faktúr. Písomné oznámenie Zhotoviteľa o spôsobe 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.

6.12 Ak si Zhotoviteľ nesplní riadne a včas svoju povinnosť podľa bodu 6.11 tejto Zmluvy, za záväzný spôsob fakturácie sa považuje listinná (tlačená) forma.

6.13 Zhotoviteľ 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 Zhotoviteľovi.

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

VII. PODMIENKY VYKONANIA DIELA

Povinnosti Zmluvných strán

7.1 Zhotoviteľ vykoná dielo na svoje náklady a vlastné nebezpečenstvo.

7.2 Vlastnícke právo k zhotovenému dielu prechádza na Objednávateľa protokolárnym odovzdaním a prevzatím celého diela osobám Objednávateľa oprávnenými rokovať vo veciach technických. Týmto okamihom prechádza na Objednávateľa aj nebezpečenstvo škody na diele.

7.3 Zhotoviteľ sa zaväzuje po vypracovaní Míľnika č. 1 pripraviť prezentáciu výsledkov a záverov vykonaného diela a odprezentovať ju objednávateľovi na oponentskom konaní v zmysle bodu 7.4 tejto Zmluvy.

7.4 Pri plnení Míľnika č. 1 Objednávateľ je povinný zvolať najneskôr do 20 pracovných dní po doručení časti diela oponentské konanie. Z oponentského konania bude vyhotovený písomný protokol. V prípade, že na základe oprávnených pripomienok Objednávateľa na oponentskom konaní bude nevyhnutné dopracovať alebo prepracovať predložené časti diela, Zhotoviteľ je povinný doručiť takto dopracované alebo prepracované časti diela Objednávateľovi v súlade s bodom 7.9.3 tejto Zmluvy.

7.5 Zhotoviteľ je povinný v priebehu riešenia konzultovať s objednávateľom svoje zásadné metodické postupy riešenia častí diela a tieto prispôsobiť požiadavkám objednávateľa.

7.6 Zhotoviteľ je povinný akceptovať pripomienky objednávateľa uplatnené počas realizácie diela a v plnom rozsahu ich dodatočne zapracovať do odovzdaného výsledného riešenia. Pripomienky objednávateľa sa môžu týkať aj úprav metodiky použitej zhotoviteľom. ***Ak to bude potrebné podľa stanoviska objednávateľa uplatneného počas oponentského konania***, zhotoviteľ bude povinný v dohodnutom termíne prepracovať časti diela v rozsahu metodiky upravenej podľa pripomienok objednávateľa. V tomto prípade objednávateľ rozhodne, či bude potrebné zopakovať oponentské konanie.

7.7 Podmienkou odovzdania a prevzatia diela je preukázanie jeho funkčnosti vykonaním skúšok funkcionality jednotlivých častí a preukázanie funkčnosti celého diela.

7.8 Objednávateľ potvrdí prevzatie časti diela, resp. celého diela písomne, protokolom o odovzdaní a prevzatí časti diela, resp. záverečným protokolom o odovzdaní a prevzatí diela, podpísaným osobami Objednávateľa oprávnenými rokovať vo veciach technických. Časť diela bude Zhotoviteľom odovzdaná a Objednávateľom prevzatá aj v prípade, že v zápise o odovzdaní a prevzatí časti diela budú uvedené nedorobky, ktoré samy o sebe, ani v spojení s inými nebránia plynulej a bezpečnej prevádzke (užívaniu). Tieto zjavné nedorobky musia byť uvedené v protokole o odovzdaní a prevzatí časti diela so stanovením termínu ich odstránenia. Objednávateľ je oprávnený až do odstránenia uvedených vád a nedorobkov zadržať 10% z ceny časti diela. Uvedená suma bude Zhotoviteľovi uhradená do 15 dní od písomného potvrdenia Objednávateľa, že vady a nedorobky boli odstránené.

7.9 Zhotoviteľ sa zaväzuje:

7.9.1 V priebehu realizácie diela podľa potreby zvolať pracovné stretnutie (minimálne raz mesačne) k riešeniu predmetu diela a vypracovať zápisnicu, ktorá bude odsúhlasená osobami oprávnených rokovať vo veciach technických.

7.9.2 V prípade vzniku odpadov nakladať s nimi v súlade so zákonom č. 79/2015 Z. z. o odpadoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Zhotoviteľ počas realizácie predmetu zmluvy zabezpečí uloženie vzniknutého odpadu na vyhradené miesto, ktoré určí Objednávateľ. Zhodnotenie, resp. zneškodnenie odpadu zabezpečí Objednávateľ na vlastné náklady.

7.9.3 Odovzdať spolu s dielom dokumentáciu, definovanú v Prílohe č. 1, Prílohe č. 2 a Prílohe č. 8 tejto Zmluvy 2x v papierovej forme a 1x v elektronickej forme.

7.9.4 Odovzdať spolu s dielom dokumenty, informácie a ostatné podklady týkajúce sa diela na pamäťovom médiu dohodnutého typu v rozsahu:

7.9.4.1 Prevádzková dokumentácia (Inštalačná príručka, Administrátorská príručka, Disaster and Recovery plán, Popis procesu zálohovania).

7.9.4.2 Užívateľská dokumentácia (Používateľská príručka).

7.9.4.3 Odovzdanie licencií.

7.9.5 Po ukončení diela odovzdať Objednávateľovi všetky dokumenty či už vo forme písomnej, výkresovej alebo elektronickej s vyhlásením, že nedošlo počas tvorby projektovej a inej dokumentácie k zneužitiu, strate alebo odcudzeniu informácií a dokumentov.

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

7.11 Zhotoviteľ je povinný vykonať dielo v zmysle tejto Zmluvy, ako aj v súlade so súťažnými podkladmi pre vyhotovenie tohto diela.

7.12 Zhotoviteľ sa zaväzuje, že si bude riadne a včas plniť svoje zmluvné záväzky voči svojim subdodávateľom, ktorých poveril realizáciou časti diela v súlade s touto Zmluvou. Porušenie záväzku podľa predchádzajúcej vety zakladá nárok Objednávateľa na uplatnenie zmluvnej pokuty.

7.13 Zhotoviteľ 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.

7.14 Zhotoviteľ 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 7.13, a to kedykoľvek od podpisu tejto zmluvy a počas trvania zmluvného vzťahu.

7.15 S poukazom na skutočnosť, že v rámci diela môže dochádzať k spracúvaniu osobných údajov dotknutých osôb, zhotoviteľ je povinný zhotoviť dielo tak, aby bolo plne v súlade s požiadavkami na ochranu osobných údajov, ktoré ukladajú nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje Smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (spolu ďalej len „**Legislatíva o ochrane osobných údajov**") v znení ich prípadných neskorších zmien. Zhotoviteľ je povinný zhotoviť dielo tak, aby najmä avšak nielen obsahovalo účinné bezpečnostné, technické, resp. iné ďalšie opatrenia s cieľom zaistiť čo možno najvyššiu úroveň bezpečnosti a ochrany osobných údajov vyžadovanú Legislatívou o ochrane osobných údajov.

Spolupôsobenie Zmluvných strán

7.16 Vzniknuté rozpory v priebehu plnenia tejto Zmluvy, ktoré sa nepodarí vyriešiť na priebežných konzultáciách, sa budú riešiť na pracovných stretnutiach za účasti osôb konajúcich v mene Zmluvných strán.

7.17 Pracovné stretnutia v zmysle bodu 7.9.1 bude organizovať a zabezpečovať Zhotoviteľ za účasti zástupcov Zmluvných strán oprávnených rokovať vo veciach zmluvných a technických a nimi poverených pracovníkov.

7.18 Osoba Objednávateľa oprávnená rokovať vo veciach technických je povinná poskytnúť na požiadanie Zhotoviteľa odbornú konzultáciu v nevyhnutnom rozsahu a poskytnúť technickú dokumentáciu skutočného stavu ako podklad pre vypracovanie projektovej dokumentácie.

7.19 Každá činnosť súvisiaca s realizáciou predmetného diela, ktorá by mala za následok výpadok ktorejkoľvek časti siete alebo systémov SEPS, bude vopred komunikovaná a odsúhlasovaná odbornými útvarmi objednávateľa.

7.20 Objednávateľ poskytne Zhotoviteľovi nevyhnutnú súčinnosť. Rozsah a podmienky súčinnosti budú písomne dohodnuté na pracovných stretnutiach zmluvných strán.

VIII. BEZPEČNOSŤ PRI PRÁCI A OCHRANA PRED POŽIARMI

8.1 Zhotoviteľ 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. 6 tejto Zmluvy.

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

IX. ZÁRUČNÁ DOBA - ZODPOVEDNOSŤ ZA VADY

9.1 Zhotoviteľ zodpovedá za to, že dielo je zhotovené podľa podmienok tejto Zmluvy a v súlade s platnými všeobecne záväznými právnymi predpismi a príslušnými technickými normami a že funkčné a technické vlastnosti diela zodpovedajú vlastnostiam dohodnutým v tejto Zmluve.

9.2 Zhotoviteľ poskytne na dielo záruku po dobu 24 mesiacov. Záruka začne plynúť odo dňa písomného prevzatia diela záverečným protokolom o odovzdaní a prevzatí diela podpísaným osobami Objednávateľa oprávnenými rokovať vo veciach technických alebo povereným zástupcom.

9.3 Dielo má vady, ak nemá vlastnosti požadované touto Zmluvou.

9.4 Počas záručnej doby má Objednávateľ právo požadovať a Zhotoviteľ povinnosť bezplatne odstrániť vady.

9.5 Objednávateľ sa zaväzuje, že prípadnú reklamáciu vady diela uplatní bezodkladne po jej zistení písomnou formou.

9.6 Zhotoviteľ sa zaväzuje počas záručnej doby začať s odstraňovaním prípadných vád diela hneď nasledujúci pracovný deň od uplatnenia reklamácie. Termín odstránenia konkrétnej vady diela sa dohodne elektronickou formou. V prípade, že Zmluvné strany nedosiahnu dohodu do 3 dní v zmysle predchádzajúcej vety, je Objednávateľ oprávnený stanoviť primeraný termín na odstránenie vád.

9.7 Ak Zhotoviteľ po takomto oznámení neodstráni vadu počas určenej doby, môže Objednávateľ zabezpečiť vlastnými silami alebo u iného dodávateľa odstránenie tejto vady, pričom všetky náklady s tým spojené, vrátane sprievodných nákladov, má povinnosť uhradiť Zhotoviteľ.

9.8 Pokiaľ dôjde k sporu, či ide o vadu alebo nie, Objednávateľ má právo dať uvedenú skutočnosť posúdiť u nezávislého posudzovateľa. Pokiaľ sa preukáže odborným posudkom, že reklamácia vady diela bola oprávnená, tak Objednávateľ má právo voči Zhotoviteľovi na bezplatné odstránenie vady a úhradu nákladov za vykonaný odborný posudok.

9.9 Zhotoviteľ zodpovedá za vady, ktoré má dielo v čase jeho odovzdania Objednávateľovi. Za vady vzniknuté po odovzdaní zodpovedá Zhotoviteľ iba vtedy, ak boli spôsobené porušením jeho povinnosti.

X. ÚROKY Z OMEŠKANIA, ZMLUVNÉ POKUTY, NÁHRADA ŠKODY

10.1 V prípade, že Zhotoviteľ bude v omeškaní s dokončením a odovzdaním časti diela, pokiaľ toto omeškanie nie je zapríčinené vinou Objednávateľa, je Objednávateľ oprávnený uplatniť si u Zhotoviteľa zmluvnú pokutu vo výške 0,1 % z ceny časti diela za každý deň omeškania, maximálne však v celkovej výške 10 % z ceny diela.

10.2 Ak Zhotoviteľ nezačne s odstraňovaním prípadných vád diela počas záručnej doby v lehote podľa bodu 9.6 tejto Zmluvy, je Objednávateľ oprávnený uplatniť si u Zhotoviteľa zmluvnú pokutu vo výške 0,1 % z celkovej zmluvnej ceny za každý kalendárny deň omeškania, maximálne však v celkovej výške 10 % z ceny diela.

10.3 Ak Zhotoviteľ neodstráni prípadné vady diela počas záručnej doby v lehote podľa bodu 9.6 tejto Zmluvy, je Objednávateľ oprávnený uplatniť si u Zhotoviteľa zmluvnú pokutu vo výške 0,1 % z celkovej zmluvnej ceny za každý kalendárny deň omeškania, maximálne však v celkovej výške 20 % z ceny diela.

10.4 Za každé jednotlivé porušenie povinnosti podľa bodu 15.6 tejto Zmluvy je Zhotoviteľ povinný zaplatiť zmluvnú pokutu vo výške 1 500,- EUR (slovom tisícpäťsto eur).

10.5 Za každé jednotlivé porušenie povinnosti podľa článku VIII. tejto Zmluvy je Zhotoviteľ povinný zaplatiť zmluvnú pokutu vo výške uvedenej v Prílohe č. 6 tejto Zmluvy.

10.6 Za každé jednotlivé porušenie povinností v zmysle čl. XII. tejto Zmluvy a v zmysle Prílohy č. 10 je Zhotoviteľ povinný zaplatiť zmluvnú pokutu uvedenú v Prílohe č. 10 bod 15.

10.7 Za každé jednotlivé porušenie povinností v zmysle čl. XIII. tejto Zmluvy je Zhotoviteľ povinný zaplatiť zmluvnú pokutu vo výške 5 000,- EUR (slovom päťtisíc eur).

10.8 Za porušenie povinnosti Zhotoviteľa podľa bodu 7.12 tejto Zmluvy je Objednávateľ oprávnený uplatniť si u Zhotoviteľa zmluvnú pokutu vo výške 5 000 EUR (slovom päťtisíc eur).

10.9 Za porušenie povinnosti zhotoviteľa podľa bodu 7.9.2 tejto Zmluvy je zhotoviteľ povinný nahradiť objednávateľovi škodu, ktorá objednávateľovi vznikla a to v celom rozsahu. Povinnosť náhrady škody za porušenie povinnosti zhotoviteľa podľa bodu 7.9.2 tejto Zmluvy sa vzťahuje na prípadné sankcie pre objednávateľa zo strany príslušných orgánov štátnej správy.

10.10 Nárok na zmluvnú pokutu podľa tohto článku Zmluvy je Objednávateľ povinný uplatniť si u Zhotoviteľa písomnou formou. Uplatnením zmluvnej pokuty nezaniká Objednávateľovi právo na náhradu škody spôsobenej Zhotoviteľom porušením zmluvných povinností v celom rozsahu.

XI. OKOLNOSTI VYLUČUJÚCE ZODPOVEDNOSŤ

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

11.2 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.

11.3 Ak bude plnenie diela zastavené v dôsledku okolností vylučujúcich zodpovednosť, je Zhotoviteľ povinný bezodkladne vykonať opatrenia na zabezpečenie diela, aby sa minimalizovali riziká zničenia alebo poškodenia diela, odcudzenia časti diela alebo iné škody.

11.4 Rozsah a spôsob vykonania opatrení na zabezpečenie diela podľa bodu 11.3 a úhradu nákladov na realizáciu týchto opatrení dohodnú Zmluvné strany pred vykonaním prác na základe návrhu, ktorý predloží Zhotoviteľ.

11.5 Ak je výsledkom okolností vylučujúcich zodpovednosť havarijný stav, vykoná Zhotoviteľ opatrenia na zabezpečenie diela bezodkladne. Ocenenie realizácie týchto opatrení dohodnú Zmluvné strany následne.

XII. OCHRANA DÔVERNÝCH INFORMÁCIÍ

12.1 V tejto Zmluve "dôverné informácie" znamenajú informácie, ktoré sa týkajú alebo môžu týkať diela, 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.

12.2 Ďalšie práva a povinnosti Zmluvných strán vo vzťahu k zabezpečeniu primeranej úrovne dôvernosti, dostupnosti a integrity informácií definuje Príloha č. 6 až Príloha č. 10 tejto Zmluvy.

XIII. AUTORSKÉ PRÁVA

13.1 Autorské práva sa riadia zákonom č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov (ďalej len „**Autorský zákon**").

13.2 Zhotoviteľ prehlasuje, že Predmet plnenia neporušuje autorské práva tretích osôb.

13.3 Zhotoviteľ vyhlasuje, že je oprávnený vykonávať majetkové práva k softvéru dodanému objednávateľovi na základe tejto Zmluvy a iného druhu plnenia, ktoré by bolo autorským dielom podľa § 2 Autorského zákona v súlade s Autorským zákonom.

13.4 Zmluvné strany si sú vedomé, že Softvér dodaný podľa tejto Zmluvy sa môže riadiť licenčnými ustanoveniami výrobcu Zariadenia alebo licenčnými podmienkami tretích strán, ktoré budú obsahovať časové, miestne alebo vecné obmedzenia. Zhotoviteľ sa zaväzuje zabezpečiť, aby licenčné podmienky takéhoto Softvéru umožnili použitie počítačového programu v počtoch a rozsahu, ktorý zabezpečí plné a neobmedzené využívanie Hardvéru v súlade s účelom a technickou špecifikáciou podľa tejto Zmluvy, a to po celú dobu životnosti Hardvéru.

13.5 Zhotoviteľ poskytuje objednávateľovi na základe tejto Zmluvy licenciu v rovnakom rozsahu aj vo vzťahu k tzv. **upgradu** („vylepšeniu" resp. technickému zhodnoteniu dodaného Softvéru) a tzv. **updatu** (aktualizácie) dodaného Softvéru, ktoré slúžia na zabezpečenie funkcionalít

Hardvéru, a to vrátane licencie k technickej a užívateľskej dokumentácii nevyhnutne potrebnej k ďalšiemu užívaniu prevádzkovaného Softvéru.

XIV. UKONČENIE ZMLUVY

14.1 Zmluvu je možné ukončiť dohodou Zmluvných strán alebo odstúpením od tejto Zmluvy.

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

14.2.1 nesplnenie povinností podľa bodu 7.11 tejto Zmluvy a to ani v dodatočnej lehote na odstránenie nedostatkov stanovenej Objednávateľom v predchádzajúcej písomnej výzve,

14.2.2 nedodržanie termínu vyhotovenia diela podľa bodu 4.1 tejto Zmluvy o viac ako 30 kalendárnych dní,

14.2.3 porušenie vyhlásenia a povinnosti zhotoviteľa podľa bodu 7.13 a 7.14 tejto Zmluvy,

14.2.4 ak Zhotoviteľ preukázateľne poruší povinnosť zachovávania mlčanlivosti alebo iných povinností vyplývajúcich mu z čl. XII (Ochrana dôverných informácií) a Prílohy č. 10 tejto Zmluvy,

14.2.5 ak Zhotoviteľ preukázateľne poruší povinnosť zachovávania mlčanlivosti alebo iných povinností vyplývajúcich mu z čl. XII a Prílohy č. 10 tejto Zmluvy.

14.3 Podstatné porušenie tejto Zmluvy alebo jej opakované porušenia, ktoré nie sú podstatné, predstavujú závažné porušenie zmluvných a 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.

14.4 Nepodstatným porušením tejto Zmluvy sa rozumie nedodržanie ostatných zmluvných podmienok tejto Zmluvy okrem podmienok uvedených v bode 14.2. Na nepodstatné porušenie tejto Zmluvy Objednávateľ Zhotoviteľa písomne upozorní. Po opakovanom porušení tej istej zmluvnej povinnosti je Objednávateľ oprávnený od tejto Zmluvy odstúpiť.

14.5 Odstúpenie od tejto Zmluvy je účinné dňom doručenia písomného oznámenia o odstúpení od tejto Zmluvy druhej Zmluvnej strane. Odstúpením sa zrušuje táto Zmluva ex nunc a Zhotoviteľ je povinný zastaviť všetky práce na zhotovovanom diele do troch dní od oznámenia tejto skutočnosti Objednávateľom a je oprávnený na základe zápisu o rozpracovanosti diela (potvrdenom oboma Zmluvnými stranami) vzniknuté náklady fakturovať. Vzniknuté preukázané a Objednávateľom uznané náklady Objednávateľ uhradí do 30 dní.

XV. ZÁVEREČNÉ USTANOVENIA

15.1 Zmluva nadobúda platnosť dňom podpísania obidvomi Zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia tejto Zmluvy v súlade s ust. § 47a ods. 1 zákona č.40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.

15.2 Nakoľko spoločnosť Slovenská elektrizačná prenosová sústava, a. s., je povinnou osobou v zmysle zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám v platnom znení (ďalej len „zákon o slobodnom prístupe k informáciám"), Zmluvné strany sú oboznámené s tým, že Zmluva a daňové doklady súvisiace so Zmluvou budú zverejnené takým spôsobom, ktorý pre povinne zverejňované zmluvy, objednávky a faktúry ukladá zákon o slobodnom prístupe k informáciám vo svojom ust. § 5a a § 5b.

15.3 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.

15.4 Zmluvu je možné meniť alebo dopĺňať len písomnou dohodou Zmluvných strán vo forme dodatkov k tejto Zmluve.

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

15.6 Zoznam subdodávateľov podľa Prílohy č. 5 tejto Zmluvy je možné meniť len na základe vzájomnej dohody oboch Zmluvných strán formou dodatku k tejto Zmluve, ktorého obsahom bude nový zoznam subdodávateľov. Navrhovaný subdodávateľ musí spĺňať § 32 ods. 1. a 2. a nesmú existovať dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7 a ods. 8 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení zákonov v znení neskorších predpisov. Objednávateľ si vyhradzuje právo písomne požiadať zhotoviteľa o nahradenie subdodávateľa, ktorý má sídlo v treťom štáte, s ktorým nemá Slovenská republika alebo Európska únia uzavretú medzinárodnú zmluvu zaručujúcu rovnaký a účinný prístup k verejnému obstarávaniu v tomto treťom štáte pre hospodárske subjekty so sídlom v Slovenskej republike. Objednávateľ požiada zhotoviteľa o nahradenie subdodávateľa vždy, ak má subdodávateľ sídlo v treťom štáte, alebo ak ide o zákazku, o ktorých to ustanoví vláda nariadením (§ 41 ods. 2 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov).

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

15.8 Ak by niektoré z ustanovení tejto Zmluvy bolo, alebo sa stalo neúčinným, neplatným, nezákonným alebo nevykonateľným (ďalej aj ako "vada pôvodného ustanovenia"), nebude tým dotknutá, ani obmedzená platnosť, účinnosť a vykonateľnosť ostatných ustanovení tejto Zmluvy. Zmluvné strany sa zaväzujú, že takto dotknuté ustanovenia 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.

15.9 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.

15.10 Zhotoviteľ 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.

15.11 Neoddeliteľnou súčasťou tejto Zmluvy je:

15.11.1 Príloha č. 1 - Špecifikácia predmetu plnenia

15.11.2 Príloha č. 2 - Technická špecifikácia predmetu plnenia

15.11.3 Príloha č. 3 - Tabuľky technických špecifikácií

15.11.4 Príloha č. 4 - Kalkulácia ceny diela

15.11.5 Príloha č. 5 - Zoznam subdodávateľov

15.11.6 Príloha č. 6 - Všeobecné zmluvné podmienky zabezpečovania BOZP a OPP

15.11.7 Príloha č. 7 - Bezpečnostné opatrenia na informačnú a kybernetickú bezpečnosť pre Dodávateľov/Zhotoviteľov SEPS

15.11.8 Príloha č. 8 - Vymedzenie rozsahu a spôsobu plnenia bezpečnostných opatrení (požadovaných vyhláškou č. 362/2018 Z. z.).

15.11.9 Príloha č. 9 - Záväzné požiadavky na zabezpečenie vzdialeného prístupu k prostriedkom a technológiám ICT, Slovenskej elektrizačnej prenosovej sústavy, a.s.

15.11.10 Príloha č. 10 - Všeobecné podmienky zachovania mlčanlivosti

Slovenská elektrizačná
a.s.

V Bratislave dňa

Za Objednávateľa:

.....

Ing. Martin Magát
predseda predstavenstva

.....

Ing. Miloš Bikár, PhD.
podpredseda predstavenstva

V ..... dňa ..

Za Zhotoviteľa:

.....

Ing. Marián Skákala
výkonný riaditeľ a konateľ spoločnosti

Zvýšenie zabezpečenia DWDM - MPLS bezpečnostný monitoring - špecifikácia:

1. **Predmetom plnenia je dodávka, konfigurácia, inštalácia zariadení pre zvýšenie zabezpečenia DWDM - MPLS bezpečnostný monitoring:**

1.1. Návrhu technickej architektúry riešenia (HLD/LLD dizajn) v zmysle požiadaviek uvedených v Prílohe č. 2 „Technická špecifikácia predmetu diela" a v Prílohe č. 3 „Tabuľky technických špecifikácií".

1.2. Dodávky potrebného HW a SW vrátane podpory výrobcu na obdobie 2 rokov (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 1.1.) a všetkých potrebných hardvérových a softvérových licencií pre dodávané riešenie.

1.3. Konfigurácia zariadení, inštalácia zariadení, inštalácie všetkých dodaných komponentov a potrebného inštalačného materiálu (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 1.1.).

1.4. Inštalácia a konfigurácia SW (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 1.1.).

1.5. Realizácia testovacích scenárov a Disaster recovery plán (v zmysle odsúhlaseného návrhu technickej architektúry riešenia v zmysle bodu 1.1.).

1.6. Dokumentácie skutočného vyhotovenia, prevádzková dokumentácia.

1.7. Príručky administrátora, tabuľky elektrických a tepelných výkonov.

1.8. Oboznámenie obsluhy a administrátorov.

Zoznam subdodávateľov

Príloha č. 5

	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.											

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:

   Funkcia:

   a technika požiarnej ochrany zhotoviteľa

   Meno a priezvisko:

   Číslo osvedčenia:

   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 pracovisku objednávateľa dodržiavať všetky zmluvné podmienky a predpisy bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi pri prácach, ktoré bude v zmysle zmluvy a počas doby jej plnenia vykonávať. Na skutočnosti odporujúce predpisom bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi je povinný písomne upozorniť zodpovedného zástupcu objednávateľa.
18. Povinnosťou zhotoviteľa je preukázateľne upozorniť objednávateľa na riziká, vyplývajúce z činnosti 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. **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.
23. 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.

Bezpečnostné opatrenia na informačnú a kybernetickú bezpečnosť pre Dodávateľov/Zhotoviteľov 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/Zhotoviteľom.

Všeobecné ustanovenia

1. Dodávateľ/Zhotoviteľ 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/Zhotoviteľ zaväzuje prijať a dodržiavať po celý čas trvania zmluvného vzťahu založeného Zmluvou je vymedzený v časti 2. tejto Prílohy.
2. Konkrétny rozsah činností Dodávateľa/Zhotoviteľa vyplýva zo Zmluvy a jej príloh.
3. Dodávateľ/Zhotoviteľ 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/Zhotoviteľ povinný sa bezodkladne oboznámiť a dôsledne ju dodržiavať.
4. Dodávateľ/Zhotoviteľ 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 v zmluvnom vzťahu zabezpečuje v samostatnej prílohe uzatváranej zmluvy. V prípade objednávky alebo iných predzmluvných vzťahov sa podpisuje osobitný dokument „Dohoda o mlčanlivosti".
5. Dodávateľ/Zhotoviteľ 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/Zhotoviteľ 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/Zhotoviteľovi vykonať u Dodávateľa/Zhotoviteľa audit za

účelom preverenia účinnosti Dodávateľom/Zhotoviteľom 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/Zhotoviteľ 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/Zhotoviteľ je povinný zabezpečiť prítomnosť svojich zamestnancov a iných osôb poverených plnením povinností v oblasti kybernetickej bezpečnosti.

c. Spoločnosť SEPS predloží Dodávateľovi/Zhotoviteľovi záverečnú správu o výsledkoch auditu spolu s opatreniami na nápravu zistených nedostatkov a s lehotami na ich odstránenie. V prípade, ak Dodávateľ/Zhotoviteľ 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/Zhotoviteľa 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/Zhotoviteľ nie je oprávnený zapojiť ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie predmetu Zmluvy bez písomného súhlasu spoločnosti SEPS;

b. Ak Dodávateľ/Zhotoviteľ 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/Zhotoviteľa 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/Zhotoviteľa za riadne plnenie predmetu Zmluvy, ako ani zodpovednosť za plnenie povinností v oblasti kybernetickej bezpečnosti.

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

a. Dodávateľ/Zhotoviteľ 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/Zhotoviteľ povinný adresovať kontaktným osobám spoločnosti SEPS uvedeným v časti 3. tejto Prílohy.

b. Dodávateľ/Zhotoviteľ 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/Zhotoviteľom s cieľom napraviť porušenie kybernetickej bezpečnosti a podľa potreby, opatrení na zmiernenie potenciálnych nepriaznivých dôsledkov kybernetického bezpečnostného incidentu vrátane preventívnych opatrení.

Oznámenie je Dodávateľ/Zhotoviteľ povinný adresovať kontaktným osobám spoločnosti SEPS uvedeným v časti 3. tejto Prílohy.

d. Ak do okamihu oznámenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, Dodávateľ/Zhotoviteľ je povinný odoslať spoločnosti SEPS neúplné oznámenie, v ktorom túto skutočnosť uvedie; neúplné oznámenie je Dodávateľ/Zhotoviteľ 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/Zhotoviteľ je povinný v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní.

g. Dodávateľ/Zhotoviteľ sa zaväzuje zdokumentovať každý kybernetický bezpečnostný incident, jeho hrozbu, následky a opatrenia prijaté na jeho nápravu. Dokumentáciu o kybernetickom bezpečnostnom incidente je Dodávateľ/Zhotoviteľ 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/Zhotoviteľ 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/Zhotoviteľa 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/Zhotoviteľa na úseku kybernetickej bezpečnosti. Náhradou podľa predchádzajúcej vety nie je dotknuté právo spoločnosti SEPS na náhradu celej škody spôsobenej porušením povinnosti Dodávateľa/Zhotoviteľa, 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/Zhotoviteľ 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/Zhotoviteľa zachovávať mlčanlivosť.

12. Po ukončení zmluvného vzťahu založeného Zmluvou je Dodávateľ/Zhotoviteľ 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/Zhotoviteľ 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/Zhotoviteľ 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/Zhotoviteľ povinný zaviesť a implementovať.

4. Dodávateľ/Zhotoviteľ 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/Zhotoviteľom a je poverený rokovať s Dodávateľom/Zhotoviteľom o zmluvných podmienkach. Koordinuje aj osoby oprávnené rokovať o veciach technických. Je zodpovedný za celý životný cyklus zmluvy s Dodávateľom/Zhotoviteľom – 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/Zhotoviteľom 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/Zhotoviteľa bezpečnostný audit v rozsahu definovanom medzinárodným štandardom ISO 27001. MKB musí úzko spolupracovať s Manažérom bezpečnosti Dodávateľa/Zhotoviteľa 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/Zhotoviteľov.

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/Zhotoviteľa: Manažér Dodávateľa/Zhotoviteľa je osoba Dodávateľa/Zhotoviteľa definovaná v zmluve ako osoba oprávnená rokovať vo veciach technických, v anglických pomenovaniach je rola známa ako „Delivery manager". Zodpovednosťou manažéra Dodávateľa/Zhotoviteľa 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/Zhotoviteľa: Manažér bezpečnosti Dodávateľa/Zhotoviteľa zodpovedá za dodržiavanie bezpečnostných pravidiel a politík objednávateľa. Manažér bezpečnosti Dodávateľa/Zhotoviteľa spolupracuje pri bezpečnostných auditoch vykonaných MKB alebo ním povereným externým subjektom u Dodávateľa/Zhotoviteľa a je zodpovedný za implementáciu primeraných organizačných, technických alebo personálnych opatrení za účelom zníženia rizík identifikovaných bezpečnostným auditom. Manažér bezpečnosti Dodávateľa/Zhotoviteľa je ďalej zodpovedný za priebežnú aktualizáciu a riadenie rizík súvisiacich s dodávanými prácami, službami alebo tovarmi s potenciálnym dopadom na objednávateľa. Manažéra bezpečnosti Dodávateľa/Zhotoviteľa určí manažér Dodávateľa/Zhotoviteľa. V prípade, že Dodávateľ/Zhotoviteľ nemá vytvorenú funkciu manažéra bezpečnosti Dodávateľa/Zhotoviteľa, túto rolu/funkciu prevezme manažér Dodávateľa/Zhotoviteľa sám.

1 Všeobecné bezpečnostné požiadavky a pravidlá pre Dodávateľov/Zhotoviteľov

1.1 Preskúmanie procesov informačnej a kybernetickej bezpečnosti u Dodávateľa/Zhotoviteľa

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

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

1.1.3 Dodávateľ/Zhotoviteľ 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/Zhotoviteľ 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/Zhotoviteľovi 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/Zhotoviteľ 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/Zhotoviteľ mal uzavretú so SEPS dohodu o mlčanlivosti;

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 informácií za SEPS.

1.2.5.8 Údaje a dokumenty SEPS používané Dodávateľom/Zhotoviteľom 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/Zhotoviteľa. Manažér Dodávateľa/Zhotoviteľa 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/Zhotoviteľ 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/Zhotoviteľ 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/Zhotoviteľské 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/Zhotoviteľ 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/Zhotoviteľa, ktorý zabezpečuje dodávku tovarov, prác alebo služieb pre objednávateľa na kritických systémoch, aplikáciách, resp. má prístup k citlivým informáciám.

1.3.2 Manažér Dodávateľa/Zhotoviteľa 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/Zhotoviteľa, ktorí sa podieľajú na plnení predmetu zmluvy. Manažér Dodávateľa/Zhotoviteľa 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/Zhotoviteľa 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/Zhotoviteľa informuje o existencii a kvalite kontinuity plánov Dodávateľa/Zhotoviteľa 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/Zhotoviteľa musí udržiavať a aktualizovať plán odozvy na bezpečnostné incidenty.

1.5.2.2 Manažér bezpečnosti Dodávateľa/Zhotoviteľa musí SEPS MKB bezodkladne informovať o bezpečnostných incidentoch, ktoré Dodávateľ/Zhotoviteľ 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/Zhotoviteľa 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/Zhotoviteľa 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/Zhotoviteľa, 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/Zhotoviteľ 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/Zhotoviteľ povinný zdokumentovať v bezpečnostnej dokumentácii vypracovanej v súlade so Zákonom o kybernetickej bezpečnosti a Vyhláškou NBÚ; bezpečnostnú dokumentáciu je Dodávateľ/Zhotoviteľ 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/Zhotoviteľa s prístupom k informáciám a údajom spoločnosti SEPS a doručovanie informácií druhej strane

Meno a priezvisko	Pracovná rola / pozícia	E-mail	Tel. číslo
Martin Vozár	Systémový špecialista		
Matej Pilko	Systémový špecialista		
Ľubomír Macík	Projektový manažér		
Filip Gajdy	Systémový špecialista		
Pavol Šipoš	Systémový špecialista		

Kontaktné osoby a doručovanie

1. Spoločnosť SEPS určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom/Zhotoviteľom na v oblasti informačnej a kybernetickej bezpečnosti:

   Meno, priezvisko: Funkcia: ved. odboru infor. a kyber. bezpečnosti

   Telefónne číslo: Email: frantisek.varinsky@sepsas.sk

2. Dodávateľ/Zhotoviteľ 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.

Príloha č. 7

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).

SEPS Slovenská elektrizačná prenosová sústava

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
	§ 4	(2) Klasifikácia informácií a kategorizácia sietí a informačných systémov reflektuje požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií, siete a informačného systému, a to najmä vo fáze a) špecifikácie, ako definície požiadaviek a potrieb vedúcich k rozhodnutiu o vzniku informačného systému alebo akéhokoľvek spracúvania informácií, b) návrhu procesu, systému alebo dátovej štruktúry, c) vývoja systému alebo spôsobu spracúvania informácií, d) implementácie systému ako inštalácie, nasadenia, zavedenia alebo oživenia systému, alebo začatia procesu spracúvania informácií, e) prevádzky procesu ako štandardného využívania a údržby systému a údržby informácií, f) zmeny existujúceho, bežiaceho systému alebo spracúvania informácií, rozvoja a inovácie spracúvania podľa aktuálnych potrieb prevádzkovateľa základnej služby, g) nahradenia systému alebo procesu spracúvania informácií novým systémom alebo procesom	*Dodané riešenie musí zohľadniť požiadavky Vyhlášky 362/2018 Z.z. na narábanie s chránenými a prísne chránenými informáciami. Klasifikáciu informácii dodá SEPS.*	
a)	§ 5 písm. a)	Na organizáciu kybernetickej bezpečnosti sa uplatňuje najmä zásada: najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na plnenie pridelených úloh,	*Aplikačné role musia zohľadniť princíp minimálnych pridelených oprávnení a princíp segregation of duties (SoD).*	*Zoznam rolí a oprávnení dodaného riešenia aj s ich popisom.*
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*
	§ 8 ods. 4 písm a)	Pri riadení prístupov k sieťam a informačným systémom sa každému používateľovi siete a informačného systému prideľuje jednoznačný identifikátor na autentizáciu na vstup do siete a informačného systému,	*Dodané riešenie musí podporovať integráciu na identity a access manažment systém napr. prostredníctvom AD*	
	§ 8 ods. 4 písm b)	Pri riadení prístupov k sieťam a informačným systémom sa zabezpečuje riadenie jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,	*Dodané riešenie nesmie používať zdieľané kontá*	
d)	§ 8 ods. 4 písm c)	Pri riadení prístupov k sieťam a informačným systémom 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,	*Dodané riešenie musí podporovať integráciu na identity a access manažment systém napr. prostredníctvom AD*	
e)	§ 9 ods.2 písm a)	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).*	
f)	§ 10 písm. b)	Riadenie bezpečnosti prevádzky sietí a informačných systémov sa zaisťuje prostredníctvom určených pravidiel, zodpovedností 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.*	
f)	§ 10 písm. c)	Riadenie bezpečnosti prevádzky sietí a informačných systémov sa zaisťuje prostredníctvom určených pravidiel, zodpovedností 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)*	

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
f)	§ 10 písm. d)	Riadenie bezpečnosti prevádzky sietí a informačných systémov sa zaisťuje prostredníctvom určených pravidiel, zodpovedností 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)*	
f)	§ 10 písm. e)	Riadenie bezpečnosti prevádzky sietí a informačných systémov sa zaisťuje prostredníctvom určených pravidiel, zodpovedností a postupov na zaznamenávanie 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 bezpečnostných záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...*	
f)	§ 10 písm. f)	Riadenie bezpečnosti prevádzky sietí a informačných systémov sa zaisťuje prostredníctvom určených pravidiel, zodpovedností a postupov na zaznamenávanie a vyhodnocovanie prevádzkových 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 záznamov do centrálneho systému pre zber a vyhodnocovanie udalostí. Musia podporovať protokoly SYSLOG, SNMP v3, ...*	
g)	§ 11 ods.1 písm. a)	Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom a) nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,	*Dodávateľ je povinný poskytnúť informácie o nástroji (ak taký existuje) na detekciu zraniteľností dodávaného riešenia (aplikácie alebo jej časti) a poskytnúť max. súčinnosť pri jej odstránení (hot fix, workaround, patch, update/upgrade).*	
g)	§ 11 ods.1 písm. b)	Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom b) nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,	*Dodávateľ je povinný bezodkladne informovať o akejkoľvek známej bezpečnostnej zraniteľnosti dodaného riešenia (podpornej infraštruktúry) a poskytnúť max. súčinnosť pri jej odstránení (hot fix, workaround, patch, update/upgrade).*	
g)	§ 11 ods.1 písm. c)	Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom c) využitia verejných zoznamov 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.*	
g)	§ 11 odsek 2	Cieľom procesu riadenia záplat a aktualizácií je zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií a plošnú aplikáciu aktualizácií na zariadenia, pre ktoré je softvérová aktualizácia či záplata vydaná.	*Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na aplikáciu záplat a aktualizácií.*	
g)	§ 11 odsek 3	Úlohami procesu riadenia záplat a aktualizácií sú najmä a) identifikácia potrieb softvérových záplat a aktualizácií, b) evidencia softvérových záplat a aktualizácií a informácia o ich nasadení alebo o dôvodoch ich nenasadenia, c) rozhodnutie o vhodnom prístupe k otestovaniu softvérových záplat a aktualizácií, d) zabezpečenie implementácie softvérových záplat a aktualizácií, e) aktualizácia plánu softvérových záplat a aktualizácií.	*Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy na aplikáciu záplat a aktualizácií.*	
g)	§ 11 odsek 4	Neschválené aktualizácie nie sú prípustné.	*Dodávateľ sa podieľa na procese schvaľovania záplat na dodané riešenie a dáva odporúčania na ich implementáciu. Neschválené záplaty v prípade, že ich nasadzuje dodávateľ nie sú prípustné.*	

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
h)	§ 12 ods. 1 písm a)	Požiadavkami na ochranu proti škodlivému kódu sú najmä určenie zodpovednosti používateľov za prevenciu pred škodlivým kódom,	*Súčasťou dodávky riešenia Sietí a IS musia byť pravidlá a postupy pre používateľov na ochranu pred škodlivým kódom.*	
	§ 12 ods. 1 písm b)	Požiadavkami na ochranu proti škodlivému kódu sú najmä určenie pravidiel pre inštaláciu a používanie systémov prevencie škodlivého kódu,	*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.*	
	§ 12 ods. 1 písm c)	Požiadavkami na ochranu proti škodlivému kódu sú najmä monitorovanie potenciálnych ciest prieniku škodlivého kódu do prostredia sietí a informačných systémov.	*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.*	
h)	§ 12 ods. 2 písm. a)	Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že v reálnom čase vykonávajú kontrolu prístupu k digitálnemu obsahu vrátane sieťovej prevádzky, sťahovania, spúšťania alebo otvárania súborov, priečinkov na vymeniteľnom alebo vzdialenom úložisku a prístupu k webovým sídlam a cloudovým službám.	*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 v zmysle požiadavky § 12 ods. 2 písm. a).*	
h)	§ 12 ods. 2 písm. b)	Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že spúšťajú pravidelné kontroly úložísk vrátane cloudových a pripojených vymeniteľných úložísk, najmenej raz ročne,	*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 v zmysle, ktoré musia byť nakonfigurované v zmysle požiadavky § 12 ods. 2 písm. b).*	
h)	§ 12 ods. 2 písm. c)	Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že neoprávneným používateľom je zabránené v prístupe k obsahu prostredníctvom funkcie filtrovania obsahu,	*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 v zmysle, ktoré musia byť nakonfigurované v zmysle požiadavky § 12 ods. 2 písm. c).*	
h)	§ 12 ods. 2 písm. d)	Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že používateľom je zamedzené v pokusoch odinštalovať alebo zakázať funkcie systému na ochranu proti škodlivému kódu.	*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 v zmysle, ktoré musia byť nakonfigurované v zmysle požiadavky § 12 ods. 2 písm. d).*	
i)	§ 13 ods. 1 písm. a)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami, a to najmä využitím nástrojov na ochranu integrity sietí, ktoré sú zabezpečené segmentáciou sietí, informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len informačné systémy s rovnakými bezpečnostnými požiadavkami, rovnakej kategórie a s podobným účelom,	*Dodávateľ pri návrhu riešenia zohľadní 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.*
	§ 13 ods. 1 písm. b)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä tým, že spojenia medzi segmentmi siete, ktoré sú chránené firewallom 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.*	

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
	§ 13 ods. 1 písm. c)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä prostredníctvom bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup, napríklad s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,	*Ak je požadovaný vzdialený prístup, realizovať ho striktne prostredníctvom infraštruktúry ICT SEPS s použitím dvojfaktorovej autentizácie. V zmluve/objednávke je nevyhnutné ošetriť podmienky pre vzdialený prístup.*	
	§ 13 ods. 1 písm. d)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä tým, že v sieťach sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete,	*Súčasťou dodávky riešenia musí byť aj návrh topológie, aby bolo zabezpečené, že každý segment = zóna = časť (PLC, operatorske stanice, HMI, servery, servisné stenice) 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.*	
	§ 13 ods. 1 písm. e)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä tým, že spojenia do externých sietí sú smerované cez sieťový firewall,	*Prepoje do externých sietí musia byť riadené firewallom.*	
	§ 13 ods. 1 písm. f)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,	*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.*	
	§ 13 ods. 1 písm. g)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä udržiavaním zoznamu 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.*	
	§ 13 ods. 1 písm. h)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou	*Prepoje do externých sietí musia byť riadené firewallom s aktivovaným systémom IDS/IPS.*	
	§ 13 ods. 1 písm. i)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä prostredníctvom blokovania neoprávnených spojení zo zdrojov identifikovaných ako škodlivé alebo spôsobujúce hrozby, ak to nastavenie informačného systému umožňuje,	*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.*	
	§ 13 ods. 1 písm. j)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä 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.*	
	§ 13 ods. 1 písm. k)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,	*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.*	

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
	§ 13 ods. 1 písm. l)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä v závislosti od prostredia 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.*	
	§ 13 ods. 1 písm. m)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä 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 gatewa[illegible].*	
	§ 13 ods. 1 písm. n)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä 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.*	
	§ 13 ods. 1 písm. o)	Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä vykonávaním pravidelného alebo nepretržitého posudzovania technických zraniteľností, a posudzovania technických zraniteľností 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, žiadame popísať spôsob zabezpečenie jeho ochrany a posúdenie súladu s požiadavkami legislatívy. Pred nadviazaním vzdialeného pripojenia do siete SEPS 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.*	
j)	§ 14 ods. 1 písm. c)	Požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami, ktorých zamýšľané a odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k sieťam a informačným systémom sa určujú najmä zavedením pravidiel a postupov c) na zabezpečenie kontroly nad verziami softvéru a zabudovaného softvéru,	*Dodávané riešenie musí spĺňať podmienku dodania najvyššej stabilnej verzie softvéru pri zohľadnení väzieb na už prevádzkované informačné systémy SEPS.*	
j)	§ 14 ods. 1 písm. d)	Požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami, ktorých zamýšľané a odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k sieťam a informačným systémom sa určujú najmä zavedením pravidiel a postupov d) pre riadenie konfigurácií, ktoré predchádzajú neschváleným a nezdokumentovaným zmenám konfigurácií, s cieľom udržovania sietí a informačných systémov v požadovanom, konzistentnom a očakávanom stave ich funkcií	*Dodávané riešenie musí obsahovať zdokumentované konfiguračné parametre všetkých dodávaných komponentov.*	*Prevádzková dokumentácia Sietí a IS musí obsahovať konfiguračné parametre všetkých komponentov.*

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
j)	§ 14 ods. 1 písm. e)	Požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami, ktorých zamýšľané a odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k sieťam a informačným systémom sa určujú najmä zavedením pravidiel a postupov e) pre vykonávanie údržby sietí a informačných systémov, ktoré zaručia vymedzenie zodpovedností a pracovných postupov, ktorých cieľom je minimalizácia hrozieb vyplývajúcich z neúmyselných chýb alebo úmyselnej manipulácie pri údržbe sietí a informačných systémov.	*Ak súčasťou dodávky je aj výkon údržby Sietí a IS musia byť zmluvne vymedzené kompetencie a zodpovednosti dodávateľa a popísané pracovné postrupy údržby.*	*Prevádzková dokumentácia Sietí a IS musí obsahovať pracovné postupy údržby.*
j)	§ 14 ods. 2 písm. b)	Požiadavky na metodiku softvérového vývoja sú určené s cieľom najmä b) zaručiť, že sa použijú najnovšie a najbezpečnejšie verzie nástrojov a komponentov na vývoj softvéru,	*Dodávané riešenie musí spĺňať podmienku na použitie najnovšej a najbezpečnejšie stabilnej verzie nástrojov a komponentov na vývoj softvéru.*	*Dodávateľ predloží zoznam nástrojov a komponentov na vývoj softvéru.*
j)	§ 14 ods. 2 písm. c)	Požiadavky na metodiku softvérového vývoja sú určené s cieľom najmä c) zaručiť, že sa použijú len softvérové knižnice a komponenty, ktoré pochádzajú od dôveryhodných dodávateľov a sú aktívne podporované,	*Dodávané riešenie musí spĺňať podmienku, že sa použijú len softvérové knižnice a komponenty, ktoré pochádzajú od dôveryhodných dodávateľov a sú aktívne podporované.*	*Dodávateľ predloží zoznam softvérových knižníc a komponentov na vývoj softvéru.*
	§ 14 ods. 2 písm. e)	Požiadavky na metodiku softvérového vývoja sú určené s cieľom najmä e) zaručiť, že je udržovaný register softvérových komponentov,	*Dodávané riešenie musí obsahovať register softvérových komponentov.*	*Register softvérových komponentov*
	§ 14 ods. 2 písm. f)	Požiadavky na metodiku softvérového vývoja sú určené s cieľom najmä f) zaručiť validáciu postupov tak, že softvérový modul neakceptuje nesprávny a neočakávaný vstup,	*Dodávané riešenie musí byť zabezpečené tak, aby softvérový modul neakceptoval nesprávny a neočakávaný vstup.*	
	§ 14 ods. 2 písm. g)	Požiadavky na metodiku softvérového vývoja sú určené s cieľom najmä g) zaručiť, že vo vyvíjanom softvéri je nakonfigurovaný proces logovania, ktorý umožňuje včas zachytiť systémové a bezpečnostné udalosti, s cieľom identifikovať, analyzovať a riešiť neobvyklé udalosti a podozrivé správanie v rámci sietí a informačných systémov.	*Dodávané riešenie musí mať implementovaný proces logovania, ktorý umožňuje včas zachytiť systémové a bezpečnostné udalosti, s cieľom identifikovať, analyzovať a riešiť neobvyklé udalosti a podozrivé správanie v rámci sietí a informačných systémov.*	
k)	§ 15 ods. 1	Zaznamenávanie udalostí a monitorovanie sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho 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.*

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
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 poverným ich analýzou.	*Prevádzkové záznamy sú zabezpečené najmenej tak, že sú čitateľné výlučne osobám poverením 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.*	

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
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, samostatné 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. (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, musí dodržiavať postupy a predpisy SEPS.*	
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").	*V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS), musí zabezpečiť prevádzku Siete a IS v monitorovanom zabezpečenom priestore s riadeným vstupom a v uzamykateľných rackoch s vyvedením signalizácie do centrálneho monitorovacieho systému. V prípade prevádzkovania riešenia v rámci infraštruktúry SEPS, musí dodržiavať postupy a predpisy SEPS.*	
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.	*V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS), musí zabezpečiť prevádzku Siete a IS v monitorovanom zabezpečenom priestore s riadeným vstupom a v uzamykateľných rackoch s vyvedením signalizácie do centrálneho monitorovacieho systému. V prípade prevádzkovania riešenia v rámci infraštruktúry SEPS, musí dodržiavať postupy a predpisy SEPS.*	
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, musí dodržiavať postupy a predpisy SEPS.*	
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 ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS) 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 ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS) musí zabezpečiť 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.*	

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
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*
	§ 17 ods. 1 písm. b)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmä z monitorovania a analyzovania udalostí v sieťach a informačných systémoch,	*Dodávateľ poskytne zoznam kľúčových ukazovateľov, ktoré sú kritické z pohľadu analýzy vzniknutých kybernetických incidentov.*	
	§ 17 ods. 1 písm. c)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmä z detekcie kybernetických bezpečnostných incidentov,	*Dodávateľ poskytne indikátory bezpečnostných incidentov pre dané riešenie.*	
	§ 17 ods. 1 písm. d)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmä zo zberu relevantných informácií o kybernetických bezpečnostných incidentoch,	*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.)*	
	§ 17 ods. 1 písm. e)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmä z vyhodnocovania kybernetických bezpečnostných incidentov,	*Dodávateľ poskytne indikátory bezpečnostných incidentov pre dané riešenie a odporúčaný spôsob ich vyhodnotenia.*	
	§ 17 ods. 1 písm. f)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmä z riešenia zistených kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov	*Dodávateľ poskytne odporúčaný postup reakcie na kybernetické bezpečnostné incidenty.*	
	§ 17 ods. 1 písm. g)	Riešenie kybernetických bezpečnostných incidentov pozostáva najmä z vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatia opatrení alebo zavedenia nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov.	*n/a*	
m)	§ 17 ods. 2 písm. c)	Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmä 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*
m)	§ 17 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.*	

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
m)	§ 17 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.*	
m)	§ 17 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 súvislacich s kybernetickým 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.*	
m)	§ 17 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.*	
m)	§ 17 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.*	
m)	§ 17a ods. 1	Dôvernosť, integrita 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 určujú pravidlá kryptografickej ochrany údajov a) pri ich prenose v rámci sietí a informačných systémov a b) pri ich 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, ...).*	

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
m)	§ 17a ods. 2	Systém správy kryptografických kľúčov a certifikátov je zabezpečený počas celého životného cyklu kryptografických kľúčov a certifikátov. Správa kryptografických kľúčov a certifikátov zahŕňa najmä 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 a c) umožnenie kontroly a auditu systému správy kryptografických kľúčov a certifikátov.	*Správa kľúčov je zabezpečená v súlade s politikami správy kryptografických identifikátorov SEPS.*	
m)	§ 17b ods. 3 písm a-f)	Postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmä a) frekvenciu a rozsah jej dokumentovania a schvaľovania, b) určenie osoby zodpovednej za zálohovanie, c) časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní, d) požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom, e) požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa „chránené" a „prísne chránené", f) požiadavku na vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.	*Pre dodávané riešenie dodávateľ vypracúva postupy zálohovania a plány obnovy údajov zo záloh. Rozsah a frekvenciu zálohovania odporúča dodávateľ riešenia Sietí a IS. V prípade ak dodávateľ prevádzkuje riešenie off-site(mimo infraštruktúry SEPS) je nutné zabezpečiť šifrovanie záloh a pravidelné preverovanie vykonaných záloh.*	*Plány zálohovania a havarijnej obnovy.*

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 15. 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 15. a 16. 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.