ZMLUVA O POSKYTOVANÍ VEREJNE DOSTUPNÝCH SLUŽIEB

uzatvorená v súlade s ust. § 84 Z. č. 452/2001 Z.z. o elektronických komunikáciách v znení neskorších predpisov a v zmysle zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov
(ďalej len **„Zmluva“**)

Článok I
Zmluvné strany

Obchodné meno:	Fakultná nemocnica s poliklinikou Nové Zámky
Právna forma:	štátna príspevková organizácia
Sídlo:	Slovenská 5587/11A, 940 34 Nové Zámky
v mene ktorého podpisujú:	JUDr. Mgr. Mikuláš Blaško - riaditeľ
IČO:	17336112
DIČ:	2021068324
IČ DPH:	SK2021068324
bankové spojenie:	Štátna pokladnica
medzinárodný kód banky (BIC):	SPSRSKBA
číslo účtu v tvare IBAN :	SK88 8180 0000 0070 0054 0295
zapísaný v:	register organizácií vedený Štatistickým úradom Slovenskej republiky a živnostenský register Okresného úradu Nové Zámky pod č. 404-9729

(ďalej len **„Verejný obstarávateľ“**)

a

obchodné meno:	Slovanet, a.s.
právna forma :	akciová spoločnosť
sídlo/miesto podnikania :	Galvaniho 19, 821 04 Bratislava
v mene ktorého podpisuje/ú :	Ing. Peter Máčaj, predseda predstavenstva Ing. Peter Tomášek, člen predstavenstva
e-mail :	vo@slovanet.net
IČO :	35 954 612
DIČ :	2022059094
IČ DPH:	SK2022059094
bankové spojenie :	Tatra banka, a.s.
číslo účtu v tvare IBAN :	SK44 1100 0000 0026 2519 1125
zapísaný v :	Obchodný register Mestského súdu Bratislava III, Oddiel: sa, vložka č. 3692/B

(ďalej len **„Poskytovateľ“**)

(ďalej aj ako **„Zmluvné strany“**)

Článok II
Predmet Zmluvy

1.1 Predmetom zákazky je zriadenie primárneho a záložného bezpečného pripojenia na adrese verejného obstarávateľa – Fakultná nemocnica s poliklinikou Nové Zámky, Slovenská ulica 5587/11 A, 940 34 Nové Zámky 1 (ďalej len „Verejný obstarávateľ“ alebo „FNsP NZ“) vrátane poskytovania súvisiacich služieb na obdobie 24 mesiacov.

1.2 Poskytovateľ sa zaväzuje poskytovať Verejnému obstarávateľovi elektronickú komunikačnú službu alebo elektronické komunikačné služby podľa Špecifikácie Služby, ktorá tvorí neoddeliteľnú súčasť tejto Zmluvy ako príloha č. 1. Verejný obstarávateľ sa zaväzuje platiť za poskytovanie Služby dojednanú cenu Poskytovateľovi.

1.3 Poskytovanie jednotlivej Služby za dojednanú cenu podľa príslušnej Špecifikácie Služby uvedenej v prílohe tejto Zmluvy predstavuje samostatný a oddeliteľný predmet tejto Zmluvy. Pokiaľ je poskytovaných Služieb viac, každá Služba predstavuje čiastočný, samostatný a oddeliteľný predmet tejto Zmluvy.

Článok II
Cena Služby, platobné podmienky a fakturácia

2.1 Zmluvné strany sa dohodli na odmene nasledovne: Za Služby podľa tejto Zmluvy, prináleží Poskytovateľovi odmena podľa cenníka jednotlivých úkonov Poskytovateľa, ktorý tvorí ako príloha č. 1 k Zmluve jej neoddeliteľnú súčasť.

2.2 Prípadné nevyužívanie Služby poskytovanej Verejnému obstarávateľovi na základe tejto Zmluvy nemá vplyv na povinnosť Verejnému obstarávateľovi uhrádzať Cenu Služby podľa tejto Zmluvy.

2.3 Zmluvné strany sa dohodli, že za poskytnutie služieb Poskytovateľ vystaví Verejnému obstarávateľovi faktúru spolu s prílohami jedenkrát mesačne, najneskôr do 5 pracovných (piatich) dní odo dňa skončenia kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola poskytnutá služba podľa tejto Zmluvy. Lehota splatnosti faktúry je 60 dní odo dňa jej doručenia Verejnému obstarávateľovi. Faktúra musí byť vystavená v súlade s platnými právnymi predpismi, musí obsahovať všetky náležitosti účtovného a daňového dokladu.

2.4 Poskytovateľ sa zaväzuje odoslať faktúru Verejnému obstarávateľovi v deň jej vystavenia, inak splatnosť faktúry začína plynúť dňom jej doručenia. Poskytovateľ bude zasielať Verejnému obstarávateľovi elektronickú faktúru formou elektronickej pošty na jeho e-mailovú adresu: faktury@nspnz.sk.

Článok III.
Práva a povinnosti Zmluvných strán

3.1 Poskytovateľ je oprávnený poveriť vykonaním niektorých činností podľa tejto Zmluvy inú odborne spôsobilú osobu, s tým, že to vopred oznámi verejnému obstarávateľovi.

3.2 Verejný obstarávateľ je povinný umožniť Poskytovateľovi včasný a riadny prístup na miesto poskytovania Služby a poskytnúť mu všetku potrebnú súčinnosť pri plnení tejto Zmluvy. Počas doby omeškania Verejného obstarávateľa s poskytnutím súčinnosti alebo splnením svojich povinností nie je Poskytovateľ v omeškaní so splnením povinností podľa tejto Zmluvy.

3.3 Ak Verejný obstarávateľ neuhradí cenu služby ani do 30 dní odo dňa splatnosti ceny služby, Poskytovateľ je oprávnený prerušiť poskytovanie Služby, a to až do úplného zaplatenia ceny služby. Prerušením poskytovania služieb nie je dotknuté právo Poskytovateľa požadovať zaplatenie ceny služby.

3.4 Ak niektorá Zmluvná strana poruší právnu povinnosť a spôsobí tým druhej strane škodu, je povinná ju nahradiť. Zmluvné strany sa dohodli, že si budú nahrádzať len skutočnú (priamu) škodu, nie ušlý zisk.

3.5 Poskytovateľ zodpovedá za škodu vzniknutú porušením povinnosti Poskytovateľa poskytovať službu v rozsahu a kvalite podľa tejto Zmluvy len v prípade, ak porušenie povinnosti zavinil, pričom jeho povinnosť na náhradu škody je obmedzená na povinnosť vrátiť Verejnému obstarávateľovi pomernú časť ceny služby za čas neposkytovania služby v rozsahu a kvalite podľa tejto Zmluvy, pre tento prípad sa neuplatní druhá veta bodu 3.4 Zmluvy.

3.6 Poskytovateľ nezodpovedá za neposkytovanie služby v rozsahu a kvalite podľa tejto Zmluvy alebo za prípadnú škodu tým spôsobenú, ak k nemu dôjde z dôvodov vylučujúcich zodpovednosť podľa § 374 Obchodného zákonníka, alebo preto, že Verejný obstarávateľ zasiahol do zariadenia Poskytovateľa prenechaného Verejnému obstarávateľovi do dočasného užívania na účely poskytovania služby alebo umožnil takýto zásah tretej osobe.

3.7 Zmluvné strany sa zaväzujú, že zachovajú mlčanlivosť o skutočnostiach, o ktorých sa dozvedia pri plnení tejto Zmluvy.

3.8 Poskytovateľ je oprávnený jednostranne započítavať proti všetkým splatným pohľadávkam Verejného obstarávateľa na základe tejto Zmluvy všetky svoje pohľadávky voči Verejnému obstarávateľovi vzniknuté v súvislosti s touto Zmluvou.

3.9 Špecifikácia Služby môže určiť obsah a rozsah spracúvania osobných údajov. Zmluvné strany si pre účely plnenia tejto zmluvy poskytujú osobné údaje zástupcov zmluvných strán, vrátane štatutárnych zástupcov a zamestnancov (ak je aplikovateľné) (ďalej len „dotknuté osoby“). Zbierané a spracovávané osobné údaje sú profesijné (pracovné údaje) a ide najmä o meno, priezvisko, osobné číslo, funkciu, e-mail, telefónne číslo, poštová adresa, a to v súlade s § 78 ods. 3 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Na účely tejto zmluvy v rámci spracovania osobných údajov vystupujú Poskytovateľ a Verejný obstarávateľ ako samostatní prevádzkovatelia v zmysle platných právnych predpisov v oblasti ochrany osobných údajov. Zmluvné strany sú povinné plniť povinnosti prevádzkovateľa, ktoré vyplývajú z platných právnych predpisov oblasti ochrany osobných údajov. Ak pri plnení tejto zmluvy zmluvná strana poskytne druhej zmluvnej strane osobné údaje dotknutých osôb, zmluvná strana, ktorá obdržala osobné údaje sa zaväzuje chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania, pričom na tento účel prijme primerané technické, organizačné a personálne opatrenia.

Zmluvné strany sú oprávnené spracúvať informácie obsahujúce osobné údaje dotknutých osôb len na účel, na ktorý boli údaje podľa tejto zmluvy poskytnuté a len počas doby nevyhnutnej na naplnenie tohto účelu. Zmluvné strany si sú vedomé, že osobné údaje nemôžu byť spracúvané na žiadny iný účel ako je účel ich poskytnutia v súlade s touto zmluvou. Zmluvné strany sa ďalej zaväzujú neposkytovať osobné údaje dotknutých osôb nad rozsah a obsah, ktorý je nevyhnutný na dosiahnutie riadneho a efektívneho plnenia tejto zmluvy. Zmluvná strana môže spracúvať poskytnuté osobné údaje dotknutých osôb druhej zmluvnej strany prostredníctvom tretej osoby len na základe predchádzajúceho písomného súhlasu tejto druhej zmluvnej strany, a to s výnimkou spracúvania informácií prostredníctvom právnych zástupcov a daňových alebo účtovných poradcov zmluvných strán. Zásady spracúvania osobných údajov Poskytovateľom sú zverejnené https://www.slovanet.net/privacy-policy/ v sekcii Ochrana osobných údajov. Účastník súhlasí, aby osobné údaje zamestnanca boli použité pre marketingové účely po dobu 3 rokov odo dňa ukončenia poslednej zo Služieb poskytovaných na základe tejto Zmluvy. Súhlas podľa predchádzajúcej vety môže Verejný obstarávateľ kedykoľvek odvolať alebo zmeniť.

3.10 Zmluvné strany sú povinné navzájom sa bez zbytočného odkladu informovať o všetkých prekážkach, ktoré im bránia v riadnom plnení predmetu Zmluvy.

3.11 Poskytovateľ je povinný súčasne s podpisom zmluvy podpísať a plniť povinnosti vyplývajúce z Prílohy č. 2 – Dodatok o bezpečnostných opatreniach a notifikačných povinnostiach

Článok IV
Sankcie

4.1 Za nedodržanie lehoty splatnosti faktúry je Poskytovateľ oprávnený požadovať úrok z omeškania v zmysle ustanovení Obchodného zákonníka

Článok V
Trvanie Zmluvy a jej ukončenie

5.1 Zmluva sa uzatvára na dobu určitú, 24 mesiacov odo dňa účinnosti Zmluvy.

5.2 Ak Poskytovateľ poskytuje Verejnému obstarávateľovi na základe tejto Zmluvy niekoľko Služieb, ukončenie poskytovania niektorej zo Služieb má povahu čiastočného ukončenia tejto Zmluvy len v rozsahu ukončovanej Služby.

5.3 Poskytovanie jednotlivých Služieb možno ukončiť:
a. dohodou Zmluvných strán
b. výpoveďou poskytovania Služby podľa bodu 5.5 Zmluvy
c. odstúpením od Zmluvy podľa bodu 5.7 Zmluvy

d. odstúpením od poskytovania Služby podľa bodu 5.6 alebo bodu 5.8 Zmluvy

5.4 Dojednanie Doby viazanosti Služby v Špecifikácii Služby predstavuje dojednanie Zmluvných strán o poskytovaní takej Služby na dobu určitú. Zmluvné strany sa dohodli, že počas doby viazanosti Zmluvné strany nie sú oprávnené vypovedať poskytovanie Služby.

5.5 V prípade, že sa Zmluvné strany v Špecifikácii dohodli na poskytovaní Služby bez určenia minimálnej doby poskytovania Služby, sú Zmluvné strany oprávnené vypovedať túto Službu kedykoľvek počas poskytovania Služby. Výpovedná doba je jeden kalendárny mesiac a začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď poskytovania Služby doručená druhej Zmluvnej strane.

5.6 Verejný obstarávateľ môže odstúpiť od poskytovania Služby, ak:

a) mu Poskytovateľ oznámi podstatnú zmenu zmluvných podmienok poskytovania Služby najmenej jeden mesiac vopred a Verejný obstarávateľ túto zmenu neakceptuje; v tomto prípade môže Verejný obstarávateľ odstúpiť od poskytovania Služby najneskôr do jedného mesiaca od oznámenia podstatnej zmeny,
b) mu Poskytovateľ neoznámil podstatnú zmenu zmluvných podmienok poskytovania Služby najmenej jeden mesiac vopred; v tomto prípade môže Verejný obstarávateľ od poskytovania Služby odstúpiť do jedného mesiaca odkedy sa o zmene dozvedel,
c) Poskytovateľ ani po opakovanej uznanej reklamácii neposkytuje Službu podľa Zmluvy alebo ju neposkytuje v stanovenej kvalite; v tomto prípade môže Verejný obstarávateľ od poskytovania Služby odstúpiť do jedného mesiaca odo dňa doručenia oznámenia o uznaní opätovnej reklamácie a ak porušenie povinnosti stále pretrváva,
d) Poskytovateľ neoznámi výsledok prešetrenia reklamácie v lehotách uvedených v Reklamačnom poriadku; v tomto prípade môže Verejný obstarávateľ od poskytovania Služby odstúpiť do jedného mesiaca odo dňa uplynutia lehoty na oznámenie výsledku vybavenia reklamácie.

5.7 Poskytovateľ môže odstúpiť od Zmluvy:
a) ak Verejný obstarávateľ opakovane neoprávnene zasiahne do zariadenia verejnej siete alebo takýto zásah umožní tretej osobe, hoci aj z nedbanlivosti,
b) ak Verejný obstarávateľ nezaplatí Cenu Služby ani do 45 dní odo dňa jej splatnosti,
c) ak Verejný obstarávateľ pripojí na verejnú sieť zariadenie, ktoré nespĺňa požiadavky príslušných právnych predpisov, alebo používa takéto zariadenie v rozpore so schválenými podmienkami a ani na výzvu Poskytovateľa ho neodpojí,
d) ak Verejný obstarávateľ opakovane použije poskytovanú Službu spôsobom, ktorý znemožňuje Poskytovateľovi kontrolu jej používania,
e) ak Verejný obstarávateľ opakovane poruší podmienky tejto Zmluvy,
f) ak Verejný obstarávateľ uviedol v Zmluve údaje, ktoré sa dodatočne ukážu ako nepravdivé,
g) ak nemôže Službu poskytovať v dohodnutom rozsahu alebo kvalite z dôvodov technickej neuskutočniteľnosti poskytovania Služby,
h) z dôvodu modernizácie verejnej služby, s ktorou je spojené ukončenie poskytovania Služby; v tomto prípade je povinný spolu s oznámením o odstúpení od Zmluvy doručiť Verejnému obstarávateľovi ponuku na poskytovanie inej, technicky a cenovo blízkej verejnej služby s jej zvýhodneným zriadením,
i) ak je Verejný obstarávateľ insolventný, najmä ak Účastník vstúpil do likvidácie, alebo na jeho majetok bol vyhlásený konkurz, alebo bola súdom povolená reštrukturalizácia alebo bol zamietnutý konkurz pre nedostatok majetku alebo bola uvalená nútená správa alebo nariadená daňová alebo iná exekúcia.

5.8 V prípade, že sa dôvod odstúpenia podľa bodu 5.7 Zmluvy týka iba niektorej z poskytovaných Služieb, je Poskytovateľ tiež oprávnený odstúpiť len od poskytovania tej Služby, ktorá je priamo dotknutá dôvodom odstúpenia alebo ktorej poskytovanie nie je možné technicky oddeliť od Služby, ktorej sa dôvod odstúpenia priamo dotýka.

5.9 Ukončením niektorej Služby podľa bodu V. Zmluvy nie je dotknuté poskytovanie ostatných Služieb na základe tejto Zmluvy. Pre vylúčenie pochybnosti Zmluvné strany výslovne uvádzajú, že ukončenie poskytovania jednotlivej Služby má za následok iba čiastočné ukončenie tejto Zmluvy, len v rozsahu ukončovanej Služby.

5.10 Ukončením všetkých poskytovaných Služieb dochádza k ukončeniu celej Zmluvy.

Článok VI
Kybernetická bezpečnosť

6.1 Poskytovateľ sa zaväzuje podpísať a plniť Prílohu č. 2– Dodatok o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Podpis sa vykoná v rovnaký deň, ako deň podpisu tejto Zmluvy. Účinnosť dodatku je v rovnaký deň, ako deň účinnosti tejto Zmluvy.

6.2 Poskytovateľ sa zaväzuje prístupy do informačných systémov neposkytnúť tretím stranám vrátane subdodávateľov s výlukou tých, ktorých schváli manažér kybernetickej bezpečnosti, štatutárny orgán alebo vedúci odboru informatiky.

6.3 Poskytovateľ sa zaväzuje uviesť zoznam všetkých pracovníkov, ktorí budú mať prístup do informačného systému objednávateľa, priamo verejnému obstarávateľovi na e-mailovú adresu: hana.cvikova@nspnz.sk spoločne s ich telefónnym číslom alebo e-mailovou adresou do 10 kalendárnych dní od účinnosti tejto Zmluvy.
Poskytovateľ sa zaväzuje, že túto povinnosť vykonajú aj subdodávatelia do 10 kalendárnych dní od účinnosti tejto Zmluvy. V prípade uzatvorenia pracovného pomeru alebo dohody o pracovnej činnosti s novým pracovníkom alebo ukončenia pracovného pomeru alebo ukončenia dohody o pracovnej činnosti pracovníka u poskytovateľa alebo jeho subdodávateľov zaznamená a zašle do 30 dní na e-mailovú adresu: hana.cvikova@nspnz.sk

6.4 Prístup do informačných systémov nie je povolený pracovníkom poskytovateľa alebo jeho subdodávateľov, ktorí nemajú uzatvorenú s poskytovateľom pracovný pomer alebo dohodu o pracovnej činnosti.

6.5 Poskytovateľ a jeho subdodávatelia sa zaväzujú, že ich všetky technické zariadenia, ktorými budú pristupovať do informačného systému verejného obstarávateľa, sú raz mesačne skenované na zraniteľnosti a zistené zraniteľnosti sú v primeranom rozsahu a čase vyriešené. Verejný obstarávateľ má právo na vykonanie auditu na vlastné náklady u poskytovateľa v prípade potreby, minimálne ale túto skutočnosť musí ohlásiť písomne 10 pracovných dní pred návrhom verejným obstarávateľom.

6.6 Poskytovateľ a jeho subdodávatelia sa zaväzujú, že spĺňajú požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a Vyhlášku Národného bezpečnostného úradu č. 362/2018 Z. z. pre kategóriu 3 podľa „Príloha č. 2 k vyhláške č. 362/2018 Z. z.“ v časti KLASIFIKAČNÁ SCHÉMA časť B. Kritéria kategorizácie sietí a informačných systémov a zároveň od 01.01.2025 aj smernicu Európskeho parlamentu a rady so všeobecným názvom „smernica NIS 2“ alebo „DIRECTIVE NIS 2“ pod číslom 2022/2555 uvedenú v úradnom vestníku Európskej únie.

Článok VII
Odstraňovanie porúch a plánované prerušenie prevádzky

7.1 Poskytovateľ zodpovedá za to, že služby budú poskytované v súlade s ustanoveniami tejto zmluvy, podľa všeobecne záväzných právnych predpisov a že budú spôsobilé k zmluvnému účelu.

7.2 V prípade poruchy, je poskytovateľ povinný bezplatne vykonať opravu do štyroch hodín od jej nahlásenia poverenou osobou verejného obstarávateľa. V prípade sporu sa za nahlásenie poruchy považuje čas zvukového záznamu z telefonického nahlásenie poruchy.

7.3 Poskytovateľ sa zaväzuje zabezpečiť nepretržitú prevádzku kontaktného pracoviska na nahlasovanie porúch, pričom verejný obstarávateľ je oprávnený kedykoľvek nahlasovať poruchy telefonicky alebo e- mailom.

7.4 Pokiaľ verejný obstarávateľ zistí poruchu na poskytnutých službách, je povinný túto skutočnosť bez zbytočného odkladu telefonicky a následne e-mailom oznámiť poskytovateľovi. Takéto oznámenie musí obsahovať označenie poruchy, miesto výskytu a popis, ako sa porucha prejavuje. Verejný obstarávateľ je povinný poskytnúť všetku potrebnú súčinnosť, najmä umožniť Poskytovateľovi prístup na miesto výskytu poruchy.

7.5 Nebezpečenstvo a všetky náklady súvisiace s výkonom prác uvedených v tomto článku znáša Poskytovateľ.

7.6 V prípade, ak poskytovateľ poruchu neodstráni do štyroch hodín od nahlásenia v súlade s touto zmluvou napriek tomu, že verejný obstarávateľ vytvoril podmienky na jej odstránenie, má Verejný obstarávateľ právo bez súhlasu Poskytovateľa :
a) odstrániť poruchu sám na náklady Poskytovateľa, alebo

b) poveriť odstránením poruchy tretiu osobu na náklady Poskytovateľa.

7.7 V cene služby nie sú zahrnuté plnenia súvisiace s poruchami, ak vznikli ako následok porušenia niektorej z povinností Verejného obstarávateľa tomuto vyplývajúcich z ustanovení zmluvy alebo všeobecne záväzných právnych predpisov, resp. ak takéto poruchy vzniknú ako dôsledok zásahu Verejného obstarávateľa do koncového zariadenia Poskytovateľa, ktoré sa nachádza v priestoroch Verejného obstarávateľa, ak tento zásah vykonal bez súhlasu Poskytovateľa. Poskytovateľ je však povinný aj takéto poruchy na žiadosť Verejného obstarávateľa odstrániť za cenu pre takýto prípad osobitne s ním dohodnutú, ktorá nebude vyššia ako cena na trhu obvyklá.

7.8 Poskytovateľ je povinný zaslať e-mailom verejnému obstarávateľovi oznámenie o plánovanom prerušení prevádzky služby najneskôr 5 pracovných dní pred uskutočnením daného prerušenia. Plánovaná údržba môže byť najviac 4 hodiny v mesiaci

Článok VIII
Záverečné ustanovenia

1. Zmluva nadobúda platnosť dňom podpísania oboma zmluvnými stranami. Zmluva nadobudne účinnosť dňom nasledujúcim po dni zverejnenia Zmluvy v Centrálnom registri zmlúv v zmysle ustanovenia § 47a ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov. Všetky práva a povinnosti vyplývajúce z tejto Zmluvy ako aj vzťahy v tejto Zmluve bližšie neupravené sa riadia príslušnými ustanoveniami Obchodného zákonníka a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky.

2. Meniť alebo doplňovať obsah tejto Zmluvy je možné len formou písomných dodatkov, ktoré budú datované, číslované a podpísané štatutárnymi zástupcami obidvoch zmluvných strán. Pre platnosť dodatkov k tejto Zmluve sa vyžaduje dohoda o celom obsahu. Len tak sa dodatok stáva súčasťou Zmluvy. Uzavretie dodatku musí byť v súlade so zákonom č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3. Zmluvné vzťahy výslovne neupravené touto Zmluvou sa spravujú ustanoveniami zák. č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov a Obchodného zákonníka.

4. Všetky spory vyplývajúce z tejto Zmluvy, alebo vzniknuté v súvislosti s ňou, budú Zmluvné strany riešiť predovšetkým vzájomnou dohodou.

5. Postúpenie pohľadávok Poskytovateľa podľa § 524 a nasl. Zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej len ,,Občiansky zákonník“) bez predchádzajúceho písomného súhlasu zriaďovateľa Verejného obstarávateľa (MZ SR) je zakázané. Právny úkon, ktorým budú postúpené pohľadávky Poskytovateľa v rozpore s dohodou Verejného obstarávateľa a Poskytovateľa podľa predchádzajúcej vety bude podľa § 39 Občianskeho zákonníka neplatné a porušenie zákazu podľa prvej vety je sankcionované zmluvnou pokutou vo výške 20 % z istiny pohľadávky postúpenej v rozpore so zákazom. Týmto nie je dotknutý nárok Verejného obstarávateľa na náhradu škody aj v rozsahu prevyšujúcom výšku dohodnutej zmluvnej pokuty a rovnako týmto nie je dotknutý nárok na inú zmluvnú pokutu podľa tejto Zmluvy.

6. Akceptácia ručiteľského vyhlásenia podľa § 303 a nasl. Zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov zo strany Poskytovateľa je bez predchádzajúceho súhlasu zriaďovateľa Verejného obstarávateľa (MZ SR) zakázaná. Právny úkon, ktorým Poskytovateľ akceptuje ručiteľské vyhlásenie tretej osoby, na základe ktorého sa tretia osoba stane veriteľom Verejného obstarávateľa v rozpore s dohodou Poskytovateľa a Verejného obstarávateľa podľa predchádzajúcej vety bude podľa § 39 Zákona č.40/1964 Zb. Občiansky zákonník v znení neskorších predpisov neplatné a porušenie zákazu podľa prvej vety je sankcionované zmluvnou pokutou vo výške 20 % z istiny pohľadávky postúpenej v rozpore so zákazom. Týmto nie je dotknutý nárok Verejného obstarávateľa na náhradu škody aj v rozsahu prevyšujúcom výšku dohodnutej zmluvnej pokuty a rovnako týmto nie je dotknutý nárok na inú zmluvnú pokutu podľa tejto Zmluvy.

7. Poskytovateľ sa zaväzuje, že pohľadávky vzniknuté z tejto Zmluvy nepoužije ako predmet zálohu. Poskytovateľ sa zaväzuje zdržať sa aj iných právnych úkonov, ktoré by mali za následok zmenu v osobe veriteľa peňažného záväzku voči Poskytovateľovi, a to pod sankciou neplatnosti takéhoto úkonu.

8. Účastníci berú na vedomie, že táto Zmluva podlieha zverejneniu podľa zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a s jej zverejnením týmto vyjadrujú súhlas.

9. Zmluvné strany sú povinné navzájom si oznámiť každú zmenu, ktorá by mohla ovplyvniť v Zmluve dohodnuté podmienky.

10. Táto Zmluva bola vyhotovená v troch rovnopisoch, z ktorých každá má platnosť originálu. Dve vyhotovenia tejto Zmluvy prevezme Verejný obstarávateľ a jedno vyhotovenie prevezme Poskytovateľ.

11. Obidve Zmluvné strany vyhlasujú, že si túto Zmluvu pred jej podpisom prečítali a že bola uzatvorená po vzájomnom oboznámení sa s jej obsahom ako určitý, vážny a zrozumiteľný prejav slobodnej vôle Zmluvných strán bez akéhokoľvek nátlaku a nie za nevýhodných podmienok pre ktorúkoľvek zo Zmluvných strán. Na dôkaz potvrdenia tejto skutočnosti pripájajú poverení zástupcovia oboch Zmluvných strán svoje vlastnoručné podpisy.

12. Neoddeliteľnou súčasťou tejto Zmluvy sú prílohy:
    Príloha č. 1 – Návrh na plnenia kritéria
    Príloha č. 2 – Dodatok o bezpečnostných opatreniach a notifikačných povinnostiach

Príloha:
Príloha č. 1 : Návrh na plnenia kritéria
Príloha č. 2: Dodatok o bezpečnostných opatreniach a notifikačných povinnostiach

V Bratislave, dňa: 03.03.2025

V Nových Zámkoch, dňa:

v mene Poskytovateľa
Ing. Peter Máčaj
predseda predstavenstva, Slovanet, a.s.

v mene Verejného obstarávateľa
JUDr. Mgr. Mikuláš Blaško
Riaditeľ FNsP Nové Zámky

Ing. Peter Tomášek
člen predstavenstva, Slovanet, a.s.

Príloha č. 2
Dodatok o bezpečnostných opatreniach a notifikačných povinnostiach

Bezpečnostné opatrenia zahŕňajú najmä nasledujúce opatrenia:

1. Organizácia informačnej bezpečnosti

1.1. Poskytovateľ má interne zavedený systém manažérstva informačnej bezpečnosti s definovaným rozsahom, cieľmi, politikami, rolami a zodpovednosťami (vlastník, správca, garant, kontaktná osoba)
1.2 Kontaktná osoba Poskytovateľa pre oblasť informačnej a kybernetickej bezpečnosti je RNDr. Ján Gallo
1.3 Kontakty Objednávateľa pre oblasť informačnej a kybernetickej bezpečnosti je spoločnosť Energotel, a.s.

2 Riadenie aktív, hrozieb a rizík

2.1 Poskytovateľ udržiava a pravidelne aktualizuje zoznam informačných aktív, ktoré svojou podstatou prispievajú k prevádzke služieb poskytovaných objednávateľovi.
2.2 Poskytovateľ je povinný na žiadosť objednávateľa predložiť aktuálny štruktúrovaný zoznam. Povinné položky – identifikátor, názov, lokalita, typ, výrobca, väzba na iné aktíva. Voliteľné položky – kapacita, operačný systém, typ SW alebo firmware, verzia, MAC alebo IP adresa.
2.3 Poskytovateľ v dostatočnom časovom predstihu informuje objednávateľa o zámere vyradiť alebo zlikvidovať časti informačných aktív, a to najmä dáta, kópie alebo archívy dát ako aj fyzické nosiče dát. Objednávateľ určí vhodný spôsob likvidácie vzhľadom na klasifikáciu informačného aktíva.
2.4 Objednávateľ a Poskytovateľ pravidelne vyhodnocujú riziká, zraniteľnosti a slabiny informačných aktív.
2.5 Informácie o zistených hrozbách, zraniteľnostiach alebo slabinách s vysokým rizikom nepriaznivého dopadu na Dôvernosť, Dostupnosť a Integritu poskytovanej služby si zmluvné strany vymieňajú. Technické zraniteľnosti uverejnené v databáze NBÚ (https://www.sk-cert.sk/sk/sluzby/odber-bulletinov-a-varovani/index.html) https://nvd.nist.gov/vuln/full-listing so skóre CVSS 7(Vysoká) až 10(Kritická) najneskôr do 3 pracovných dní.

3 Personálna bezpečnosť
3.1 Informácie bez ohľadu na to či sú v hmotnej alebo nehmotnej forme, či sú vyjadrené ústne, písomne alebo v akejkoľvek inej podobe a to aj v prípade, ak nie sú výslovne označené ako Dôverné/Prísne dôverné musia byť chránené zamestnancami Objednávateľa a Poskytovateľ a to počas aktívnej spolupráce ako aj po jej skončení. Z toho dôvodu uzatvára Objednávateľ s Poskytovateľom dohodu o mlčanlivosti, ktorá je platná pre všetky osoby v priamom alebo nepriamom pracovnom vzťahu v súlade s bodom 6 čl. IX. a čl. X. tejto zmluvy.
3.2 Poskytovateľ s ohľadom na stav a potreby systému riadenia informačnej bezpečnosti pripraví plán rozvoja bezpečnostného povedomia svojich zamestnancov a subdodávateľov.
3.3 Objednávateľ má povinnosť poučiť zamestnancov Poskytovateľa resp. subdodávateľov, ktorí pristupujú k informačným aktívam klasifikovaným ako Dôverné, Prísne dôverné, Mission Critical alebo Business critical o pravidlách informačnej bezpečnosti.
3.4 Poskytovateľ v dostatočnom predstihu informuje Objednávateľa o zmene/výmene zamestnanca, ktorý bude vykonávať činnosti súvisiace s poskytovanou službou.
3.5 Poskytovateľ zabezpečí odovzdanie zodpovedností na nového zamestnanca. Objednávateľ si vyhradzuje právo pre kontrolu odovzdania/preberania know-how resp. zodpovedností.
3.6 Objednávateľ má právo žiadať výmenu zamestnanca/zástupcu Poskytovateľa pokiaľ svojou aktivitou spôsobil kybernetický bezpečnostný incident, alebo spôsobil výrazné zhoršenie poskytovaných služieb.
3.7 Poskytovateľ je povinný vymeniť svojho zamestnanca/zástupcu s okamžitou platnosťou ak spôsobil závažný kybernetický bezpečnostný incident alebo do troch mesiacov ak spôsobil kybernetický bezpečnostný incident resp. zhoršil kvalitu poskytovaných služieb.
3.8 Objednávateľ si vyhradzuje právo pre monitorovanie a kontrolu dodržiavania pravidiel informačnej bezpečnosti a mlčanlivosti na informačných systémoch vo vlastnej správe.
3.9 Porušenie mlčanlivosti je považované za kybernetický bezpečnostný incident o ktorom sa Objednávateľ s Poskytovateľom navzájom informujú.

4 Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov

4.1 Poskytovateľ informuje objednávateľa v prípade angažovania alebo zmeny tretej strany (subdodávateľ) na činnosti, ktoré priamo súvisia s dodávkou tovarov a služieb pre objednávateľa.
4.2 Objednávateľ sa riadi formálnym postupom pre prideľovanie, zmeny a zrušenie prístupu Poskytovateľa k informačným aktívam objednávateľa.
4.3 Objednávateľ si vyhradzuje právo monitorovať alebo blokovať aktivity Poskytovateľa v prípade podozrenia z narušenia informačnej bezpečnosti. Takéto blokovanie sa nepovažuje za prekážku vo výkone zmluvných činností Poskytovateľ a.
4.4 Poskytovateľ sa zaväzuje v rámci dodávky poskytovaných tovarov a služieb uvádzať zoznam dokumentov, softvér, návrhy, obchodné značky, patenty, licencie na ktoré sa vzťahuje ochrana duševného vlastníctva.
4.5 Objednávateľ a Poskytovateľ sa zaväzujú nepoužívať softvér, ku ktorému nie je možné preukázať doklad o nadobudnutí.
4.6 Poskytovateľ sa zaväzuje informovať Objednávateľa o používaní programov, utilít alebo zariadení, ktoré môžu mať schopnosť obísť systémové a aplikačné opatrenia. Takéto programy sú napr. backdoor, rootkit, keylogger alebo SW nástroje využívajúce privilegovaný účet (administrátor).
4.7 Pokiaľ je predmetom dodávky softvérové riešenie dodané a customizované výhradne pre Objednávateľa Poskytovateľ odovzdá Objednávateľovi zdrojové kódy alebo ich sprístupní a pravidelne vykonáva aktualizáciu pri zmenách.
4.8 Objednávateľ sa zaväzuje obmedziť prístup ku knižnici zdrojových kódov tak, aby nedochádzalo k nežiadúcej modifikácii. O sprístupnení zdrojových kódov vedie Objednávateľ záznam.
4.9 Pre informačné aktíva klasifikované ako Mission Critical alebo Prísne dôverné, ktorých zdrojové kódy sú uložené v knižnici Objednávateľa sú pravidelne, minimálne 1x za dva roky skompilované a protokolárne otestovaná funkčnosť. Kompiláciu vykonáva Poskytovateľ a test Objednávateľ.
4.10 Pre informačné aktíva klasifikované ako Mission Critical alebo Prísne dôverné Poskytovateľ vytvorí vývojový, testovací a produkčný systém. Všetky tri systémy sú striktne oddelené (databáza, aplikačná a prezentačná vrstva), aby nedochádzalo k neautorizovanému zásahu do produkčného systému.
4.11 Dáta klasifikované ako Dôverné alebo Prísne dôverné nemôžu byť použité vo vývojovom alebo testovacom systéme bez predchádzajúcej anonymizácie resp. pseudonymizácie. Proces anonymizácie-pseudonymizácie zabezpečí Poskytovateľ pokiaľ sa nedohodne s Objednávateľom inak.
4.12 Ak je predmetom dodávky vývoj a údržba softvéru vypracuje Poskytovateľ pracovný postup pre preklápanie zmien z vývojového resp. testovacieho systému na produkčný.
4.13 Objednávateľ sa zaväzuje postupovať podľa vypracovaného postupu.

5 Technické zraniteľnosti systémov a zariadení
5.1 Objednávateľ s Poskytovateľom sa navzájom informujú, pokiaľ sa dozvedia o technickej zraniteľnosti prostredníctvom kontaktného kanála.
5.2 Objednávateľ ani Poskytovateľ nesmú testovať zraniteľnosť na produkčnom systéme.
5.3 Poskytovateľ sa zaväzuje vykonať testovanie zraniteľností pre dodané riešenie pokiaľ riešenie je dostupné z verejného internetu.
5.4 Objednávateľ si vyhradzuje právo vykonať testovanie (audit, penetračné testy) o tomto zámere však je povinný informovať Poskytovateľa.
5.5 Poskytovateľ aplikuje opravy a bezpečnostné záplaty systémov a zariadení štandardizovaným procesom po súhlase Objednávateľa.
5.6 Poskytovateľ na vyžiadanie Objednávateľa otestuje kompatibilitu pripravovaných bezpečnostných záplat.

6 Riadenia bezpečnosti sietí a informačných systémov
6.1 Poskytovateľ a Objednávateľ sa zaväzuje zabezpečiť segmentáciu komunikačnej siete tak, aby boli v primeranej miere chránené informácie v jednotlivých segmentoch a aby sa zabránilo šíreniu kybernetických bezpečnostných incidentov do ďalších segmentov:
a) segment prístupný z internetu má byť oddelený od ostatných segmentov,
b) segment používateľských počítačov má byť oddelený od segmentu serverov,
c) segment riadenia, konfigurácie a logovania sieťových prvkov má byť oddelený od segmentu na prenášanie prevádzkových dát,
d) segment s bezdrôtovými technológiami má byť oddelený od ostatných segmentov, atď.
6.2 Poskytovateľ s Objednávateľom zabezpečia, aby oddelenie segmentov sietí bolo realizované zariadením (perimetrom), ktoré:
a) aktívne filtruje prenášané dáta,
b) vytvára záznamy/logy o úspešných aj neúspešných prenosoch,
c) má schopnosť posielať záznamy na nadradené systémy pre spracovávanie logov,
d) má možnosť notifikovať vybrané udalosti,
e) má možnosť segregácie interface pre management/logovanie a prevádzku.

6.3 Objednávateľ určí zodpovednosti a postupy riadenia pre sieťové prvky v jednotlivých segmentoch.
6.4 Objednávateľ s Poskytovateľom navrhnú primerané riešenie, ktoré pomocou kryptografie zabezpečí dôvernosť a integritu pre vzdialený prístup, vzdialenú správu alebo prístup používateľov.
6.5 Správu sieťových zariadení informačných aktív klasifikovaných ako Mission Critical alebo Prísne dôverné, môže vykonávať administrátor, ktorý:

a) je pred vykonaním zmien jednoznačne autorizovaný,
b) pristupuje bezpečným kanálom chráneným primeranou kryptografiou,
c) pristupuje z dôveryhodného zariadenia ako je napr. terminálový server.

Osobný počítač administrátora sa štandardne nepovažuje za dôveryhodné zariadenie, preto je nevyhnutné zabezpečiť pre prístup ku konfigurácii sieťových prvkov a zariadení filtrovanie komunikačného kanála (obmedzenie na nevyhnutný typ komunikačného protokolu, kontrola škodlivého kódu,...).
6.6 Objednávateľ s Poskytovateľom zabezpečia, aby komunikácia prostredníctvom verejného internetu mala aplikované kryptografické nástroje pre zabezpečenie dôvernosti a integrity. Šifrovací kanál môže byť prerušený alebo ukončený len na dedikovanom bode/segmente siete, ktorý je oddelený od bežného používateľského resp. serverového alebo manažment segmentu.
6.7 Objednávateľ zabezpečí vykonanie pravidelných penetračných testov na všetky informačné aktíva, ktoré sú dostupné z verejného internetu, prvýkrát pred uvedením do prevádzky.
6.8 Objednávateľ s Poskytovateľom zabezpečia, aby bezdrôtové siete mali aplikovanú primerané nástroje na autorizáciu a kryptovanie prenášaných dát.

7 Riadenie prevádzky

7.1 Poskytovateľ sa zaväzuje vypracovať prevádzkové postupy aktivít používateľov a správcov. Prevádzkové postupy obsahujú: inštaláciu a konfiguráciu systémov, štandardné narábanie s informačným aktívom, zálohovanie, riešenie chybových stavov, atď.
7.2 Objednávateľ sa zaväzuje realizovať školenia a dodržiavať stanovené prevádzkové postupy vypracované Poskytovateľom.
7.3 Objednávateľ si vyhradzuje právo dodržiavať interné postupy pre riadenie zmien, ktorý je formalizovaný a reflektuje požiadavky kybernetickej bezpečnosti.
7.4 Poskytovateľ s objednávateľom vykonávajú monitoring využívania zdrojov (capacity management). Monitoring je vykonávaný jedným technickým nástrojom dostupným podľa požiadaviek obidvoch strán.
7.5 Objednávateľ stanoví kapacitné limity pri ktorých sú notifikované obidve strany. Prekročenie limitu sa považuje za incident a je riešený štandardným dohodnutým procesom.
7.6 Poskytovateľ sa zaväzuje poskytnúť informácie o kompatibilite dodávaných tovarov a služieb s riešením Objednávateľa pre ochranu pred škodlivým kódom.
7.7 Objednávateľ vyžaduje udržiavať aktualizovaný systém ochrany pred škodlivým kódom na pracovných staniciach, na serveroch a na perimetroch oddeľujúcich jednotlivé sieťové segmenty.
7.8 Objednávateľ informuje Poskytovateľa o výskyte škodlivého kódu na informačných aktívach klasifikovaných ako Mission Critical alebo Prísne dôverné.
7.9 Výskyt škodlivého kódu je riešený ako štandardný incident podľa formalizovaného postupu Objednávateľa alebo podľa postupu dohodnutom zmluvne s Poskytovateľom.
7.10 Poskytovateľ sa zaväzuje pripájať sa k informačným aktívam iba koncovým zariadením s aktualizovaným systémom pre ochranu pred škodlivým kódom.
7.11 Objednávateľ si vyhradzuje právo blokovať nežiadúci softvér, komunikáciu, mailové správy alebo prístup na webové stránky.
7.12 Objednávateľ udržiava dokumentovaný systém zálohovania, ktorý je primeraný definovaným požiadavkám klasifikácie (RTO a RPO). Pre informačné aktíva klasifikované ako Mission Critical je objednávaný taký systém zálohovania, s ktorým je možné vykonať úplnú obnovu dát v súlade s RPO.
7.13 Objednávateľ zabezpečí aby proces zálohovania bol logovaný a monitorovaný.
7.14 Objednávateľ udržiava systémy na synchronizáciu času.
7.15 Poskytovateľ zabezpečí aby dodávané zariadenia a služby si synchronizovali čas zo systémov Objednávateľa.
7.16 Objednávateľ udržiava zoznam autorizovaného softvéru a formalizovaný postup pre inštaláciu softvéru. Vyhradzuje si právo blokovať inštaláciu neautorizovaného softvérového kódu.
7.17 Objednávateľ vykonáva pravidelný audit objednávaných informačných systémov.
7.18 Poskytovateľ sa zaväzuje že nebude brániť vo výkone auditu.

8 Riadenie prístupov

8.1 Objednávateľ udržiava formalizovaný proces riadenia prístupových práv, pričom je v súlade s princípom minimálneho prístupu (need-to-know).
8.2 Poskytovateľ bude mať prístup do infraštruktúry Objednávateľom prostredníctvom VPN tunel – OpenVPN.

8.3 Každý používateľ (fyzická osoba), technický účet má pridelené jedinečné prihlasovacie konto, pod ktorým je identifikovaný v informačných systémoch a logoch.
8.4 Privilegovaný účet určený pre správu systému je oddelený od bežného používateľského účtu.
8.5 Pre prístup k informačným systémom je preferovaný Role Based Access Control (priraďovanie prístupu skupine/role, používatelia sú priraďovaný do skupín) a Single-sign-on (používateľ zadáva prihlasovacie údaje iba raz).
8.6 Pre prístup k dátam v informačných systémoch klasifikovaných ako Prísne dôverné a pre privilegované účty je odporúčaný autentizačný mechanizmus, ktorý nie je závislý iba na použití identifikátora účtu a hesla ale na viacfaktorovej autentizácii s minimálne dvomi rôznymi typmi faktorov.
8.7 Ak nie je možné použiť viacfaktorovú autentizáciu pre systémy klasifikované ako Prísne dôverné alebo pre používateľov s privilegovanými právami (správca) je odporúčané voliť heslo, ktoré:

a) Má dĺžku minimálne 14 znakov,
b) Pozostáva z kombinácie malých veľkých písmen, číslic a špeciálnych znakov,
c) Je odlišné ako 12 predchádzajúcich hesiel,
d) Je pravidelne menené maximálne do 18 mesiacov (toto pravidlo sa neaplikuje na technické účty a účty pre obnovu systému),
e) Je zmenené po jeho prvom použití ak bolo nastavené východzia hodnota
f) Nesmie byť menené viackrát v priebehu 24 hodín.

8.8 Pre prípad nečinnosti užívateľa – správcu nastaví Poskytovateľ na jeho pracovných staniciach time out 300 sekúnd.
8.9 Objednávateľ pravidelne vykonáva audit prístupových práv a to aj na systémoch, ktoré sú objednávané Poskytovateľ.
8.10 Objednávateľ si vyhradzuje právo vykonávať zmeny v prístupových právach.
8.11 Poskytovateľ sa zaväzuje umožniť objednávateľovi výkon riadenia prístupu a auditu oprávnení.

9 Kryptografické opatrenia
9.1 Objednávateľ požaduje implementáciu vhodných kryptografických opatrení pre informačné systémy klasifikované ako Prísne dôverné, Dôverné a pre systémy s vysokým stupňom Integrity:

a) Ukladanie dát na zašifrované úložisko, resp. aplikovanie kryptografických metód v databázových systémoch alebo prenosných médiách,
b) Archivácia dát na zašifrované médiá,
c) Prenos dát v šifrovanom kanály,

9.2 Pre zaručenie Dôvernosti a Integrity je odporúčané použiť systém správy kľúčov a certifikátov (PKI), ktorý:

a) Zabezpečuje generovanie, distribúciu, ukladanie, archiváciu, zmeny, obmedzenie platnosti, obnovu, revokáciu certifikátov a likvidáciu kľúčov.
b) Umožní audit a kontrolu

9.3 Poskytovateľ môže použiť len také kryptografické nástroje, ktoré odsúhlasil Objednávateľ.
9.4 Objednávateľ si vyhradzuje právo zneplatniť šifrovacie kľúče, aby zabránil znehodnoteniu informácií.

10 Riešenie kybernetických bezpečnostných incidentov
10.1 Objednávateľ a Poskytovateľ spolupracujú v súlade so zákonnými požiadavkami pri riešení kybernetických incidentov.
10.2 Poskytovateľ sa zaväzuje bezodkladne informovať objednávateľa o výskyte kybernetického bezpečnostného incidentu na systéme alebo na podpornom systéme, ktorý priamo súvisí s poskytovanými službami. Informácia obsahuje:

a) Typ, funkciu a popis zariadenia, typ a verziu operačného systému alebo firmware, sieťový protokol
b) Identifikátor – Názov, IP adresa, MAC adresa,
c) Lokalitu – umiestnenie zariadenia
d) Čas vzniku incidentu a zistenia, trvanie,
e) Identifikovaný zdroj/príčinu incidentu napr.
    a. Neefektívne bezpečnostné opatrenia,
    b. Ľudské chyby,
    c. Nedodržanie bezpečnostných postupov alebo politiky,
    d. Porušenie opatrení fyzickej bezpečnosti,
    e. Neriadené zmeny systémov
    f. Škodlivý kód
    g. Porušenie prístupových práv.
f) Detailný popis priebehu kybernetického bezpečnostného incidentu,
g) Vykonané kroky pre návrat funkcionality,

10.3 Objednávateľ zabezpečí zber údajov potrebných pre analýzu incidentu ako napr. auditné logy, zdroj útoku (mail, súbor, URL), obraz pamäti servera (dump), záznam sieťovej komunikácie (packet capturing).
10.4 Poskytovateľ poskytne maximálnu súčinnosť pre zber dôkazov a identifikáciu kybernetického bezpečnostného incidentu.
10.5 Objednávateľ vykoná kategorizáciu kybernetického bezpečnostného incidentu v zmysle platnej vyhlášky NBÚ a postupuje v súlade so stanovenými postupmi.
10.6 V prípade určenia závažného kybernetického incidentu kategórie I.- až III. Poskytovateľ s Objednávateľom vytvoria virtuálny CIRT (Computer Incident Response Team) z odborníkov, ktorí vedia vecne prispieť k riešeniu a eliminácii dopadov kybernetického incidentu.
10.7 Virtuálny CIRT vykoná analýzu vzniku, rozsahu a následkov incidentu.
10.8 Virtuálny CIRT eskaluje incident na zástupcov managementu Objednávateľa a Poskytovateľ.
10.9 Objednávateľ a Poskytovateľ zabezpečia informovanie svojich zamestnancov v miere potrebnej pre zabránenie rozšírenia incidentu.
10.10 V prípade kategórie I. až III. CIRT spolupracuje s NBÚ so špecializovanou jednotkou SK-CERT.
10.11 CIRT vyhotovuje záznam o vykonaných krokoch.
10.12 CIRT vyhotoví záverečnú formálnu správu (lessons-learned) s odporúčaniami pre elimináciu výskytu obdobného incidentu.

11 Monitorovanie, testovanie bezpečnosti a bezpečnostných auditov
11.1 Prevádzkové udalosti informačného a komunikačného systému, používateľov a administrátorov sú zaznamenávané a spracovávané vhodným technickým riešením.
11.2 Poskytovateľ poskytne Objednávateľovi prístup alebo zabezpečí doručovanie takýchto udalostí so zreteľom na zachovanie integrity záznamov v minimálnom formáte:

a) Dátum a čas
b) Typ udalosti (napr. prihlásenie, odhlásenie, zmena, mazanie)
c) Identifikácia aktíva, ktorá udalosť zaznamenala
d) Jednoznačná identifikácia účtu pod ktorým bola činnosť vykonaná
e) Jednoznačnú sieťovú identifikáciu zariadenia zdroja,
f) Úspešnosť alebo neúspešnosť činnosti

11.3 Objednávateľ si vyhradzuje právo definovať typ udalosti, ktorý má byť zaznamenávaný.
11.4 Záznamy musia byť chránené pred nežiaducou editáciou a mazaním.
11.5 Prekročenie kapacity záznamových médií alebo vymazanie záznamov generujú automatické záznamy.
11.6 Poskytovateľ sa zaväzuje zaznamenávať prihlásenie/odhlásenie privilegovaných účtov resp. ich aktivitu v potrebnom rozsahu.

12 Fyzická bezpečnosť a bezpečnosť prostredia
12.1 Objednávateľ stanovuje fyzický bezpečnostný perimeter ohraničujúci oblasť v ktorej sú uchovávané a spracovávané informácie a umiestnené technické aktíva informačných a komunikačných systémov.
12.2 Poskytovateľ sa zaväzuje dodržiavať ohraničené oblasti.
12.3 Serverové časti a centrálne komunikačné zariadenia informačných aktív klasifikovaných ako Prísne dôverné alebo Mission Critical môžu byť umiestnené len v objektoch s nepretržitým monitorovaním a obmedzením prístupu. Miestnosti musia byť uzamykateľné s detekciou narušenia, výskytu dymu, požiaru, zaplavenia atď. Pohyb zamestnancov Poskytovateľa je povolený pod dohľadom zodpovedného zamestnanca Objednávateľa alebo s jeho zadokumentovaným povolením.
12.4 Vytváranie audio-vizuálnych záznamov v miestnostiach, kde sú uložené centrálne zariadenia informačných aktív klasifikovaných ako Prísne dôverné alebo Mission Critical, môžu len zamestnanci Objednávateľa. Poskytovanie takýchto záznamov druhej strane je riadené zmluvou o mlčanlivosti.
12.5 V prípade elektrického zabezpečovacieho systému sa zaznamenáva dátum a čas príchodu a odchodu. Tieto záznamy sú uchovávané po dobu min. 12 mesiacov.
12.6 Objednávateľ sa zaväzuje oboznámiť zamestnancov Poskytovateľa pred vstupom do priestorov s nebezpečenstvom.
12.7 Poskytovateľ je povinný informovať Objednávateľa o likvidácii/vyradení/poškodení zariadení informačných aktív klasifikovaných ako Prísne dôverné alebo Mission Critical.
12.8 Objednávateľ je povinný vykonať kontrolu uložených dáta alebo konfigurácií takýchto zariadení a zabrániť úniku dát viacnásobným prepísaním úložiska zariadenia alebo fyzickou likvidáciou obsahu.
12.9 Nosiče s dátami klasifikovanými ako Prísne Dôverné alebo Dôverné musia byť mimo ich používania uzamknuté.
12.10 Počítač zamestnanca Objednávateľa alebo Poskytovateľa s prístupom k Prísne dôverným a Dôverným informáciám musia byť v prípade jeho neprítomnosti v stave odhlásené alebo so zamknutou obrazovkou

13 Riadenie kontinuity procesov

13.1 Pre informačné systémy klasifikované ako Mission Critical a Business Critical vypracuje Objednávateľ plány obnovy resp. plán kontinuity. Pokiaľ je služba poskytovaná Poskytovateľom, je povinný predložiť plány obnovy na odsúhlasenie Objednávateľovi.

13.2 Pre informačné aktíva klasifikované ako Mission Critical a Business Critical sú testované plány obnovy a kontinuity pravidelne minimálne jedenkrát za dva roky alebo po výraznej zmene informačného aktíva. Správa z testu s návrhom na riešenie zistených nedostatkov je bez zbytočného odkladu odovzdaná Objednávateľovi.

13.3 Záložné médiá a prostriedky pre obnovu kontinuity činnosti musia byť umiestňované v zabezpečených priestoroch mimo hlavných prevádzkových pracovísk.