NÁRODNÝ ÚSTAV DETSKÝCH CHORÔB
Limbová 1, 833 40 Bratislava, Slovenská republika

ZMLUVA O ZABEZPEČENÍ PLNENIA BEZPEČNOSTNÝCH OPATRENÍ A NOTIFIKAČNÝCH POVINNOSTÍ

Článok č. 1. Zmluvné strany

Objednávateľ: **Národný ústav detských chorôb**
Limbová 1, 833 40 Bratislava
Konajúci prostredníctvom: MUDr. Peter Bartoň, riaditeľ
IČO: 00 607 231
DIČ: 2020848368
IČ pre DPH: SK2020848368
Bankové spojenie:
IBAN:
SWIFT:

Zriaďovacou listinou zo dňa 18.12.1990 č. j. 1841/1990-A/III-2 s účinnosťou od 1.1.1991 v znení neskorších rozhodnutí

Kontaktná osoba:
Telefonický kontakt:
E-mail:

(ďalej len **„Objednávateľ,“ „Prevádzkovateľ základnej služby,“ „Poskytovateľ“** alebo **„PZS“**)

Dodávateľ: **STAPRO SLOVENSKO s.r.o.**
Hroncova 3, 040 01 Košice
Konajúci prostredníctvom: Ing. Adrián Petrik, konateľ
IČO: 31 710 549
DIČ: 2020483982
IČ pre DPH: SK2020483982

Spoločnosť je zapísaná v Obchodnom registri Mestského súdu Košice I
Oddiel: Sro, vložka č.: 6435/V

Kontaktná osoba:
Telefonický kontakt:
E-mail:

(ďalej len **„Dodávateľ“** alebo **„Poskytovateľ“**)

Prevádzkovateľ a dodávateľ sa ďalej označujú jednotlivo ako **„zmluvná strana“** a spoločne ako **„zmluvné strany“**. Táto Zmluva sa ďalej označuje spoločne s jej prílohami ako **„Zmluva.“** Zmluvné strany s úmyslom byť viazané podmienkami uvedenými nižšie uzatvárajú túto zmluvu v zmysle § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a podľa § 8 vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Článok č. 2. Úvodné ustanovenia

2.1. Zmluvné strany potvrdzujú, že medzi sebou uzatvorili Zmluvu o poskytovaní služieb – podpora prevádzky IS 109/2023 zo dňa 27.03.2023, predmetom ktorej je podpora prevádzky IS (ďalej len **„Hlavná zmluva“**).

2.2. Pri plnení Hlavnej zmluvy vykonáva Dodávateľ činnosti, ktorých konkrétny rozsah je uvedený v Prílohe 1 tejto Zmluvy.

2.3. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí bez zbytočného odkladu, najneskôr však do 5 pracovných dní od účinnosti príslušnej zmeny. Zoznam pracovných rolí Dodávateľa, ktoré majú mať prístup k informáciám a údajom Prevádzkovateľa ku dňu uzatvorenia Zmluvy je uvedený v Prílohe č. 2 tejto Zmluvy.

Článok č. 3. Definície pojmov a výkladové pravidlá

3.1. Ak nie je výslovne uvedené inak,

(a) pojmy a výrazy používané v tejto Zmluve, ktoré sú definované v Zákone a vo vykonávacích predpisoch, majú význam definovaný v týchto právnych predpisoch, pričom výklad ich obsahu musí byť v súlade s ich vymedzením v Smernici Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,

(b) alebo ak z obsahu nevyplýva niečo iné, jednotné číslo zahŕňa aj množné číslo a naopak,

(c) akýkoľvek odkaz na akýkoľvek bod, písmeno alebo prílohu je odkazom na bod, písmeno alebo prílohu tejto Zmluvy.

Článok č. 4. Predmet zmluvy

4.1. Predmetom tejto Zmluvy je úprava vzájomných práv a povinností Zmluvných strán s cieľom zabezpečiť plnenie bezpečnostných opatrení a notifikačných povinností pri výkone činností podľa Hlavnej zmluvy, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby (ďalej len **„Plnenie Hlavnej zmluvy“**).

4.2. Účelom tejto Zmluvy je predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby pri Plnení Hlavnej zmluvy.

Článok č. 5. Práva a povinnosti Zmluvných strán

5.1. Dodávateľ vyhlasuje, že sa pred uzavretím tejto Zmluvy oboznámil s bezpečnostnými politikami uplatňovanými u Prevádzkovateľa, s týmito bezpečnostnými politikami vyjadruje svoj súhlas a zaväzuje sa ich v celom rozsahu dodržiavať. Bezpečnostné politiky podľa predchádzajúcej vety sú uvedené v Prílohe č. 4 tejto Zmluvy - **Bezpečnostné politiky.**

5.2. Dodávateľ sa zaväzuje prijať a dodržiavať bezpečnostné opatrenia, ktorých minimálny rozsah a konkrétna špecifikácia sú uvedené v Prílohe č. 3 tejto Zmluvy a s týmito bezpečnostnými opatreniami vyjadruje Dodávateľ svoj súhlas (ďalej len **„Bezpečnostné opatrenia“**).

5.3. Vzhľadom na skutočnosť, že sa Bezpečnostné opatrenia u Prevádzkovateľa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu, je Prevádzkovateľ v závislosti na obsahu bezpečnostnej dokumentácie oprávnený jednostranne meniť obsah Bezpečnostných politík a upravovať rozsah a druhy Bezpečnostných opatrení, a to predovšetkým v prípade, ak sú dostupné prostriedky schopné zabezpečovať kybernetickú bezpečnosť účinnejšie než doposiaľ uplatňované. Úprava Bezpečnostných opatrení sa bude vykonávať zmenou Prílohy č. 3 tejto zmluvy.

5.4. Prevádzkovateľ si vyhradzuje právo vykonávať v rámci vlastných alebo ním prevádzkovaných sietí a informačných systémov, ku ktorým má Dodávateľ prístup, kontroly bezpečnosti vykonávaných zásahov a prijímať opatrenia za účelom identifikácie zneužitia prístupu k týmto sieťam a informačným systémom.

5.5. Dodávateľ sa zaväzuje, že po ukončení Hlavnej zmluvy Prevádzkovateľovi vráti, prevedie alebo podľa jeho pokynov aj zničí všetky informácie, ku ktorým má počas trvania Hlavnej zmluvy prístup.

5.6. Dodávateľ je povinný bezodkladne, avšak najneskôr do 4 hodín od zistenia kybernetického bezpečnostného incidentu, informovať Prevádzkovateľa o kybernetickom bezpečnostnom incidente týkajúcom sa služieb poskytovaných na základe Hlavnej zmluvy. Dodávateľ môže informovať Prevádzkovateľa osobne prostredníctvom zodpovednej osoby uvedenej v Zmluve, zabezpečenou formou prostredníctvom e-mailu na andrej.gall@nudch.eu.

Článok č. 6. Kontrolné činnosti, audity a nápravné opatrenia

6.1. Ak je to potrebné na zabezpečenie kybernetickej bezpečnosti pri Plnení Hlavnej zmluvy, je Prevádzkovateľ oprávnený vydávať Dodávateľovi zdokumentované pokyny. V takom prípade je Dodávateľ povinný postupovať podľa pokynov Prevádzkovateľa a pri Plnení Hlavnej zmluvy je týmito pokynmi viazaný.

Dodávateľ je vždy povinný upozorniť Prevádzkovateľa, ak podľa jeho názoru záväzný pokyn Prevádzkovateľa porušuje Zákon, vykonávacie predpisy alebo je v rozpore so Zmluvou.

6.2. Prevádzkovateľ je oprávnený kedykoľvek overovať či Dodávateľ dodržiava Zákon, vykonávacie predpisy a či koná v súlade so Zmluvu, a to spôsobom, aby takéto kontroly nezasahovali nad nevyhnutne nutnú mieru do činnosti Dodávateľa. Kontroly je možné vykonávať najviac 4 (štyri) krát ročne, to neplatí ak sa jedná o opakovanú kontrolu na zistenie plnenia opatrení zistených pri poslednej kontrole. Tieto kontroly je Prevádzkovateľ oprávnený vykonávať aj v priestoroch Dodávateľa nahliadaním do príslušnej dokumentácie a prístupom do sietí a informačných systémov prevádzkovaných Dodávateľom a využívaných na výkon činností pri Plnení Hlavnej zmluvy. Prevádzkovateľ je oprávnený výsledky takýchto kontrol zaznamenávať a dokumentovať. Prevádzkovateľ môže takéto kontroly vykonávať sám, alebo ich vykonaním poveriť ním určenú tretiu osobu. Náklady na kontrolu znáša každá Zmluvná strana samostatne.

6.3. Prevádzkovateľ je oprávnený kedykoľvek požadovať od Dodávateľa preukázanie plnenia jeho povinností vrátane splnenia všetkých podmienok a požiadaviek podľa Zákona, vykonávacích predpisov a Zmluvy.

6.4. Dodávateľ je najmä povinný:

(a) na základe výzvy Prevádzkovateľa kedykoľvek v priebehu Plnenia Hlavnej zmluvy preukázať plnenie povinností vrátane splnenia všetkých podmienok a požiadaviek podľa Zákona, vykonávacích predpisov a Zmluvy,

(b) v rámci vykonávania kontrol alebo auditov poskytovať Prevádzkovateľovi alebo ním poverenej tretej osobe potrebné informácie, podklady, a ďalšiu súčinnosť a náležite s ním spolupracovať,

(c) poskytnúť riadne a včas všetky jemu dostupné informácie, podklady a požadovanú súčinnosť v prípade kontroly alebo auditu vykonávaného akreditovaným orgánom posudzovania zhody v oblasti kybernetickej bezpečnosti alebo Úradom a v celom rozsahu s nimi spolupracovať,

(d) bez zbytočného odkladu, najneskôr však v lehote stanovenej Prevádzkovateľom, zjednať nápravu v prípade, ak Prevádzkovateľ zistí, že Dodávateľ porušuje alebo neplní svoje povinnosti vyplývajúce mu zo Zákona, vykonávacích predpisov a ďalších všeobecne záväzných právnych predpisov alebo nepostupuje v súlade so Zmluvou.

6.5. Dodávateľ je povinný informovať Prevádzkovateľa, ak je pravdepodobné, že uplatňované Bezpečnostné politiky alebo prijaté Bezpečnostné opatrenia nemusia byť z hľadiska požiadaviek Zákona alebo vykonávacích predpisov dostatočné.

Článok č. 7. Súčinnosť Dodávateľa pri plnení povinností Prevádzkovateľa

7.1. Dodávateľ je povinný bezodkladne informovať Prevádzkovateľa o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti.

7.2. Dodávateľ je povinný poskytnúť Prevádzkovateľovi všetky jemu dostupné informácie, podklady, a ako aj ďalšiu možnú súčinnosť, ktorá je potrebná za účelom plnenia povinnosti Prevádzkovateľa:

(a) prijať bezpečnostnú dokumentáciu a udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu,

(b) riešiť kybernetický bezpečnostný incident na základe rozhodnutia Úradu podľa § 27 ods. 3 Zákona, vykonať reaktívne opatrenie na základe rozhodnutia Úradu podľa § 27 ods. 5 Zákona alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa § 27 ods. 6 Zákona,

(c) predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8 Zákona,

(d) bezodkladne hlásiť závažný kybernetický bezpečnostný incident (nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 Zákona alebo odoslať neúplné hlásenie podľa § 24 ods. 5 Zákona),

(e) spolupracovať s Úradom a Ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

(f) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,

(g) oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

(h) poskytnúť Úradu v prípade výkonu kontroly požadovanú súčinnosť,

(i) prijať na základe výsledku kontroly opatrenia na odstránenie zistených nedostatkov a príčin ich vzniku a predložiť ich Úradu,

(j) predložiť Úradu písomnú správu o splnení opatrení prijatých na odstránenie zistených nedostatkov,

(k) preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia Prevádzkovateľa do registra prevádzkovateľov základnej služby,

(l) preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa vykonávacích predpisov, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale,

(m) predložiť Úradu záverečnú správu o výsledkoch auditu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu,

(n) vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu.

7.3. V prípade, ak je poskytnutie informácií, podkladov alebo súčinnosti zo strany Dodávateľa pre splnenie povinnosti Prevádzkovateľa podľa bodu 7.2 písm. a) až n) nevyhnutné, je Dodávateľ povinný konať podľa pokynov, ktoré mu Prevádzkovateľ za tým účelom preukázateľne vydal.

7.4. Informácie, podklady a ďalšie skutočnosti, ktorých hlásenie alebo predloženie je Prevádzkovateľom požadované na účely plnenia jeho povinností podľa bodu 7.2 písm. a) až n) bude Dodávateľ Prevádzkovateľovi poskytovať spôsobom a vo forme dohodnutej v bode 12.3.

Článok č. 8. Dôvernosť poskytnutých informácií

8.1. Dodávateľ je povinný chrániť všetky informácie poskytnuté Prevádzkovateľom a zachovávať o nich mlčanlivosť. Povinnosť mlčanlivosti trvá aj po ukončení Hlavnej zmluvy.

8.2. Povinnosť Dodávateľa zachovávať mlčanlivosť alebo dôvernosť informácií, ak bola založená na základe inej zmluvy uzavretej s Prevádzkovateľom alebo uložená osobitným predpisom, nie je týmto dotknutá a zostáva zachovaná.

8.3. Dodávateľ nesmie informácie získané pri Plnení Hlavnej zmluvy použiť pre iné účely, než výslovne stanovuje Zmluva alebo Hlavná zmluva. Tieto informácie nie je oprávnený poskytnúť tretím stranám bez predchádzajúceho písomného súhlasu Prevádzkovateľa, s výnimkou prípadov, kedy je také poskytnutie informácií vyžadované všeobecne záväznými právnymi predpismi. V takom prípade sa Dodávateľ zaväzuje o tejto skutočnosti Prevádzkovateľa bez zbytočného odkladu informovať, ak to nie je v rozpore s týmito právnymi predpismi alebo sa jedná o poskytnutie informácií schváleným Subdodávateľom, ak títo potrebujú mať k uvedeným informáciám prístup pre účely Plnenia Hlavnej zmluvy. Bez predchádzajúceho súhlasu Prevádzkovateľa si dodávateľ nesmie zhotovovať žiadne kópie alebo duplikáty informácií; to neplatí pre zálohovanie za účelom zabezpečenia Plnenia Hlavnej zmluvy.

8.4. Dodávateľ je povinný zaviazať mlčanlivosťou všetky osoby zúčastnené na predmete plnenia Hlavnej zmluvy tým, že zabezpečí, aby sa tieto osoby písomne zaviazali k zachovávaniu mlčanlivosti o skutočnostiach, o ktorých sa dozvedeli v súvislosti s plnením úloh podľa Hlavnej zmluvy alebo Zákona alebo vykonávacích predpisov a ktoré nie sú verejne známe. Tým nie sú dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

Článok č. 9. Subdodávatelia

9.1. Ďalšieho dodávateľa, ktorý bude namiesto Dodávateľa úplne alebo čiastočne zabezpečovať Plnenie Hlavnej zmluvy (ďalej len „**Subdodávateľ**"), smie Dodávateľ zapojiť len s predchádzajúcim písomným súhlasom Prevádzkovateľa. Pri Plnení Hlavnej zmluvy Subdodávateľom má Dodávateľ voči Prevádzkovateľovi zodpovednosť, akoby Plnenie Hlavnej zmluvy vykonával sám.

9.2. Prevádzkovateľ týmto súhlasí so zapojením Subdodávateľov, uvedených v Prílohe č. 5 tejto Zmluvy, na vykonávanie činností pri Plnení Hlavnej Zmluvy namiesto Dodávateľa.

9.3. Dodávateľ je povinný uložiť každému Subdodávateľovi rovnaké povinnosti ako má Dodávateľ podľa tejto Zmluvy.

9.4. Dodávateľ je povinný pred zapojením každého Subdodávateľa a následne v pravidelných intervaloch vykonávať kontroly u Subdodávateľov za účelom preverenia, či Subdodávateľ tieto povinnosti dodržiavajú a najmä, či dodržiava Bezpečnostné politiky a či postupuje v súlade s Bezpečnostnými opatreniami. Výsledky takých kontrol musia byť písomne zdokumentované a na požiadanie predložené Prevádzkovateľovi.

9.5. Dodávateľ je povinný zaistiť v jeho zmluve so Subdodávateľom, že Prevádzkovateľ bude mať rovnaké práva kontroly nad Subdodávateľom, ako má Prevádzkovateľ nad samotným Dodávateľom podľa Hlavnej zmluvy a tejto Zmluvy bez toho, aby tým bola dotknutá zodpovednosť Dodávateľa za Subdodávateľa. Dodávateľ sa zaväzuje, že poskytne Prevádzkovateľovi na jeho žiadosť informácie o obsahu jeho zmluvy so Subdodávateľom, ktoré sú nevyhnutné na oboznámenie sa s povinnosťami Subdodávateľa vo vzťahu k zabezpečeniu kybernetickej bezpečnosti.

Článok č. 10. Trvanie Zmluvy

10.1. Zmluva sa uzatvára na dobu trvania Hlavnej zmluvy. Zánik Hlavnej zmluvy spôsobuje zánik Zmluvy, a to s účinkom súčasného zrušenia oboch zmlúv.

10.2. Zmluvné strany sa dohodli, že ktorákoľvek zmluvná strana môže od Zmluvy odstúpiť z dôvodu jej podstatného porušenia druhou Zmluvnou stranou. Odstúpením Zmluva zaniká dňom, keď je odstúpenie doručené druhej Zmluvnej strane.

10.3. Za podstatné porušenia tejto Zmluvy Dodávateľom sa považuje najmä: (i) nedodržiavanie Bezpečnostných politík, (ii) neprijatie alebo nedodržanie Bezpečnostných opatrení, (iii) neinformovanie Prevádzkovateľa o kybernetickom bezpečnostnom incidente, (iv) neoznámenie všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti Prevádzkovateľovi (v) neposkytnutie požadovanej informácie, podkladu alebo ďalšej možnej súčinnosti Prevádzkovateľovi na účely plnenia jeho zákonných povinností, (vi) nekonanie alebo konanie v rozpore s pokynom Prevádzkovateľa, (vii), marenie alebo sťaženie výkonu kontroly alebo auditu čiastočne alebo celkovo, (viii) porušenie povinnosti zachovávať mlčanlivosť alebo dôvernosť informácií, (ix) zapojenie vopred neschváleného Subdodávateľa v akomkoľvek rozsahu alebo (x) ak sa porušenia uvedeného v predchádzajúcich bodoch (i) až (ix) dopustí Subdodávateľ Dodávateľa.

Článok č. 11. Zodpovednosť a sankcie

11.1. Dodávateľ zodpovedá v celom rozsahu za nesplnenie alebo porušenie ktorejkoľvek povinnosti vyplývajúcej z tejto Zmluvy, vrátane prípadu, ak sa tohto porušenia dopustil jeho Subdodávateľ.

11.2. Ak Dodávateľ alebo jeho Subdodávateľ nesplní alebo poruší niektorú zo svojich povinností vyplývajúcich z tejto Zmluvy je povinný zaplatiť Prevádzkovateľovi zmluvnú pokutu výške 4.385,89,- EUR (slovom štyritisíctristoosemdesiatpäť eur a osemdesiatdeväť centov) za každé jednotlivé porušenie.

11.3. Prevádzkovateľ je oprávnený, nie však povinný, požadovať od Dodávateľa úhradu zmluvnej pokuty po vzniku nároku na jej zaplatenie, a to buď v celej výške alebo len v určitej jej časti určenej podľa svojej vlastnej úvahy.

11.4. Nárok na náhradu škody zostáva zachovaný popri nároku na zmluvnú pokutu a preto uplatnenie nároku na zmluvnú pokutu nemá vplyv na povinnosť Dodávateľa nahradiť Prevádzkovateľovi škodu vzniknutú nesplnením alebo porušením jeho povinností podľa tejto Zmluvy, a to v plnej výške vrátane sumy prevyšujúcej výšku uplatnenej zmluvnej pokuty.

11.5. Za škodu sa za každých okolností bude považovať uloženie sankcie zo strany Úradu Prevádzkovateľovi z dôvodu nesplnenia alebo porušenia povinností vyplývajúcej zo Zákona, vykonávacieho predpisu alebo iného

všeobecne záväzného právneho predpisu, ak toto porušenie je spôsobené konaním, resp. nekonaním Dodávateľa alebo jeho Subdodávateľa alebo uloženie inej finančnej povinnosti právoplatným rozhodnutím iného orgánu verejnej moci (napr. súdu) vo veci týkajúcej sa porušenia alebo nesplnenia povinnosti v oblasti zabezpečenia kybernetickej bezpečnosti Dodávateľa alebo jeho Subdodávateľa.

Článok č. 12. Spoločné a záverečné ustanovenia

12.1. Dodávateľ sa zaväzuje, že po ukončení Hlavnej zmluvy udelí, poskytne, prevedie alebo postúpi všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na Prevádzkovateľa; tento záväzok Dodávateľa ostáva v platnosti po dobu päť rokov po ukončení Hlavnej zmluvy.

12.2. Ak je Hlavnou zmluvou zmluva rámcová, vzťahujú sa ustanovenia tejto Zmluvy aj na všetky čiastkové zmluvy zavretej na základe Hlavnej zmluvy alebo objednávky k Hlavnej zmluve.

12.3. Zmluvné strany sa dohodli, že ich vzájomná komunikácia pri plnení Zmluvy vrátane **hlásenia všetkých informácií majúcich vplyv na Zmluvu** vyžaduje písomnú formu, ktorú považujú za zachovanú aj v prípade elektronickej komunikácie prostredníctvom elektronickej pošty (e-mailu). Všetky informácie, údaje, oznámenia, hlásenia, pokyny, podklady a akékoľvek iné skutočnosti ktoré by mohli mať vplyv na plnenie Zmluvy, budú doručované v listinnej podobe poštou, kuriérom, osobne na adresu sídla danej Zmluvnej strany alebo jej príslušnej prevádzkarne alebo elektronickými prostriedkami na e-mailové adresy Zmluvných strán. Úkony zmluvných strán urobené v podobách uvedených podľa predchádzajúcej vety sa považujú za úkony vykonané v písomne zdokumentovanej forme.

12.4. Pre prípad, že by sa ktorékoľvek ustanovenie tejto Zmluvy ukázalo byť neplatné, neúčinné, či nevykonateľné, Zmluvné strany sa dohodli, že ho bez zbytočného odkladu po zistení tejto skutočnosti nahradia ustanovením, ktoré bude najlepšie zodpovedať obsahu a účelu pôvodného ustanovenia.

12.5. Zmluva je vyhotovená v dvoch rovnopisoch, každý s platnosťou originálu, pričom Dodávateľ dostane jedno vyhotovenie a Prevádzkovateľ tiež jedno vyhotovenia Zmluvy.

12.6. Zmluvu možno meniť len formou písomného dodatku podpísaného oboma Zmluvnými stranami, ktorý sa musí uzatvoriť v listinnej podobe alebo elektronickej podobe. Riadne uzatvorený dodatok sa stáva neoddeliteľnou súčasťou Zmluvy.

12.7. Zmluvné vzťahy vyplývajúce zo Zmluvy sa riadia slovenským právom. Na riešenie prípadných sporov zo Zmluvy sú príslušné slovenské súdy.

12.8. Zmluva nadobúda platnosť jej podpisom obomi Zmluvnými stranami a účinnosť dňom nasledujúcim po zverejnení Zmluvy v Centrálnom registri zmlúv.

12.9. Zmluvné strany vyhlasujú, že si Zmluvu pred jej podpísaním prečítali, jej obsahu porozumeli a na znak toho, že obsah Zmluvy zodpovedá ich skutočnej a slobodnej vôli, ju podpísali.

12.10. Zmluva bude zaradená do evidencie všetkých uzatvorených zmlúv s treťou stranou, ktorá tvorí súčasť bezpečnostnej dokumentácie Prevádzkovateľa podľa § 2 ods. 1 písm. c) Vyhlášky.

12.11. Zoznam príloh – neoddeliteľnou súčasťou tejto zmluvy sú:

(a) Príloha č. 1 Konkrétny rozsah činností Dodávateľa
(b) Príloha č. 2 Zoznam pracovných rolí Dodávateľa
(c) Príloha č. 3 Minimálny rozsah a špecifikácia bezpečnostných opatrení
(d) Prílohe č. 4 Bezpečnostné politiky
(e) Príloha č. 5 Zoznam schválených subdodávateľov

V Bratislave, dňa 30.8.2023

V Bratislave, dňa 25 -08- 2023

STAPRO SLOVENSKO s.r.o.
Ing. Adrián Petrik

Národný ústav detských chorôb
MUDr. Peter Bartoň

Príloha č. 1: Konkrétny rozsah činností Dodávateľa

1. Vymedzenie predmetu dodávky služieb:

Dodávateľ sa zaväzuje poskytovať dohodnuté služby na ďalej vymenované informačné technológie informačného systému objednávateľa.

Aplikačný software

Dodávateľ sa zaväzuje dodávať dohodnuté služby na vymenovaný aplikačný software (ďalej jen ASW) v tomto rozsahu licencií modulov a licencií pracovných staníc:

Licencie ASW modulov StaproMEDEA, výrobca: STAPRO s.r.o.

Správa systému
Medea mail
Obecné tlačové zostavy
Centrálny register
Evidencia hospitalizovaných
Štatistika
Lôžkové oddelenie
Ambulancia
Operačná sála
Žiadanky do laboratórií
Rádiodiagnostika
Rádiodiagnostika - komunikačný modul worklist
PANAKEA - Ústavná lekáreň - HVLP, IR
PANAKEA - Ústavná lekáreň - ZM
PANAKEA - elaborácie
PANAKEA - objednávanie z oddelení
PANAKEA - sklady lôžkové oddelenie
PANAKEA - sklady operačné sály
PANAKEA - nadstavba pre "bar code"
GURMED, pacientská strava
GURMED, zamestnanecké stravovanie, celok
GURMED, doplnkový predaj
GURMED, nadstavba pre ID karty
StaproFONS – Výkazníctvo SK
Ošetrovateľský proces
MIS BI - PANAKEA
MIS BI - StaproFONS
MIS BI - EIS Noris

Počet licencií pracovných staníc StaproMEDEA: 498 licencií
Počet licencií pracovných staníc StaproFONS: 225 licencií

Licencie ASW modulov FONS Openlims, výrobca: STAPRO s.r.o.

FONS Openlims – biochémia, hematológia, imunológia
FONS Openlims – jazyková mutácia SK
FONS Openlims – legislatívny modul SK
FONS Openlims - moduly pripojenia analyzátorov

Bio-Rad Laboratories, D-10	1ks
Bayer(Siemens), Rapidlab 1265	2ks
Roche Diagnostics, Cobas Integra 400 plus	1ks
Roche Diagnostics, Cobas Integra 800	1ks
Johnson&Johnson, Vitros Fusion 5.1	1ks
Johnson&Johnson, Vitros 5600	1ks
Lachema, Laura	1ks
Roche Diagnostics, Cobas e411	1ks
Nova Biomedical, Stat Profile CCX	1ks
Nova Biomedical, Stat Profile pHOx Ultra	1ks

Siemens (Sysmex), CA-1500	1ks
Siemens (Behring), BCS XP	1ks
Elstasit, UPD	1ks
Sysmex, XT-4000	1ks
Sysmex, KX-21 (3 p Diff)	1ks
SP 1000i (Sysmex)	1ks
SPA Plus – The binding site	1ks
RADIM(SEAC), BRIO	1ks
Biomedica, HYTEC 288	1ks

Počet licencií pracovných staníc FONS Openlims: 67 licencií

biochémia	30x
hematológia	27x
imunológia	7x
IT	1x
DKAIM, OPN	2x

Licencie ASW modulov MEDIX, výrobca: STAPRO s.r.o.

Centrálna sterilizácia (CS)
Centrálna operačné sály (COS)

Počet licencií pracovných staníc MEDIX CS:7 licencií
Počet licencií pracovných staníc MEDIX COS:10 licencií

2. Podpora aplikačných software

Aplikačný sw StaproMEDEA

Dodávateľ sa zaväzuje poskytovať pre podporu ASW StaproMEDEA a databázového prostredia firmy Progress Software Corp., v rozsahu modulov a licencií podľa kap. 1, nasledujúce služby:

Základná podpora aplikačného sw StaproMEDEA - program starostlivosti o aplikáciu zahŕňa:
- Garancia funkčnosti ASW a db prostredia – poskytovanie opravných kódov (hot-fix a patch).
- Garancia rozvoja ASW a db prostredia – poskytovanie update a upgrade.
- Garancia legislatívnych update – poskytovanie legislatívnych upgrade.
- Servisná garancia – garancia dostupnosti servisných služieb.
- Garancia dostupnosti služby HelpDesk – prístup k systému služby HelpDesk Centra podpory zákazníkov
- Garancia podpory prevádzky db prostredia.
- Garancia vybraných služieb:
- Zabezpečenie migrácie ASW StaproMEDEA na vyššiu verziu db prostredia.
- Garancia informovanosti – poskytovanie informácií o nových sw produktoch.
- Garancia možnosti účasti užívateľov na vzdelávacích stretnutiach k problematike IS.

Konzultačné hodiny - konzultačné služby poskytované dodávateľom na základe evidovanej požiadavky objednávateľa.

pracoviská s ASW StaproMEDEA: 240 hodín ročne

Konzultačné hodiny je možné čerpať:
- Riešením konzultácií a požiadaviek objednávateľa zadaných a evidovaných prostredníctvom služby HelpDesk. V prípade požiadavky na vývojové práce sa konzultačné hodiny zamieňajú za vývojové hodiny v pomere 2:1, teda 2 hodiny konzultačných prác = 1 hodina vývojových prác.
- Konzultačnou návštevou v mieste objednávateľa na základe požiadavky zadanej prostredníctvom služby HelpDesk v dohodnutom termíne podľa dohodnutých oblastí, vrátane vypracovania správy protokolu a jeho zaslanie zodpovednej osobe objednávateľa. V prípade vyžiadania osobnej konzultačnej návštevy sú hradené cestovné náklady nad rámec supervízie v zmysle platného cenníka. Rozsah konzultačnej návštevy je 8 hodín.

Aplikačný sw Openlims

Dodávateľ sa zaväzuje poskytovať pre podporu ASW OPENLIMS a databázového prostredia v rozsahu modulov a licencií podľa kap. 1, nasledujúce služby:

Základná podpora aplikačného sw OPENLIMS - program starostlivosti o aplikáciu zahŕňa:

- Garancia funkčnosti ASW – poskytovanie opravných kódov (hot-fix a patch).
- Garancia rozvoja ASW – poskytovanie update a upgrade.
- Garancia legislatívnych update – poskytovanie legislatívnych upgrade.
- Servisná garancia – garancia dostupnosti servisných služieb.
- Garancia dostupnosti služby HelpDesk – prístup k systému služby HelpDesk Centra podpory zákazníkov
- Garancia podpory prevádzky db prostredia.
- Garancia vybraných služieb:
o inštalácie opráv (hot-fix a patch),
o zabezpečenie migrácie ASW OPENLIMS na vyššiu verziu db prostredia.
- Garancia informovanosti – poskytovanie informácií o nových sw produktoch.
- Garancia možnosti účasti užívateľov na vzdelávacích stretnutiach k problematike IS.

Konzultačné hodiny - konzultačné služby poskytované dodávateľom na základe evidovanej požiadavky objednávateľa.

pracoviská s ASW StaproMEDEA: 8 hodín ročne

Konzultačné hodiny je možné čerpať:
- Riešením konzultácií a požiadaviek objednávateľa zadaných a evidovaných prostredníctvom služby HelpDesk. V prípade požiadavky na vývojové práce sa konzultačné hodiny zamieňajú za vývojové hodiny v pomere 2:1, teda 2 hodiny konzultačných prác = 1 hodina vývojových prác.
- Konzultačnou návštevou v mieste objednávateľa na základe požiadavky zadanej prostredníctvom služby HelpDesk v dohodnutom termíne podľa dohodnutých oblastí, vrátane vypracovania správy protokolu a jeho zaslanie zodpovednej osobe objednávateľa. V prípade vyžiadania osobnej konzultačnej návštevy sú hradené cestovné náklady nad rámec supervízie v zmysle platného cenníka. Rozsah konzultačnej návštevy je 8 hodín.

Aplikačný sw FONS Medix

Dodávateľ sa zaväzuje poskytovať pre podporu ASW FONS Medix v rozsahu modulov a licencií podľa kap. 1, nasledujúce služby:

Základná podpora aplikačného sw FONS Medix - program starostlivosti o aplikáciu zahŕňa:
- Garancia funkčnosti ASW a db prostredia – poskytovanie opravných kódov (hot-fix a patch).
- Garancia rozvoja ASW a db prostredia – poskytovanie update a upgrade.
- Garancia legislatívnych update – poskytovanie legislatívnych upgrade.
- Servisná garancia – garancia dostupnosti servisných služieb.
- Garancia dostupnosti služby HelpDesk – prístup k systému služby HelpDesk Centra podpory zákazníkov
- Garancia podpory prevádzky db prostredia.
- Garancia vybraných služieb:
o zabezpečenie migrácie ASW FONS Medix na vyššiu verziu db prostredia.
- Garancia informovanosti – poskytovanie informácií o nových sw produktoch.
- Garancia možnosti účasti užívateľov na vzdelávacích stretnutiach k problematike IS.

Aplikačný sw FONS Enterprise

Dodávateľ sa zaväzuje poskytovať pre podporu ASW FONS Enterprise v rozsahu modulov a licencií podľa kap. 1, nasledujúce služby:

Základná podpora aplikačného sw FONS Enterprise - program starostlivosti o aplikáciu zahŕňa:
- Garancia funkčnosti ASW a db prostredia – poskytovanie opravných kódov (hot-fix a patch).
- Garancia rozvoja ASW a db prostredia – poskytovanie update a upgrade.
- Garancia legislatívnych update – poskytovanie legislatívnych upgrade.
- Servisná garancia – garancia dostupnosti servisných služieb.
- Garancia dostupnosti služby HelpDesk – prístup k systému služby HelpDesk Centra podpory zákazníkov
- Garancia podpory prevádzky db prostredia.
- Garancia vybraných služieb:
o zabezpečenie migrácie ASW FONS Enterprise na vyššiu verziu db prostredia.
- Garancia informovanosti – poskytovanie informácií o nových sw produktoch.
- Garancia možnosti účasti užívateľov na vzdelávacích stretnutiach k problematike IS.

3. Podpora technických prostriedkov IS

Servery pre ASW

Dodávateľ sa zaväzuje poskytovať pre podporu servery ASW definovaného v kap. 1 nasledujúci služby:

- Servisné služby podľa podmienok programu Základná podpora technických prostriedkov IS
- Preventívne (profylaktické) prehliadky – kontrola funkčnosti, zabezpečenie a optimalizácia prevádzky podľa dohodnutých oblastí, vrátane vypracovania správy – protokolu a jeho zaslanie zodpovednej osobe objednávateľa:
-

DB server ASW StaproMEDEA	1 x ročne
DB server ASW StaproFONS – výkazníctvo SK	1 x ročne
DB server ASW FONS Openlims	1 x ročne
DB server ASW FONS Enterprise	1 x ročne

Príloha č. 2: Zoznam pracovných rolí Dodávateľa

Pracovná rola	Popis
konzultant	školenie a podpora prevádzky informačných systémov, analýzy a návrhy riešení zákazníckych požiadaviek, testovanie a uvedenie sw modulov a funkčností do prevádzky, konzultácie
systémový administrátor	správa virtuálnych serverov v prostredí Microsoft Hyper-V, správa serverov na platforme Microsoft Window Server, Oracle Linux, správa databázových prostredí Microsoft SQL Server a Progress OpenEdge
technik	konfigurácia, spravovanie, diagnostika a kontrola výpočtovej techniky, HW vybavenia, inštalácia a konfigurácia periférií (klávesnice, myši, monitory, tlačiarne, skenery, atď.), oprava / výmena HW komponentov, inštalácia a podpora platformy Microsoft Windows a aplikácii

Príloha č. 3: Minimálny rozsah a špecifikácia bezpečnostných opatrení

Pre oblasť technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 9 Vyhlášky NBÚ č. 362/2018 (ďalej len „Vyhláška NBÚ") v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných PZS, najmä identifikuje technické zraniteľnosti informačných systémov patriacich Dodávateľovi, ktoré Dodávateľ priamo využíva pri poskytovaní služieb PZS prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:

- zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
- zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
- využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje Dodávateľ opatrenia podľa § 10 Vyhlášky NBÚ č. 362/2018 v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných PZS, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:

- riadenie prístupov používateľov k sieťam a IS v súlade s § 12 Vyhlášky NBÚ,
- riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a IS, ktoré Dodávateľ využíva pri poskytovaní služieb PZS, a to najmä využitím nástrojov na ochranu integrity sietí a IS, ktoré sú zabezpečené segmentáciou sietí a IS; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
- povoľovanie prepojenia medzi segmentami a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií,
- zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a IS a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,
- sieťam alebo IS sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete,
- spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov,
- servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu,
- udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
- zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
- blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ako to nastavenie IS umožňuje,
- neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty,
- zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
- implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
- smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
- vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája odo internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

Pre oblasť riadenia prístupov realizuje Dodávateľ opatrenia podľa § 12 Vyhlášky NBÚ č. 362/2018 v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných PZS, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:

- riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu

evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému,

- riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
- riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej: vypracovanie zásad riadenia prístupu k informáciám, riadenie prístupu používateľov, zodpovednosť používateľov, riadenie prístupu k sieťam, prístup k operačnému systému a jeho službám, prístup k aplikáciám, monitorovanie prístupu a používania informačného systému a riadenie vzdialeného prístupu,
- pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a IS,
- zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,
- využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy),
- výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch (min. 1x ročne),
- určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Dodávateľ opatrenia podľa § 14 Vyhlášky NBÚ č. 362/2018 v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných PZS, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:

- oboznámenie sa so štandardmi a postupmi PZS pri riešení kybernetických bezpečnostných incidentov (ďalej len „KBI")a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú najmä minimálne postupy hlásenia KBI voči PZS v súlade s právnymi predpismi, najmä ZoKB a Vyhlášky NBÚ tak, aby mal PZS primeraný čas na splnenie si svojich práv a povinností plynúcich mu z právnych predpisov,
- monitorovanie a analyzovanie udalostí v sieťach a IS, ktoré sú využívané na poskytovanie služieb PZS,
- detegovanie KBI, najmä prostredníctvom nástroja na detekciu KBI, ktorý umožňuje v rámci sietí a IS a medzi sieťami a IS overenie kontrolu prenášaných dát,
- zber relevantných informácií o KBI (najmä, nie len: lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia) a vyhodnocovanie KBI, najmä prostredníctvom nástroja na zber a nepretržité vyhodnocovanie KB udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o KBI, vyhľadávanie a zoskupovanie záznamov súvisiacich s KBI, vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako KBI, revíziu konfigurácie a monitorovaných pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných KBI,
- riešenie zistených KBI a zníženie následkov zistených KBI podľa pokynov PZS,
- vyhodnocovanie spôsobov riešenia KBI po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI v súčinnosti s PZS.

Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Dodávateľ opatrenia podľa § 14 Vyhlášky NBÚ č. 362/2018 v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných PZS, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:

- monitoruje a zaznamenáva činnosti sietí a IS, ktoré zabezpečujú ochranu IS, ktorých správou a prevádzkou bol Dodávateľ poverený a to v súlade s požiadavkami § 15 Vyhlášky NBÚ.

Príloha č. 4: Bezpečnostné politiky PZS

- Politika organizácie bezpečnosti
- Politika riadenia bezpečnostných rizík
- Politika riadenia informačných aktív
- Politika pravidiel správania a dobrej praxe
- Politika riadenia dodávateľských vzťahov
- Politika riadenia vývoja a údržby v oblasti IKT
- Politika riadenia a prevádzky IKT
- Politika súladu
- Politika kontinuity procesov a činností
- Politika riadenia bezpečnostných incidentov

Príloha č. 5: Zoznam schválených subdodávateľov

Bez subdodávateľov.