Príloha č. 1

ZMLUVA O DIELO

*uzatvorená podľa ust. § 536 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len "**Obchodný zákonník**"), ust. § 65 a nasl. zákona č. 185/2015 Z. z. Autorského zákona v znení neskorších predpisov (ďalej len "**Autorský zákon**") a v súlade so zákonom č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zmluva**")*

Zmluvné strany:

Objednávateľ:	**Národný endokrinologický a diabetologický ústav n.o.**
Sídlo:	Kollárová 282/3, 034 91 Ľubochňa
Štatutárny orgán:	JUDr. Igor Koval, riaditeľ
IČO:	37 983 687
DIČ:	2022052164
Bank. spojenie:	ČSOB a.s.
IBAN:	SK 3775000000004002660924
registrovaná:	Okresný úrad Žilina

(ďalej len „**Objednávateľ**")

a

Zhotoviteľ:	**iServices s. r. o.**
Sídlo:	Zadunajská cesta 8 851 01 Bratislava
Štatutárny orgán:	Ing. Pavol Šimák, konateľ
IČO:	43872930
DIČ:	2022500524
IČ DPH:	SK 2022500524
Bank. spojenie:	Tatra banka, a.s.
IBAN:	SK4411000000002622819087
zapísaný:	Obchodný register Mestského súdu Bratislava III, oddiel: Sro, vložka č. 49450/B

(ďalej len „**Zhotoviteľ**")
(Objednávateľ a Zhotoviteľ spolu ďalej len ako „**Zmluvné strany**")

Čl. I
Úvodné ustanovenia

1.1 Táto Zmluva sa uzatvára ako výsledok verejného obstarávania s názvom „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach - Národný endokrinologický a diabetologický ústav" v zmysle zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov (ďalej len „**Zákon o verejnom obstarávaní**"). Objednávateľ na obstaranie predmetu tejto

Zmluvy použil postup verejného obstarávania – zákazku s nízkou hodnotou podľa ust. § 117 Zákona o verejnom obstarávaní.

1.2 Táto Zmluva je realizovaná na základe uzatvorenej Zmluvy o poskytnutí nenávratného finančného príspevku Z311071CGU7 medzi Objednávateľom ako prijímateľom a Ministerstvom dopravy Slovenskej republiky (ďalej len „**Riadiaci orgán**") v zastúpení Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „**Sprostredkovateľský orgán**") ako poskytovateľom (ďalej len „**Poskytovateľ**"), zo dňa 19.04.2023 (ďalej len „**Zmluva o poskytnutí NFP**").

1.3 Objednávateľ je poskytovateľom zdravotnej starostlivosti a zároveň prijímateľom nenávratného finančného príspevku na realizáciu aktivít projektu bližšie špecifikovaného v tomto bode tohto článku Zmluvy, ktorý je predmetom schválenej žiadosti o nenávratný finančný príspevok:

Názov projektu:	Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach - Národný endokrinologický a diabetologický ústav
Kód projektu v ITMS2014+:	311071CGU7
Výzva - kód Výzvy:	OPII-2022/7/20-DOP
Použitý systém financovania:	predfinancovanie, refundácia, kombinácia týchto systémov

(ďalej len „**Projekt**").

1.4 Zhotoviteľ je podľa Zákona o verejnom obstarávaní uchádzačom, ktorý predložil ponuku, a ktorý bol vyhodnotený ako úspešný uchádzač a jeho ponuka bola prijatá.

1.5 Zhotoviteľ vyhlasuje, že je odborne spôsobilou osobou, ktorá disponuje kapacitami s potrebnými znalosťami, praktickými skúsenosťami v oblasti informačnej a kybernetickej bezpečnosti, ktoré je možné v danej oblasti predpokladať a technickými možnosťami na riadne a včasné zhotovenie diela podľa podmienok dohodnutých v tejto Zmluve.

1.6 Zhotoviteľ ďalej vyhlasuje, že disponuje všetkými oprávneniami požadovanými príslušnými orgánmi a v zmysle príslušných právnych predpisov potrebnými na vykonanie diela.

Čl. II
Predmet a účel Zmluvy

2.1 Predmetom tejto Zmluvy je záväzok Zhotoviteľa na svoje náklady a svoje nebezpečenstvo vykonať a dodať za cenu a podmienok dohodnutých ďalej v tejto Zmluve riadne a včas pre Objednávateľa obsah Projektu „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach - Národný endokrinologický a diabetologický ústav" pozostávajúci z nasledovných častí:

- Analýza a dizajn,
- Nákup technických prostriedkov, programových prostriedkov a služieb,
- Implementácia a testovanie,

- Nasadenie.

(ďalej len „**Dielo**").

2.2 Predmetom tejto Zmluvy je aj záväzok Objednávateľa Dielo prevziať a zaplatiť za jeho vykonanie dohodnutú cenu podľa čl. VIII tejto Zmluvy. Dielo bude vykonané v jednotlivých častiach ako sú tieto definované v bode 2.1 tohto článku Zmluvy a musí zodpovedať Technickej špecifikácii. Jeho súčasťou musí byť i dodanie, resp. zabezpečenie poskytnutia licencií potrebných na jeho riadne užívanie

2.3 Účelom tejto Zmluvy je zabezpečenie vytvorenia Diela, ktoré bude v plnom rozsahu zodpovedať všetkým funkčným, technickým a legislatívnym požiadavkám Objednávateľa uvedeným v tejto Zmluve, vo Výzve na predloženie cenovej ponuky (ďalej len „**Výzva**") a ktorý bude v spojení s ostatnými službami poskytnutými Zhotoviteľom na základe tejto Zmluvy spôsobilým nástrojom na plnenie úloh Objednávateľa požadovaných osobitnými predpismi a cieľov deklarovaných v prílohe č. 1 tejto Zmluvy, resp. v ďalších dokumentoch, na ktoré táto Zmluva odkazuje.

2.4 Podrobná špecifikácia obsahu, rozsahu a spôsobu vykonania Diela je uvedená v tejto Zmluve, vo Výzve, ktorej súčasťou je okrem iného Opis predmetu zákazky, ktorý tvorí aj prílohu č. 1 tejto Zmluvy, ako i v ďalších dokumentoch, na ktoré táto Zmluva odkazuje (ďalej len „**Technická špecifikácia**"), ktoré obsahujú najmä:

a) podrobný opis Diela,

b) technické požiadavky na Dielo a jeho funkcionalitu,

c) požiadavky na výkonnosť Diela,

d) ďalšie osobitné požiadavky Objednávateľa na dodávané Dielo.

2.5 Zhotoviteľ zrealizuje predmet Zmluvy prostredníctvom svojich nasledujúcich odborníkov spĺňajúcich kritériá uvedené v prílohe č. 5 tejto Zmluvy „Zoznam odborníkov a požiadaviek na odborníkov" (ďalej len „**príloha č. 5**"):

a) IT analytik,

b) IT konzultant,

c) Odborník pre IT dohľad/ Quality Assurance,

d) Špecialista pre bezpečnosť IT.

2.6 Mená odborníkov Zhotoviteľa podľa bodu 2.5 a 2.6 tejto Zmluvy sú uvedené v prílohe č. 5. Zhotoviteľ môže zmeniť konkrétneho odborníka uvedeného v prílohe č. 5 za iného, alebo doplniť nového odborníka na plnenie predmetu Zmluvy, ak spĺňa požiadavky uvedené v prílohe č. 5 pre tento druh odborníka a ak túto zmenu schváli oprávnená osoba Objednávateľa uvedená v bode 9.1 tejto Zmluvy. Zmenu podľa tohto bodu uskutočnia Zmluvné strany formou dodatku k Zmluve.

Čl. III
Práva a povinnosti Zmluvných strán

3.1 Zhotoviteľ sa týmto zaväzuje vykonať Dielo v súlade s požiadavkami Objednávateľa uvedenými v tejto Zmluve, ako aj technickými a inými špecifikáciami a požiadavkami v rozsahu uvedenom v Opise predmetu zákazky - príloha č. 1 tejto Zmluvy, s odbornou

starostlivosťou a v súlade s legislatívou platnou v oblasti informačnej a kybernetickej bezpečnosti, ktorá sa vzťahuje na Objednávateľa.

3.2 Zhotoviteľ sa zaväzuje:

a) vykonať Dielo riadne, včas, na svoje náklady a na svoje nebezpečenstvo, v súlade s požiadavkami Objednávateľa uvedenými v tejto Zmluve, vrátane jej príloh a vo Výzve, v Opise predmetu zákazky a ďalších dokumentoch verejného obstarávania,

b) postupovať s odbornou starostlivosťou, čestne, svedomito, hospodárne s využitím dostupných odborných znalostí a skúseností v súlade s jemu známymi záujmami Objednávateľa,

c) pri plnení povinností podľa tejto Zmluvy dodržiavať pokyny a podklady Objednávateľa, ktoré nie sú v rozpore s ustanoveniami tejto Zmluvy,

d) pri plnení tejto Zmluvy dodržiavať vnútorné predpisy Objednávateľa, na ktoré ho Objednávateľ upozorní, najmä bezpečnostnú politiku,

e) vykonať Dielo svojimi zamestnancami, resp. externými spolupracovníkmi, ktorí majú dostatočné skúsenosti a odbornú znalosť, a to najmä s využitím osôb/expertov, prostredníctvom ktorých preukazoval splnenie podmienok účasti v zadávaní zákazky na uzavretie tejto Zmluvy, a ktorí sa budú aktívne podieľať na plnení predmetu Zmluvy a budú garantovať kvalitu a odbornosť realizovaných činností a výstupov plnenia predmetu Zmluvy počas celej doby trvania Zmluvy,

f) bez zbytočného odkladu upozorniť Objednávateľa na nevhodnú povahu pokynov a/alebo podkladov poskytnutých mu Objednávateľom, ak mohol túto nevhodnosť zistiť pri vynaložení odbornej starostlivosti. V prípade nevhodných pokynov prerušiť vykonanie Diela, alebo jeho časti, až do doby odstránenia alebo nahradenia nesprávnych alebo nevhodných pokynov,

g) bezodkladne písomne informovať Objednávateľa o každom prípadnom omeškaní, či iných skutočnostiach, ktoré by mohli ohroziť riadne a včasné vykonanie Diela, alebo jeho časti, pričom bezodkladne sa rozumie do **24 hodín** odkedy sa o nich Zhotoviteľ dozvedel,

h) zodpovedať za to, že Dielo neobsahuje žiadne Objednávateľom nevyžiadané alebo neschválené funkcie a vlastnosti,

i) poskytnúť Oprávnenej osobe Objednávateľa alebo inej poverenej osobe Objednávateľa informáciu o stave plnenia Zmluvy alebo informáciu súvisiacu s plnením na základe žiadosti Objednávateľa, lehota na vybavenie takejto písomnej požiadavky je maximálne **5 dní**,

j) až do odovzdania a prevzatia Diela ako celku udržiavať jeho jednotlivé časti už nasadené do prevádzky v súlade s dodanou administrátorskou dokumentáciou a poskytovať Objednávateľovi nevyhnutnú súčinnosť za účelom používania nasadených častí Diela,

k) strpieť výkon kontroly/auditu súvisiaceho s plnením tejto Zmluvy kedykoľvek počas platnosti a účinnosti Zmluvy o poskytnutí NFP, a to zo strany oprávnených osôb na výkon tejto kontroly/auditu v zmysle príslušných právnych predpisov Slovenskej republiky a Európskej únie, najmä zákona č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vyššie uvedenej Zmluvy o poskytnutí NFP a jej príloh, vrátane jej všeobecných zmluvných podmienok, a poskytnúť im riadne a včas všetku

potrebnú súčinnosť,

l) umožniť Objednávateľovi vykonať audit bezpečnosti Diela vrátane informačných systémov a prostredia Zhotoviteľa používaného pri plnení Diela na overenie miery dodržiavania bezpečnostných požiadaviek relevantných právnych predpisov a zmluvných požiadaviek, ako i prijať opatrenia na zabezpečenie nápravy zistení z auditu bezpečnosti informačných systémov,

m) poskytnúť Objednávateľovi a jemu nadriadeným orgánom plnú súčinnosť pri riešení bezpečnostného incidentu a vyšetrovaní bezpečnostnej udalosti, ktoré súvisia s plnením tejto Zmluvy alebo jej predmetom,

n) poskytnúť Objednávateľovi kompletnú dokumentáciu dodaného Diela vrátane administrátorských prístupov,

o) zabezpečiť súlad dodávaného Diela so zákonom č. 95/2019 Z. z., o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon o ITVS**"),

p) zabezpečiť súlad dodávaného Diela so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon o KyB**").

q) zabezpečiť súlad dodávaného Diela so **Zákonom o eGovernmente** č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len **Zákon o eGovernmente**),

r) dodržiavať ustanovenia a riadiť sa pri vykonávaní Diela najmä vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov v znení neskorších predpisov, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, vyhláškou Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

3.3 Objednávateľ sa zaväzuje:

a) zabezpečiť Zhotoviteľovi v primeranom rozsahu potrebné informácie a prípadné konzultácie k nastavenému procesu Objednávateľa, ak bude Objednávateľ takými informáciami disponovať,

b) za predpokladu dodržania bezpečnostných a prípadných ďalších predpisov Objednávateľa zabezpečiť pre Oprávnenú osobu Zhotoviteľa potrebné oprávnenia a prístupy nevyhnutné na plnenie tejto Zmluvy,

c) za predpokladu dodržania bezpečnostných a prípadných ďalších predpisov Objednávateľa sprístupniť technickú, komunikačnú a systémovú infraštruktúru pre vykonanie Diela, a podľa potreby vzdialeného prístupu dohodnutou technológiou zabezpečiť Zhotoviteľovi na jeho žiadosť včas prístup ku všetkým zariadeniam, ku ktorým je jeho prístup potrebný pre vykonanie Diela,

d) zabezpečiť v nevyhnutnom rozsahu prítomnosť Oprávnenej osoby Objednávateľa v mieste plnenia Zmluvy v sídle Objednávateľa (prípadne na inom mieste vykonania

Diela alebo jeho časti, ak je to tak dohodnuté v Zmluve) na splnenie záväzku Zhotoviteľa v zmysle tejto Zmluvy,

e) poskytnúť Zhotoviteľovi potrebnú súčinnosť pri plnení predmetu Zmluvy, najmä poskytnúť Zhotoviteľovi na požiadanie všetky podklady, ktoré sú podľa Zhotoviteľa nevyhnutné pre zhotovenie Diela. S poskytnutými podkladmi Zhotoviteľ nie je oprávnený nakladať inak, ako za účelom zhotovenia Diela, najmä ich sprístupniť tretím osobám, a to ani po zániku/zrušení Zmluvy,

f) Objednávateľ je povinný informovať Zhotoviteľa o všetkých skutočnostiach, ktoré sú významné pre splnenie povinností Zmluvných strán podľa tejto Zmluvy, v súvislosti s vykonaním Diela podľa tejto Zmluvy alebo o dôvodoch, ktoré Objednávateľovi bránia riadne a včas splniť svoje povinnosti podľa tejto Zmluvy.

Čl. IV
Miesto a termíny vykonania Diela

4.1 Zhotoviteľ vykoná Dielo u Objednávateľa a pre Objednávateľa. Ak sa Zmluvné strany nedohodnú inak, miestom vykonania Diela je sídlo Objednávateľa. Ak to technické podmienky umožňujú a ak sa Zmluvné strany na tom dohodnú, Zhotoviteľ môže plniť Dielo aj prostredníctvom vzdialeného prístupu.

4.2 **Zmluvné strany sa dohodli, že Zhotoviteľ je povinný dodať predmet Zmluvy podľa tejto Zmluvy najneskôr do 31.12.2023**, pričom je povinný dodržiavať harmonogram aktivít, ktorý si Zmluvné strany dohodnú na úvodnom stretnutí, a ktorý bude vychádzať z harmonogramu realizácie Projektu existujúceho v súvislosti so Zmluvou o poskytnutí NFP – príloha č. 3 tejto Zmluvy (ďalej len „**Harmonogram**"). V každom prípade však platí, že konečný termín odovzdania a prevzatia celého Diela, vrátane všetkých jeho častí, resp. poslednej z jeho častí, je najneskôr do 31.12.2023 (ďalej len „**Konečný termín**").

4.3 Úvodné stretnutie Zmluvných strán k predmetu plnenia Zmluvy sa zrealizuje v dohodnutom termíne v sídle Objednávateľa, a to najneskôr do 5 pracovných dní odo dňa nadobudnutia účinnosti tejto Zmluvy. Zhotoviteľ je povinný sa na stretnutí zúčastniť.

4.4 Ak preukázateľné omeškanie Objednávateľa s poskytnutím súčinnosti, ktorá je potrebná na vykonanie Diela, alebo akejkoľvek jeho časti, Zhotoviteľom podľa tejto Zmluvy, spôsobí nedodržanie Harmonogramu a/alebo nedodržanie Konečného termínu, Zhotoviteľ nie je z tohto dôvodu v omeškaní s vykonaním Diela, alebo jeho časti, v rozsahu omeškania Objednávateľa. Lehota na vykonanie Diela sa automaticky predlžuje o čas omeškania Objednávateľa s poskytnutím súčinnosti. Zmluvné strany sa dohodli, že najneskôr druhý pracovný deň po vzniku omeškania Objednávateľa Zhotoviteľ písomne upozorní Oprávnenú osobu Objednávateľa na konkrétne vymedzenú povinnosť súčinnosti, s ktorou je Objednávateľ v omeškaní, a toto upozornenie bude pravidelne písomne opakovať najmenej 1x za 3 pracovné dni až do dosiahnutia nápravy. V prípade omeškania so zhotovením jednotlivých častí Diela, ktoré bude preukázateľne spôsobené Objednávateľom, sa lehota na plnenie primerane predĺži dohodou oboch Zmluvných strán, najmenej však o dobu omeškania spôsobeného Objednávateľom.

4.5 Zmluvné strany sa dohodli, že akúkoľvek zmenu týkajúcu sa miesta a/alebo Konečného termínu vykonania Diela ako celku alebo jeho časti, je možné uskutočniť na základe

uzatvorenia písomného dodatku k tejto Zmluve. Takýto dodatok sa uzatvára v súlade s ust. § 18 Zákona o verejnom obstarávaní.

Čl. V
Odovzdanie Diela

5.1 Kompletnosť odovzdaného Diela v priestoroch Objednávateľa bude potvrdená na základe preberacieho konania, pričom táto skutočnosť bude osvedčená vystavením Protokolu o prebierke diela pred skúšobnou prevádzkou, ktorý bude potvrdený zástupcami oboch Zmluvných strán bezodkladne po odovzdaní Diela v mieste plnenia podľa čl. IV tejto Zmluvy. Protokol bude vyhotovený dvojmo, pre každú Zmluvnú stranu 1 vyhotovenie.

5.2 Zhotoviteľ sa zaväzuje Objednávateľovi odovzdať do užívania kompletné Dielo, ktoré bude plne funkčné pre účely a potreby Objednávateľa, spôsobilé na spustenie do prevádzky podľa podmienok dohodnutých v tejto Zmluve a bude spĺňať špecifikácie podľa tejto Zmluvy, vrátane zaškolenia zamestnancov Objednávateľa a s tým súvisiacich úkonov.

5.3 Zhotoviteľ je povinný dodať Objednávateľovi súčasne s dodaním Diela dokumentáciu minimálne v rozsahu:

a) zdrojové kódy, pokiaľ budú v rámci Diela vytvorené,

b) technickú dokumentáciu v slovenskom jazyku v elektronickej forme, ktorá bude obsahovať: postup skompilovania aplikácie, dátový model informačného systému, popis integračnej, aplikačnej a technickej architektúry, väzby na iné systémy, popis tokov dát,

c) prevádzkovú dokumentáciu v slovenskom jazyku v elektronickej forme, ktorá bude obsahovať: konfiguráciu systémového SW, serverov a pracovných staníc, popis mechanizmu riadenia prístupu užívateľov k dátam a k funkciám aplikácie, popis procedúr pre zálohovanie a obnovu dát, popis použitých a navrhovaných technických číselníkov, popis integrácie nových informačných technológií,

d) užívateľskú dokumentáciu v slovenskom jazyku v písomnej forme v počte 2 kusov a v elektronickej forme, ktorá bude obsahovať: popis počítačového programu a jeho funkcií, postupy a úkony potrebné pre riadne užívanie počítačového programu.

5.4 Zhotoviteľ najneskôr 3 dni pred plánovaným odovzdaním Diela bude Objednávateľa o tejto skutočnosti písomne informovať, pričom Objednávateľ je v tejto lehote povinný vykonať preberacie konanie Diela. Vykonanie tohto preberacieho konania bude osvedčené vystavením Protokolu o prebierke Diela pred skúšobnou prevádzkou. Objednávateľ prevezme len také Dielo, ktoré spĺňa požadované parametre pre účely a potreby Objednávateľa podľa podmienok dohodnutých v tejto Zmluve.

5.5 Pre vylúčenie pochybností Zmluvné strany uvádzajú, že skúšobnou prevádzkou sa rozumie prechodné obdobie testovania a odstraňovania nájdených vád dodaného Diela podľa požadovaných parametrov v zmysle prílohy č. 1 tejto Zmluvy. Doba trvania skúšobnej prevádzky bude 30 dní odo dňa spustenia do bežnej prevádzky. Skúšobná prevádzka bude prebiehať v pracovných dňoch od 6:00 hod. do 16:00 hod.

5.6 Po ukončení skúšobnej prevádzky bude vykonaná konečná prebierka Diela. Splnenie podmienok potrebných pre začatie trvalej (ostrej) prevádzky bude osvedčené vystavením Protokolu o konečnej prebierke, ktorý bude potvrdený zástupcami oboch Zmluvných strán.

5.7 Zmluvné strany sa dohodli, že v Protokole o konečnej prebierke bude uvedený podrobný odpočet splnenia jednotlivých aktivít spolu s hárkom pracovných výstupov, presný názov softvérov vrátane ich autora a výrobcu, zoznam a špecifikácia udelených licencií (vrátane vyhlásenia o udelení licencií), doklad alebo čestné vyhlásenie o tom, že Zhotoviteľ je oprávnený udeliť licenciu Objednávateľovi na celé požadované obdobie (t.j. min. na 24 mesiacov), informácia o zaškolených zamestnancoch Objednávateľa a dátume jeho vykonania, súpis odovzdanej dokumentácie, potvrdenie o vykonaní funkčnej skúšky. V Protokole o konečnej prebierke musí byť uvedený deň ukončenia implementácie a odovzdanie plnenia do ostrej prevádzky. Protokol musí byť podpísaný oprávnenými zástupcami oboch Zmluvných strán.

5.8 Objednávateľ je oprávnený odmietnuť prevzatie Diela najmä v prípade zjavných vád, nedostatočnej kvality predmetu plnenia, nedostatočnej dokumentácie, v prípade, ak Dielo nespĺňa požadované špecifikácie, či kvalitatívne vlastnosti, ak Dielo nie je kompletné alebo bolo dodané v rozpore s touto Zmluvou, ak neprebehla skúšobná prevádzka alebo ak zo skúšobnej prevádzky sú zjavné vady (ďalej len „**vady**"). V prípade, ak Objednávateľ odmietne Dielo prevziať, oznámi túto skutočnosť Zhotoviteľovi písomne spolu s uvedením dôvodov odmietnutia a stanovením lehoty na odstránenie vád Diela.

5.9 V prípade, ak sa Objednávateľ napriek vadám uvedeným v predchádzajúcom bode 5.8 tejto Zmluvy rozhodne Dielo prevziať, má sa zato, že Objednávateľ prevzal Dielo „**s výhradou do čiastočnej prevádzky**". Vady Diela spíšu Zmluvné strany v Protokole o odstránení vád, v ktorom súčasne Objednávateľ stanoví lehotu na ich odstránenie (nie kratšiu ako 10 dní na vykonanie nápravy). Prípadné vady Diela je Zhotoviteľ v tomto prípade povinný odstrániť bezodkladne, najneskôr však do konca stanovenej lehoty, pričom ich odstránenie bude osvedčené v Protokole o odstránení vád, ktorý bude potvrdený zástupcami oboch Zmluvných strán. V prípade, ak Zhotoviteľ neodstráni uvedené vady v lehote určenej v predchádzajúcej vete tohto bodu Zmluvy, je Objednávateľ oprávnený si u Zhotoviteľa nárokovať zmluvnú pokutu vo výške 100 EUR za každý začatý deň omeškania. Nárok na náhradu škody tým nie je dotknutý.

5.10 V prípade, ak Objednávateľ odmietne prevziať Dielo na základe Protokolu o prebierke diela pred skúšobnou prevádzkou alebo Protokolu o konečnej prebierke z dôvodu, že Dielo nespĺňa požadované parametre v zmysle prílohy č. 1 tejto Zmluvy, je Objednávateľ oprávnený poskytnúť Zhotoviteľovi primeranú lehotu nie kratšiu ako 10 dní na vykonanie nápravy. V prípade, ak Zhotoviteľ nevykoná nápravu v uvedenej lehote, je Objednávateľ oprávnený odstúpiť od Zmluvy a nárokovať si od Zhotoviteľa zmluvnú pokutu vo výške 5 000 EUR. Nárok na náhradu škody tým nie je dotknutý.

5.11 Po odstránení vád, ktoré malo Dielo pri prevzatí podľa predchádzajúceho bodu tejto Zmluvy, je Zhotoviteľ povinný vykonať opätovne skúšobnú prevádzku, s výnimkou prípadov, kedy sa objektívne skúšobná prevádzka nevyžaduje.

5.12 Po odstránení vád sa spíše Protokol o odstránení vád, ktorý bude podpísaný oboma Zmluvnými stranami.

Čl. VI
Autorské práva a udelenie licencie

6.1 V prípade, že Dielo alebo ktorákoľvek jeho časť, ktorého vykonanie je predmetom tejto Zmluvy, spĺňa náležitosti autorského diela podľa Autorského zákona, týmto udeľuje Zhotoviteľ Objednávateľovi súhlas používať toto Dielo ako licenciu výhradnú, časovo neobmedzenú, územne neobmedzenú, v neobmedzenom rozsahu (najmä na neobmedzený počet zariadení a užívateľov) a na všetky spôsoby použitia, najmä v súlade s ust. § 19 ods. 4 Autorského zákona.

6.2 Zhotoviteľ zároveň touto Zmluvou udeľuje dňom protokolárneho odovzdania predmetu plnenia Objednávateľovi oprávnenie udeliť tretej osobe súhlas na použitie Diela v rozsahu udelenej licencie podľa tejto Zmluvy, t. j. sublicencie a tiež súhlas na postúpenie licencie.

6.3 Zmluvné strany sa dohodli, že odplata za udelenie licencií je zahrnutá v celkovej cene za Dielo.

6.4 Vyhlásenie o udelených licenciách bude súčasťou Protokolu o konečnej prebierke.

6.5 **Licencie na používanie softvéru podľa tejto Zmluvy je Zhotoviteľ povinný udeliť na obdobie min. 24 mesiacov, počnúc dňom protokolárneho odovzdania predmetu plnenia.**

6.6 Udelenie licencií sa vzťahuje aj na všetky budúce aktualizácie, doplnenia, opravy a úpravy softvéru, pokiaľ takéto aktualizácie, doplnenia, opravy a úpravy sú nevyhnutné pre funkčnosť softvéru.

6.7 Zhotoviteľ vyhlasuje, že je nositeľom všetkých autorských práv k Dielu, resp. má všetky potrebné oprávnenia na udelenie licencie na používanie Diela Objednávateľovi podľa tohto článku Zmluvy a Dielo nebude pri jeho odovzdaní Objednávateľovi zaťažené akýmikoľvek právami tretích osôb. V prípade, ak by sa na Diele podieľali autorsky aj iné osoby ako Zhotoviteľ, ten je povinný zabezpečiť si oprávnenie s Dielom nakladať a oprávnenie poskytovať licenciu na jeho použitie v takom rozsahu, v akom tak robí touto Zmluvou.

6.8 V prípade, ak sa po uzatvorení tejto Zmluvy preukáže neoprávnené alebo nedostatočné/neúplné poskytnutie licenčných práv Objednávateľovi, Zhotoviteľ sa zaväzuje bez zbytočného odkladu na vlastné náklady zabezpečiť Objednávateľovi bezodplatné udelenie licencie k Dielu v plnom rozsahu tak, aby používaním autorských diel Objednávateľom na základe takéhoto súhlasu nedochádzalo k akýmkoľvek zásahom do práv duševného vlastníctva tretích osôb.

6.9 Zhotoviteľ sa zaväzuje, že ak v budúcnosti vznikne potreba udeliť Objednávateľovi licenciu na Dielo z dôvodu jeho aktualizácie, upgradu alebo údržby systému a pod., zabezpečí pre Objednávateľa tieto licencie bezodplatne.

6.10 Zhotoviteľ zodpovedá Objednávateľovi za porušenie autorských práv a duševného vlastníctva pri používaní Diela na účely a v rozsahu dohodnutom v tejto Zmluve. Zhotoviteľ je povinný nahradiť Objednávateľovi škodu a náklady, ktoré vzniknú ako

dôsledok uplatňovania nárokov tretích strán k Dielu alebo jeho časti založených na autorských právach, právach duševného vlastníctva.

6.11 V prípade, ak na základe plnenia tejto Zmluvy Objednávateľ nadobudne majetok, ktorý je predmetom duševného vlastníctva, Objednávateľ je oprávnený v rozsahu, v akom to nevylučujú všeobecne-záväzné právne predpisy kogentnej povahy, použiť takéto dielo alebo vykonávať práva z priemyselného vlastníctva v súvislosti s predmetom plnenia tejto Zmluvy na základe vecne, miestne a časovo neobmedzenej, výhradnej, trvalej, bez osobitného súhlasu Zhotoviteľa prevoditeľnej, v písomnej forme vyjadrenej licencie (súhlasu), ktorej (ktorého) obsahom nebudú žiadne obmedzenia Objednávateľa pri používaní diela alebo pri vykonávaní iného práva duševného vlastníctva (vrátane priemyselného vlastníctva), ktoré by vyžadovali dodatočný alebo osobitný súhlas autora na uplatňovanie majetkových práv k dielu alebo dodatočný alebo osobitný súhlas majiteľa práva na vykonávanie iného práva duševného vlastníctva (vrátane priemyselného vlastníctva), v dôsledku čoho bude Objednávateľ oprávnený všetky práva duševného vlastníctva nerušene a neobmedzene aplikovať, užívať, požívať, šíriť, rozmnožovať, prepracovať, spracovať, adaptovať, ďalej vyvíjať a chrániť a nakladať s nimi na ľubovoľný účel, prípadne v rovnakom rozsahu ich previesť či poskytnúť čiastočne alebo v celosti tretej osobe, pričom takáto licencia sa poskytuje bezodplatne a bezpodmienečne.

6.12 Udelenie licencie nemožno zo strany Zhotoviteľa vypovedať a jej účinnosť trvá aj po skončení účinnosti tejto Zmluvy.

6.13 Práva získané v rámci plnenia tejto Zmluvy prechádzajú aj na prípadného právneho nástupcu Objednávateľa. Prípadná zmena v osobe Zhotoviteľa (napr. právne nástupníctvo) nebude mať vplyv na oprávnenia udelené v rámci tejto Zmluvy Zhotoviteľom Objednávateľovi.

Čl. VII
Plnenie subdodávateľmi a zápis v registri partnerov verejného sektora

7.1 Údaje o všetkých známych subdodávateľoch a údaje o osobe oprávnenej konať za subdodávateľa v súlade s ust. § 41 ods. 3 Zákona o verejnom obstarávaní uvádza Zhotoviteľ v prílohe č. 2 tejto Zmluvy, ktorá tvorí jej neoddeliteľnú súčasť.

7.2 Zhotoviteľ je povinný bezodkladne Objednávateľovi písomne oznámiť akúkoľvek zmenu údajov o subdodávateľovi, ako aj zmenu subdodávateľa. Zhotoviteľ je povinný Objednávateľovi 10 pracovných dní pred plánovanou zmenou subdodávateľa písomne oznámiť údaje o navrhovanom novom subdodávateľovi (vrátane informácie o jeho zástupcovi) tak, ako sú požadované v prílohe č. 2 tejto Zmluvy.

7.3 Pokiaľ Zhotoviteľ použije na plnenie svojich záväzkov podľa tejto Zmluvy subdodávateľa, zodpovedá Objednávateľovi tak, akoby záväzok plnil sám. Zhotoviteľ zodpovedá za poučenie a oboznámenie subdodávateľov so všetkými povinnosťami, ktoré mu ako Zhotoviteľovi vyplývajú z tejto Zmluvy.

7.4 Body 7.1 až 7.2 tejto Zmluvy platia aj v prípade, ak v čase uzatvorenia tejto Zmluvy Zhotoviteľ v prílohe č. 2 neuviedol žiadneho subdodávateľa.

7.5 V prípade porušenia povinností uvedených v bodoch 7.1 a 7.3 tejto Zmluvy je Objednávateľ oprávnený odstúpiť od tejto Zmluvy a uplatniť si zmluvnú pokutu vo výške

1 000 EUR za každé porušenie ktorejkoľvek z vyššie uvedených povinností, a to aj opakovane.

7.6 Ak úspešný uchádzač - Zhotoviteľ nemá v úmysle zadať časti plnenia predmetu tejto Zmluvy subdodávateľom, túto skutočnosť uvedie v prílohe č. 2.

7.7 Ak sa na Zhotoviteľa a/alebo jeho subdodávateľov vzťahuje povinnosť zapisovať sa do registra partnerov verejného sektora podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon o RPVS**"), Zhotoviteľ je povinný dodržať túto povinnosť počas celej doby platnosti a účinnosti tejto Zmluvy, pričom sa zaväzuje rovnako zabezpečiť plnenie tejto povinnosti všetkými jeho subdodávateľmi. V prípade, ak počas plnenia tejto Zmluvy dôjde k právoplatnému výmazu niektorého subdodávateľa z registra partnerov verejného sektora, je Zhotoviteľ povinný okamžite ukončiť plnenie tejto Zmluvy prostredníctvom takéhoto subdodávateľa. Porušenie tejto povinnosti sa považuje za podstatné porušenie Zmluvy a je dôvodom, ktorý oprávňuje Objednávateľa na odstúpenie od Zmluvy.

Čl. VIII
Cena a platobné podmienky

8.1 Objednávateľ je povinný zaplatiť Zhotoviteľovi za riadne a včasné vykonanie Diela na základe tejto Zmluvy cenu dojednanú v zmysle zákona NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky MF SR č. 87/1996 Z. z., ktorou sa vykonáva zákon č. 18/1996 Z. z. v znení neskorších predpisov v celkovej sume **173 959,70 EUR** (slovom: jednostosedemdesiattritisícdeväťstopäťdesiatdeväť eur sedemdesiat centov) s DPH (ďalej len „**Cena Diela**").

8.2 Zmluvné strany sú viazané výškou Ceny Diela uvedenej v tejto Zmluve, ktorá je výsledkom ponuky Zhotoviteľa vo verejnom obstarávaní. Cena Diela predstavuje odplatu za splnenie všetkých zmluvných záväzkov Zhotoviteľa vyplývajúcich z tejto Zmluvy a zahŕňa všetky náklady a výdavky Zhotoviteľa na riadne a včasné vykonanie Diela, resp. jeho jednotlivých častí podľa tejto Zmluvy, ako aj cenu za udelenie autorských majetkových práv k Dielu alebo jeho súčastiam podľa čl. VI tejto Zmluvy, najmä za licencie, a predstavuje konečnú cenu za vykonanie Diela a Zhotoviteľ nie je oprávnený nárokovať si žiadne ďalšie náklady a navýšenia ceny.

8.3 Cena Diela sa skladá z cien za jednotlivé časti Diela v súlade s prílohu č. 4 tejto Zmluvy – Návrh na plnenie kritérií (rozpočet predložený v ponuke uchádzača vo verejnom obstarávaní).

8.4 Zhotoviteľovi vzniká nárok na zaplatenie Ceny Diela po riadnom odovzdaní a prevzatí Diela (ako celku) a všetkých služieb s tým súvisiacich v súlade s touto Zmluvou, pričom predpokladom pre vznik nároku na zaplatenie Ceny Diela je podpísanie Protokolu o konečnej prebierke.

8.5 Faktúra musí obsahovať náležitosti daňového dokladu. V prípade, že daňový doklad nebude obsahovať tieto náležitosti, Objednávateľ je oprávnený ho vrátiť na doplnenie a prepracovanie. V takom prípade sa preruší lehota splatnosti a nová lehota splatnosti pre Objednávateľa začne plynúť dňom prevzatia novej, doplnenej faktúry.

8.6 Lehota splatnosti faktúr je 60 dní odo dňa ich doručenia Objednávateľovi. Úhrada faktúr sa uskutočňuje bezhotovostným platobným stykom na účet Zhotoviteľa uvedený v záhlaví tejto Zmluvy. Úhradou sa rozumie pripísanie sumy na účet Zhotoviteľa s uvedením správneho variabilného symbolu uvedeného na faktúre.

8.7 Objednávateľ zálohy, ani preddavky z Ceny Diela neposkytuje.

8.8 Zhotoviteľ je oprávnený požadovať len také zmeny dohodnutej ceny, ktoré vyplývajú zo zmien daňových predpisov *(zmena výšky zákonnej sadzby DPH)*. Úprava Ceny diela sa bude riešiť rokovaním Zmluvných strán, výsledkom ktorého bude písomný dodatok k Zmluve.

Čl. IX
Oprávnené osoby a komunikácia

9.1 Zmluvné strany sa dohodli, že osobami oprávnenými komunikovať vo veciach týkajúcich sa záležitostí súvisiacich s plnením tejto Zmluvy (najmä týkajúcich sa zhotovenia Diela, alebo jeho častí) sú:

Oprávnená osoba Zhotoviteľa:

Zhotoviteľ:	Ing. Pavol Šimák
E-mail:	pavol.simak@iservices.sk
Tel. kontakt:	+421 903 220 641

(ďalej len „**Oprávnená osoba Zhotoviteľa**")

Oprávnená osoba Objednávateľa:

Objednávateľ:	Mgr. David Maruška, MPH
E-mail:	david.maruska@nedu.sk
Tel. kontakt:	+421 911 842 171

(ďalej len „**Oprávnená osoba Objednávateľa**").

9.2 Prostredníctvom určených oprávnených osôb Zmluvné strany:

a) uskutočnia organizačné záležitosti s ohľadom na aktivity a činnosti súvisiace s plnením tejto Zmluvy,
b) zabezpečia koordináciu jednotlivých aktivít a činností Zmluvných strán súvisiacich s plnením tejto Zmluvy,
c) sledujú priebeh plnenia tejto Zmluvy,
d) navrhujú potrebné zmeny technických riešení a technickej povahy v zmysle tejto Zmluvy,
e) zabezpečia vzájomnú spoluprácu a súčinnosť.

9.3 Každá zo Zmluvných strán môže zmeniť oprávnenú osobu. Takáto zmena je účinná dňom doručenia písomného oznámenia o zmene obsahujúceho meno a kontaktné údaje novej oprávnenej osoby druhej Zmluvnej strane.

9.4 Vymenovaná oprávnená osoba Zhotoviteľa/Objednávateľa môže počas svojej plánovanej neprítomnosti (napr. dovolenka, PN a pod.) splnomocniť svojím zastupovaním ďalšiu osobu, spravidla zamestnanca Zhotoviteľa/Objednávateľa.

Čl. X
Zodpovednosť za vady Diela, reklamácia a záručné podmienky

10.1 Zhotoviteľ poskytuje na Dielo a jeho jednotlivé časti záruku počas trvania záručnej doby od podpísania Protokolu o konečnej prebierke minimálne po dobu 24 mesiacov (ďalej len „**Záručná doba**"). Počas Záručnej doby Zhotoviteľ zodpovedá za funkčnosť Diela, ktorá musí byť v súlade so Zmluvou, jej prílohami, najmä prílohou č. 1 Zmluvy, Výzvou, a ďalšími dokumentmi verejného obstarávania. Zhotoviteľ zaručuje, že v Záručnej dobe bude Dielo spôsobilé na použitie na účel zodpovedajúci jeho určeniu.

10.2 Zhotoviteľ sa zaväzuje, že Dielo bude mať počas trvania zmluvnej záruky vlastnosti stanovené touto Zmluvou (najmä požadované Objednávateľom v rámci Opisu predmetu zákazky – príloha č. 1 tejto Zmluvy) a vlastnosti obvyklé.

10.3 Zhotoviteľ zaručuje, že odovzdané Dielo v čase odovzdania nemá právne vady, predovšetkým nie je zaťažené právami tretích osôb z priemyselného alebo iného duševného vlastníctva. Zhotoviteľ sa zaväzuje nahradiť Objednávateľovi škodu spôsobenú uplatnením nárokov tretích osôb z titulu porušenia ich chránených práv súvisiacich s plnením Zhotoviteľa alebo jeho subdodávateľov podľa tejto Zmluvy.

10.4 Zhotoviteľ zaručuje, že k Dielu alebo jeho časti neexistujú v čase jeho odovzdania žiadne právne nároky vyplývajúce zo zmlúv s tretími stranami alebo iného právneho vzťahu, ktorý by prípadne obmedzil Objednávateľa v užívaní Diela.

10.5 Zhotoviteľ zodpovedá za vady Diela, za ktoré sa podľa tejto Zmluvy považujú najmä vykonanie Diela v rozpore s touto Zmluvou (a jej prílohami) a špecifikáciami, nedostatky alebo odchýlky v kvalitatívnych, technologických a technických parametroch, nedostatok iných parametrov požadovaných Objednávateľom, akékoľvek chyby a nesprávne funkcie Diela a také vady, ktoré bránia v obvyklom užívaní Diela. Uvedené platí rovnako aj pre aktualizovanú verziu Diela alebo jeho upgrade. Zhotoviteľ zodpovedá v rovnakom rozsahu aj za vady Diela, ktoré vznikli až po odovzdaní Diela.

10.6 Zmluvné strany sa dohodli, že v prípade zistenia odstrániteľných vád Diela alebo jeho nedostatkov počas trvania zmluvnej záruky, je Zhotoviteľ povinný odstrániť zistené vady bezodkladne po ich oznámení Objednávateľom, a to na vlastné náklady. Akákoľvek reklamácia vád musí byť Objednávateľom vykonaná bez zbytočného odkladu, najneskôr do 5 pracovných dní, čo sa Objednávateľ o vade dozvedel. Uplynutím tejto lehoty nedochádza k strate nárokov Objednávateľa z vád Diela. O odstránení vád bude spísaný Protokol o odstránení vád podpísaný oboma Zmluvnými stranami.

10.7 Reklamácia bude vykonávaná písomne. Za písomnú formu na účely reklamácie vád Diel považujú Zmluvné strany aj e-mailovú komunikáciu.

10.8 V prípade, ak Zhotoviteľ neodstráni vady Diela v stanovenej lehote (ktorá nesmie byť dlhšia ako 3 pracovné dní odo dňa doručenia uplatnených vád Diela zo strany Objednávateľa), Objednávateľ má právo odstrániť vady sám alebo prostredníctvom tretej osoby, a to na náklady Zhotoviteľa (náklady, ktoré vzniknú Objednávateľovi pri takto odstraňovaných vadách, vyfakturuje Objednávateľ Zhotoviteľovi samostatnou faktúrou, ktorú je povinný Zhotoviteľ uhradiť najneskôr do 30 dní od jej doručenia)

a súčasne Objednávateľovi vzniká nárok na zmluvnú pokutu. Zároveň ide o také konanie, ktoré je podstatným porušením Zmluvy a oprávňuje Objednávateľa na odstúpenie od Zmluvy.

10.9 V prípade zistenia neodstrániteľných vád alebo nedostatkov Diela počas trvania zmluvnej záruky, je Zhotoviteľ povinný zabezpečiť bezodkladne primeranú náhradu tak, aby mohol Objednávateľ Dielo nerušene a bez obmedzení užívať na účely a v rozsahu podľa tejto Zmluvy. V prípade, ak zabezpečenie náhrady podľa predchádzajúcej vety nie je možné, má Objednávateľ nárok:

- na zľavu z Ceny Diela v prípade, ak takáto vada zásadným spôsob neobmedzuje užívanie Diela,
- na odstúpenie od Zmluvy, ak takáto vada zásadným spôsobom obmedzuje alebo znemožňuje užívanie Diela.

10.10 Uplatnením nárokov z vád Diela sa Zhotoviteľ nezbavuje povinnosti nahradiť Objednávateľovi škodu, ktorá mu vznikla a povinnosti zaplatiť zmluvnú pokutu.

Čl. XI
Sankcie a zmluvné pokuty

11.1 V prípade omeškania Objednávateľa s úhradou faktúry za Dielo, má Zhotoviteľ právo uplatniť si z nezaplatenej sumy úroky z omeškania v sadzbe podľa Nariadenia vlády SR č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka.

11.2 V prípade, ak je Zhotoviteľ v omeškaní s dodaním Diela alebo jeho časti, Objednávateľ je oprávnený uplatniť si zmluvnú pokutu vo výške 1 % z Ceny Diela, a to za každý deň omeškania, čím nie je dotknutý nárok Objednávateľa na náhradu škody.

11.3 Ak bude Zhotoviteľ v omeškaní s plnením povinnosti odstrániť vadu Diela, je Objednávateľ oprávnený požadovať od Zhotoviteľa zmluvnú pokutu vo výške 5% z Ceny Diela.

11.4 Objednávateľ je oprávnený požadovať od Zhotoviteľa zmluvnú pokutu vo výške 5 000 EUR za každý deň existencie dôvodu vzniku práva na odstúpenie od Zmluvy v zmysle ust. § 15 ods. 1 Zákona o RPVS, resp. ust. § 19 ods. 3 Zákona o verejnom obstarávaní, a to až do momentu odstúpenia Objednávateľa od Zmluvy v súlade s ust. § 15 ods. 1 Zákona o RPVS, resp. podľa ust. § 19 ods. 3 Zákona o verejnom obstarávaní.

11.5 V prípade, ak sa Zhotoviteľ omešká s plnení predmetu Zmluvy a nedodá ho riadne a včas, v dôsledku čoho budú voči Objednávateľovi uplatnené sankcie vyplývajúce mu zo Zmluvy o poskytnutí NFP, je Zhotoviteľ povinný nahradiť Objednávateľovi reálne vzniknutú a preukázanú škodu. Zhotoviteľ je povinný nahradiť Objednávateľovi reálne vzniknutú škodu aj v prípade, ak sa preukáže, že dodané plnenie nie je v súlade s touto Zmluvou a Objednávateľ bude v dôsledku tejto skutočnosti povinný vrátiť poskytnutý príspevok zo Zmluvy o poskytnutí NFP alebo aj jeho časť.

11.6 Akékoľvek sankcie podľa tohto článku Zmluvy, ktoré si uplatní jedna zo Zmluvných strán, je druhá Zmluvná strana povinná uhradiť do 15 dní odo dňa doručenia výzvy na úhradu.

11.7 Zaplatením zmluvnej pokuty nezaniká povinnosť riadne splniť povinnosť zabezpečenú zmluvnou pokutou, ani povinnosť Zhotoviteľa Predmet zmluvy vykonať.

11.8 Zaplatením zmluvnej pokuty nie je dotknuté právo Objednávateľa na náhradu škody, ktorá mu vznikne porušením zmluvných povinností zo strany Zhotoviteľa.

Čl. XII
Mlčanlivosť a ochrana osobných údajov

12.1 Ochranou údajov sa na účely tejto Zmluvy rozumie prijatie a vykonávanie nevyhnutných a primeraných opatrení, ktoré smerujú k ochrane dôvernosti, integrity a dostupnosti všetkých druhov údajov bez ohľadu na ich pôvod alebo formu, ktoré Zmluvná strana môže alebo by v budúcnosti mohla spracúvať. Pod pojmom spracúvanie údajov sa rozumie akákoľvek spracovateľská operácia, ktorá má za následok vznik, zmenu, uchovanie, čítanie alebo vymazanie údajov.

12.2 Všetky skutočnosti, informácie, podklady, stanoviská, osobné údaje, údaje, ktoré sa Zmluvné strany dozvedia v súvislosti s touto Zmluvou, jej plnením, okrem skutočností, informácií a údajov, ktoré podliehajú zverejneniu a/alebo sprístupneniu podľa osobitných všeobecne záväzných právnych predpisov Slovenskej republiky, sú dôvernými informáciami. Zmluvné strany sú povinné zachovávať mlčanlivosť o dôverných informáciách, iba ak by z dohody alebo z príslušných všeobecne záväzných právnych predpisov vyplývalo niečo iné. Poskytnúť dôverné informácie tretej osobe môže niektorá zo Zmluvných strán len po predchádzajúcom písomnom súhlase druhej Zmluvnej strany. Zhotoviteľ zodpovedá za akékoľvek straty a škody, ktoré vzniknú z dôvodu nedodržania tejto povinnosti. Povinnosť mlčanlivosti trvá i po skončení tejto Zmluvy.

12.3 Povinnosť Zhotoviteľa a Objednávateľa zachovávať mlčanlivosť o informáciách, ktoré získali v súvislosti s plnením predmetu tejto Zmluvy, sa nevzťahuje na informácie, ktoré:

a) boli zverejnené už pred podpisom tejto Zmluvy,
b) sa stanú všeobecne a verejne dostupné po podpise tejto Zmluvy z iného dôvodu ako z dôvodu porušenia povinností podľa tejto Zmluvy,
c) majú byť sprístupnené alebo zverejnené na základe povinnosti stanovenej zákonom, rozhodnutím súdu, prokuratúry alebo na základe iného záväzného rozhodnutia príslušného orgánu,
d) boli získané Zhotoviteľom, resp. Objednávateľom, od tretej strany, ktorá ich legitímne získala alebo vyvinula a ktorá nemá žiadnu povinnosť, ktorá by obmedzovala ich zverejňovanie,
e) je Objednávateľ povinný zverejniť na základe povinnosti stanovenej zákonom ako napríklad túto Zmluvu a všetky jej prílohy.

12.4 Akékoľvek údaje z informačných systémov, s ktorými sa Zhotoviteľ oboznámil pri plnení tejto Zmluvy, je oprávnený použiť len v súvislosti s plnením tejto Zmluvy.

12.5 O povinnosti zachovávať mlčanlivosť podľa tejto Zmluvy, ako aj o povinnostiach v oblasti ochrany údajov, je Zhotoviteľ povinný informovať a poučiť aj svojich zamestnancov alebo tretie osoby, ktoré sa v jeho mene budú podieľať na plnení tejto Zmluvy.

12.6 Zhotoviteľ sa zaväzuje pri plnení tejto Zmluvy alebo v súvislosti s ňou vo vzťahu k Objednávateľovi dodržiavať legislatívu v oblasti ochrany údajov, a to najmä ustanovenia Nariadenia Európskeho parlamentu a Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica č. 95/46/ES (všeobecné nariadenie o ochrane údajov), (ďalej len „**GDPR**"), zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Zákona o KyB, ako aj ďalších všeobecne záväzných predpisov, ktoré upravujú ochranu údajov a súkromia.

12.7 Osobné údaje budú spracovávané v rozsahu nevyhnutnom na dosiahnutie účelu tejto Zmluvy.

12.8 Po skončení účinnosti tejto Zmluvy je Zhotoviteľ povinný vrátiť Objednávateľovi všetky kópie, záznamy zachytené na nosičoch dát či iných médiách, poskytnuté dokumenty a podklady a celú dokumentáciu prináležiacu Objednávateľovi. Zhotoviteľ nesmie dôverné informácie využívať mimo predmetu tejto Zmluvy. Táto povinnosť platí bez časového obmedzenia aj po skončení účinnosti tejto Zmluvy.

12.9 Zmluvné strany sa zaväzujú používať dôverné informácie výlučne na účel, na ktorý im boli poskytnuté a zároveň sa zaväzujú dôverné informácie ochraňovať najmenej s rovnakou starostlivosťou ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti, predovšetkým ich budú chrániť pred náhodným alebo neoprávneným poškodením a zničením, náhodnou stratou, zmenou alebo iným znehodnotením, nedovoleným prístupom alebo sprístupnením alebo zverejnením, pričom, ak nie je v tejto Zmluve ustanovené inak, zaväzujú sa, že bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany neposkytnú, neodovzdajú, neoznámia alebo iným spôsobom nevyzradia, resp. nesprístupnia dôverné informácie druhej Zmluvnej strany tretej osobe.

12.10 Zhotoviteľ sa zaväzuje prijať primerané technické, organizačné a personálne opatrenia na zabezpečenie ochrany osobných údajov, ako aj na zabezpečenie práv a povinností vyplývajúcich z tejto Zmluvy, a to vrátane poučenia svojich zamestnancov, resp. tretích osôb, ktoré sa budú v jeho mene podieľať na plnení tejto Zmluvy.

12.11 Objednávateľ je oprávnený požadovať od Zhotoviteľa preukázanie splnenia všetkých povinností vrátane vykonania všetkých predpísaných bezpečnostných opatrení na ochranu údajov, ako aj potvrdenie o zlikvidovaní údajov a Zhotoviteľ je povinný takejto žiadosti bezodkladne vyhovieť.

12.12 V prípade, ak Zhotoviteľ akýkoľvek záväzok mlčanlivosti poruší, zodpovedá Objednávateľovi za takto vzniknutú preukázanú škodu v celom rozsahu. V prípade, ak by na základe právneho predpisu, súdneho alebo iného rozhodnutia alebo akejkoľvek inej skutočnosti vznikla v súvislosti s porušením povinností mlčanlivosti povinnosť uhradiť vzniknutú škodu, zaväzuje sa Zhotoviteľ túto škodu uhradiť namiesto Objednávateľa, avšak len v prípade, ak povinnosť plnenia Objednávateľa vznikla v súvislosti s preukázaným zavineným konaním Zhotoviteľa, ktorým došlo k porušeniu jeho povinností podľa tejto Zmluvy. Pokiaľ by Zhotoviteľ túto povinnosť nesplnil a musel by ju splniť Objednávateľ, má Objednávateľ právo domáhať sa splnenia záväzku na príslušnom súde.

Čl. XIII
Skončenie Zmluvy

13.1 Táto Zmluva sa uzatvára na dobu určitú, a to do riadneho splnenia a odovzdania Diela podľa tejto Zmluvy.

13.2 Túto Zmluvu je možné ukončiť na základe vzájomnej dohody oboch Zmluvných strán ku dňu, ktorý si dohodnú. V dohode si Zmluvné strany vysporiadajú prípadné nároky vzniknuté z poskytnutých plnení. V rámci tejto dohody sa vysporiada aj udelenie licencií k odovzdaným častiam Diela, alebo Dielu celému v súlade s čl. VI tejto Zmluvy.

13.3 Zhotoviteľ je oprávnený odstúpiť od tejto Zmluvy pri podstatnom porušení Zmluvy Objednávateľom, pričom za podstatné porušenie Zmluvy Objednávateľom sa považuje, ak je Objednávateľ v omeškaní s platbou za faktúru o viac ako 60 dní po jej splatnosti.

13.4 Objednávateľ je oprávnený odstúpiť od Zmluvy najmä, nie však výlučne vtedy, ak:

- Zhotoviteľ nesplní termín dodania Diela, a to ani v dodatočnej lehote, ktorú stanoví Objednávateľ, alebo v prípade ak odovzdá Dielo s vadami a tieto neodstráni ani v dodatočne stanovenej lehote, a/alebo v prípade, ak sa preukáže, že Zhotoviteľ nemal dostatočné oprávnenie na poskytnutie licencie na plnenie predmetu tejto Zmluvy,
- Zhotoviteľ stratil spôsobilosť vyžadovanú Zákonom o verejnom obstarávaní a/alebo stratil iné právne alebo vecné predpoklady na riadne plnenie tejto Zmluvy,
- na majetok Zhotoviteľa je vyhlásený konkurz a/alebo konkurzné konanie bolo zastavené pre nedostatok majetku a/alebo je Zhotoviteľovi povolená reštrukturalizácia a/alebo Zhotoviteľ vstúpi do likvidácie, preruší alebo iným spôsobom skončí svoju podnikateľskú činnosť,
- Zhotoviteľ postúpi akúkoľvek svoju pohľadávku z tejto Zmluvy na tretiu osobu bez predchádzajúceho písomného súhlasu Objednávateľa,
- sa preukáže, že Zhotoviteľ v ponuke v rámci verejného obstarávania predložil nepravdivé doklady a/alebo uviedol nepravdivé, neúplné alebo skreslené údaje,
- kontrolou verejného obstarávania, ktorého výsledkom je táto Zmluva, bolo zistené porušenie Zákona o verejnom obstarávaní,
- ak Poskytovateľ nenávratného finančného príspevku alebo Objednávateľ odstúpia od Zmluvy o poskytnutí NFP,
- ak nedošlo k plneniu z tejto Zmluvy medzi Objednávateľom a Zhotoviteľom a výsledky finančnej kontroly Poskytovateľa nenávratného finančného príspevku podľa Zmluvy o poskytnutí NFP neumožňujú financovanie výdavkov vzniknutých z verejného obstarávania, výsledkom ktorého je uzatvorenie tejto Zmluvy, a to bez akýchkoľvek sankcií voči Objednávateľovi,
- je splnený niektorý z dôvodov na odstúpenie od Zmluvy podľa ust. § 19 Zákona o verejnom obstarávaní,
- je splnený niektorý z dôvodov na odstúpenie od Zmluvy podľa ustanovení Zákona o RPVS.

13.5 V prípade odstúpenia od tejto Zmluvy sú Zmluvné strany povinné vrátiť si všetky poskytnuté plnenia do 20 dní od účinného odstúpenia od Zmluvy s výnimkou, ak sa Zmluvné strany výslovne dohodnú inak.

13.6 Odstúpenie od Zmluvy je účinné dňom doručenia písomného oznámenia o odstúpení druhej Zmluvnej strane.

13.7 Ukončenie tejto Zmluvy nemá vplyv na povinnosť Zmluvných strán zaplatiť zmluvné pokuty a nahradiť vzniknutú škodu. Skončenie tejto Zmluvy nemá vplyv na ustanovenia, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení Zmluvy (najmä ustanovenia o povinnosti mlčanlivosti, komunikácii a riešení sporov a ustanovenia o práve duševného vlastníctva).

Čl. XIV
Osobitné povinnosti Zhotoviteľa

14.1 Zhotoviteľ berie na vedomie, že finančné prostriedky Objednávateľa určené na zaplatenie celkovej Ceny Diela podľa článku VIII tejto Zmluvy sú finančné prostriedky z Európskeho fondu regionálneho rozvoja (Operačný program Integrovaná infraštruktúra v rámci operačnej osi 7 Informačná spoločnosť) a zároveň sú finančné prostriedky zo štátneho rozpočtu Slovenskej republiky. Zhotoviteľ berie na vedomie, že podpisom tejto Zmluvy sa stáva súčasťou Systému riadenia európskych štrukturálnych a investičných fondov a Systému finančného riadenia. Zhotoviteľ zároveň berie na vedomie, že na použitie prostriedkov, kontrolu použitia týchto prostriedkov a vymáhanie ich neoprávneného použitia alebo zadržania sa vzťahuje režim upravený v osobitných predpisoch, napr. v zákone č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov (ďalej len „**zákon č. 357/2015 Z. z.**"), zákone č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov (ďalej len „**zákon o príspevku z EŠIF**") a v zmysle ďalších príslušných právnych predpisov Slovenskej republiky a právnych aktov Európskej únie.

14.2 Okrem povinností uvedených v tejto Zmluve je Zhotoviteľ povinný strpieť výkon kontroly/auditu/overovania oprávnenými osobami v súvislosti s vykonaným Dielom a poskytnúť im bezodkladnú, bezodplatnú maximálne možnú všetku potrebnú súčinnosť, a to kedykoľvek počas platnosti a účinnosti tejto Zmluvy, v termínoch stanovených pre Objednávateľa v zmluvných vzťahoch s príslušnými orgánmi zapojenými do implementácie fondov Európskej únie, resp. podľa Zmluvy o poskytnutí NFP. Oprávnenými osobami sú najmä:

a) Poskytovateľ nenávratného finančného príspevku a ním poverené osoby,
b) útvar vnútorného auditu Riadiaceho orgánu alebo Sprostredkovateľského orgánu a nimi poverené osoby,
c) Najvyšší kontrolný úrad SR a ním poverené osoby,
d) orgán auditu, jeho spolupracujúce orgány (Úrad vládneho auditu) a osoby poverené na výkon kontroly/auditu;
e) splnomocnení zástupcovia Európskej Komisie a Európskeho dvora audítorov,
f) orgán zabezpečujúci ochranu finančných záujmov EÚ,
g) osoby prizvané alebo poverené orgánmi uvedenými v písm. a) až f) v súlade s

príslušnými právnymi predpismi Slovenskej republiky a právnymi aktmi Európskej Únie.

14.3 Zhotoviteľ a jeho subdodávatelia berú na vedomie, že výkon kontroly/auditu/ kontroly na mieste súvisiacom s plnením predmetu Zmluvy sa môže týkať Zhotoviteľa, ako aj jeho subdodávateľov. Zhotoviteľ a jeho subdodávatelia berú na vedomie, že v súvislosti s povinnosťou strpieť výkon kontroly/ auditu/ kontroly na mieste súvisiacom s plnením predmetu Zmluvy, poskytovaním súčinnosti pri výkone kontroly/ auditu/ kontroly na mieste súvisiacom s plnením predmetu Zmluvy, alebo akýmikoľvek úkonmi týkajúcimi sa výkonu kontroly/ auditu/ kontroly na mieste súvisiacom s plnením predmetu Zmluvy, Zhotoviteľ ani jeho subdodávatelia nemajú nárok na odmenu, náhradu, ani na iné plnenie.

14.4 Zhotoviteľ je povinný rešpektovať právo osôb oprávnených na výkon kontroly vstupovať do objektov, ak to súvisí s predmetom tejto Zmluvy a požadovať od Zhotoviteľa predloženie originálnych dokladov a inú potrebnú dokumentáciu, alebo iné ďalšie doklady súvisiace s touto Zmluvou.

14.5 Zhotoviteľ je povinný prijať opatrenia na nápravu nedostatkov zistených kontrolou/auditom/ overovaním na mieste v lehote stanovenej osobami oprávnenými na výkon kontroly, a zároveň zaslať Objednávateľovi informáciu o splnení opatrení prijatých na nápravu zistených nedostatkov bezodkladne po ich splnení.

14.6 Zhotoviteľ sa zaväzuje poskytnúť Objednávateľovi aj ďalšiu nevyhnutnú súčinnosť v súvislosti s plnením Zmluvy o poskytnutí NFP.

14.7 Účastníci tejto Zmluvy sa zaväzujú, že počas vykonávania Diela podľa tejto Zmluvy budú navzájom spolupracovať a vyvinú maximálne úsilie a súčinnosť, aby bol jej predmet zrealizovaný v súlade s touto Zmluvou. Zhotoviteľ je povinný zabezpečiť prijatie nápravných opatrení a definovanie termínov na odstránenie zistených nedostatkov.

XV
Záverečné ustanovenia

15.1 Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpisu oboma Zmluvnými stranami. Vzhľadom na skutočnosť, že Objednávateľ je verejným obstarávateľom, nemá povinnosť v zmysle ustanovení zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov zverejňovať túto Zmluvu, keďže nie je povinnou osobu a ani táto Zmluva nie je povinne zverejňovanou Zmluvou.

15.2 Právne vzťahy, pokiaľ nie sú upravené touto Zmluvou, riadia sa predovšetkým ustanoveniami Obchodného zákonníka, Autorského zákona, Zákona o verejnom obstarávaní a ustanoveniami ostatných právnych predpisov platných v Slovenskej republike.

15.3 Zmluvné strany sa výslovne dohodli, že bez predchádzajúceho písomného súhlasu Objednávateľa Zhotoviteľ nie je oprávnený postúpiť alebo započítať akékoľvek pohľadávky (práva), ktoré vznikli podľa/na základe tejto Zmluvy tretím osobám, ani sa dohodnúť s treťou osobou na prevzatí záväzkov (povinností) vyplývajúcich z tejto Zmluvy. Právny úkon, ktorým budú pohľadávky (práva) postúpené v rozpore s týmto bodom tohto článku Zmluvy, bude neplatný.

15.4 Zmeny alebo dodatky k Zmluve sú možné len v súlade s príslušnými právnymi predpismi Slovenskej republiky, a to vo forme písomných očíslovaných dodatkov, podpísaných oprávnenými zástupcami oboch Zmluvných strán.

15.5 Ak niektoré ustanovenia tejto Zmluvy stratia účinnosť, nie je tým dotknutá platnosť a účinnosť ostatných jej ustanovení. Namiesto neúčinných ustanovení a na vyplnenie medzier sa použije úprava, ktorá sa, pokiaľ je to právne možné, čo najviac približuje zmyslu a účelu tejto Zmluvy.

15.6 Všetky spory vyplývajúce z tejto Zmluvy alebo vzniknuté v súvislosti s ňou budú Zmluvné strany riešiť predovšetkým vzájomnou dohodou. Ak k dohode nedôjde o spore vzniknutom medzi Zmluvnými stranami v súvislosti s touto Zmluvou rozhodnú súdy Slovenskej republiky.

15.7 Táto Zmluva je vyhotovená v štyroch vyhotoveniach s platnosťou originálu, z toho dve pre Objednávateľa a dve pre Zhotoviteľa.

15.8 Zmluvné strany vyhlasujú, že si túto Zmluvu prečítali, jej obsahu porozumeli a na znak toho, že Zmluva zodpovedá ich skutočnej a slobodnej vôli, ju vlastnoručne podpísali.

15.9 Zmluvné strany spoločne vyhlasujú, že túto Zmluvu uzatvárajú slobodne a vážne, že ju neuzavreli v tiesni a za nápadne nevýhodných podmienok, že sa táto Zmluva svojím obsahom alebo účelom neprieči zákonu a ani ho neobchádza. Zmluvné strany zároveň vyhlasujú, že majú plnú spôsobilosť na právne úkony.

15.10 Neoddeliteľnou súčasťou tejto Zmluvy sú tieto prílohy:

Príloha č. 1: Opis predmetu zákazky;
Príloha č. 2: Zoznam subdodávateľov;
Príloha č. 3: Harmonogram;
Príloha č. 4: Návrh na plnenie kritérií;
Príloha č. 5: Zoznam odborníkov a požiadaviek na odborníkov

Ľubochňa, dňa 25.10.2023

V Bratislave, dňa 23.10.2023

iServices
iServices s.r.o., Zadunajská cesta 8, 851 01 Bratislava
tel.: +421 2 6224 4226, email: iservices@iservices.sk
IČO: 43872930, IČ DPH: SK2022500524

NEDÚ, n.o.
Národný endokrinologický a diabetologický ústav n.o.

Ing. Pavol Šimák
konateľ
iServices s. r. o

Príloha č. 1

Opis predmetu zákazky – špecifikácia

Verejný obstarávateľ nemá aktuálne implementované riešenia a opatrenia kybernetickej bezpečnosti povinné podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o KyB**") a zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o ITVS**"). Z externého pohľadu sa zvyšuje frekvencia a závažnosť útokov, z interného pohľadu sa zase neustále zvyšuje závislosť na informačných aktívach a IT systémoch. Zvyšuje sa sofistikovanosť útokov, zraniteľnosti a následne aj dopady bezpečnostných incidentov, a preto je potrebné zvýšiť úroveň informačnej a kybernetickej bezpečnosti.

Verejný obstarávateľ v oblasti informačnej a kybernetickej bezpečnosti informačných technológií verejnej správy z dôvodu potreby plnenia požiadaviek (nakoľko verejný obstarávateľ nemá zavedený formálny proces riadenia rizík, analýzu rizík má v nedostatočnej kvalite) stanovených najmä zákonom o ITVS a zákonom o KyB, ktorými sa ustanovuje obsah a rozsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie, obstaráva poskytovanie služieb v zákazke s názvom: „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach - Národný endokrinologický a diabetologický ústav".

Predmetom zákazky je poskytovanie služieb súvisiacich so zavedením procesu riadenia v oblasti informačnej a kybernetickej bezpečnosti informačných technológií verejnej správy v súlade s projektom Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach - Národný endokrinologický a diabetologický ústav, **na základe schválenej žiadosti o poskytnutie nenávratného finančného príspevku** v súlade s výzvou OPII-2022/7/20-DOP - Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach a v súlade so zákonom o KB a zákonom ITVS.

NEDU je prevádzkovateľom nasledujúcich systémov, pre ktoré požaduje vykonať aktivity v zmysle zákona o KyB a zákona o ITVS:

- NIS (vlastný SW)
  - ambulantná časť
    - centrálny príjem
    - lekárska časť
  - lôžková časť
    - centrálny príjem
    - lekárska časť
  - zobrazovacie vyšetrenia (KV)
  - odberové miesta
  - stravovacia prevádzka
  - program pre vrátnice (samostatný program)
- Human – personálny a mzdový (Hour)

- Softip Profit – účtovníctvo a sklady (Softip)
- evidencia pošty (vlastný SW)
- SW k prístrojom
  - Hologic QDR – beží na PC od prístroja (denzitometer)
  - inBody
  - Holter

Stav infraštruktúry NEDU

Počet pracovných staníc	130
Počet serverov	5
Počet účtov Microsoft 365	0
Počet lokalít	1

Hlavnými aktivitami predmetu zákazky sú:

1. Analýza a Dizajn,
2. Nákup technických prostriedkov, programových prostriedkov a služieb,
3. Implementácia a testovanie,
4. Nasadenie.

1. **Analýza a dizajn** bude pozostávať z nasledovných častí:
   - analýza aktuálneho stavu a súladu s legislatívnymi požiadavkami,
   - inventarizácia a klasifikácia informačných aktív a kategorizácia IS a sietí,
   - analýza rizík a analýza dopadov,
   - zavedenie procesu riadenia rizík a procesu governance IB a KyB,
   - dodávka produktov definovaných na základe šablón MIRRI.

2. **Nákup technických prostriedkov, programových prostriedkov a služieb**

3. **Implementácia a Testovanie** pozostáva z „customizácia" a testovania klientskeho nástroja evidencie informačných aktív, rizík a incidentov do prostredia verejného obstarávateľa. Ďalej bude pozostávať z obstarania nástroja na bezpečnostný monitoring a riadenie kybernetickej bezpečnosti, pomocou ktorého bude možné riadiť a vyhodnocovať jednotlivé procesy a parametre v oblasti kybernetickej bezpečnosti.

   Implementačné služby minimálne v nasledujúcom rozsahu:
   - inštalácia komponentov systému v prostredí verejného obstarávateľa,
   - nastavenie a konfigurácia systému v IT prostredí verejného obstarávateľa,
   - import aktív verejného obstarávateľa do systému,
   - nastavenie metodiky analýzy rizík,
   - nastavenie bezpečnostných politík pre servery,
   - nastavenie bezpečnostných politík pre koncové zariadenia,
   - nastavenie bezpečnostných politík pre cloud prostredie,
   - nastavenie notifikačných pravidiel,
   - nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom

verejného obstarávateľa,
- vytvorenie a odovzdanie prevádzkovej dokumentácie systému, administrátorskej dokumentácie,
- kvalifikované zaškolenie a odovzdanie know-how pre vybrané skupiny/role zamestnancov verejného obstarávateľa.

4. **Nasadenie** pozostáva z nasadenia klientskeho nástroja evidencie informačných aktív, rizík a incidentov. Bude potrebné zabezpečiť zvyšovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti. Súčasťou tejto aktivity bude pravidelné testovanie užívateľov prostredníctvom phishing kampaní, ako aj realizácia školení. Služby pre zabezpečenie ochrany pracovných staníc a serverov. Služby pre zabezpečenie riadenia bezpečnosti sieti prostredníctvom riadenia prístupu užívateľov, vynucovaním prístupu najnižších opatrení, filtrovaním obsahu, segmentáciou sietí, detekovaním alebo prevenciou prieniku na úrovni siete, riadením vzdialeného pripojenia a vynucovaním viac faktorovej autentifikácie. Služby pre zabezpečenie riadenia procesu detekciu a riadenia kybernetických bezpečnostných incidentov vrátane zabezpečovania zaznamenávania činnosti sietí a informačných systémov. Služby pre zabezpečenie procesu zálohovania a obnovy dát. Služby pre zabezpečenie bezpečnostného dohľadu a riadenie kybernetických incidentov.

   Služby podpory počas projektu obsahujú:
   1. Hotline 8x5 za účelom:
      - nahlásenia vád riešenia a konzultácii týkajúcich sa bežnej prevádzky riešenia,
      - dotazy na obchodnú podporu,
      - Knowledge database, Q&A,
      - Konzultácie licenčného modelu,
      - Komunikácia s výrobcom.
   2. Odstraňovanie vád podľa nasledovných parametrov 8x5
   3. Rámcové konzultačné práce v predpokladanom objeme:
      - pravidelná kontrola funkčnosti nástroja,
      - poskytnutie updatov, upgradov a patchov riešenia,
      - pravidelná kontrola funkčnosti zberu dát,
      - pravidelná kontrola konfiguračných nastavení a aktuálneho stavu komponentov,
      - podpora pri riešení kybernetických bezpečnostných incidentov.

A) Cieľom predkladaného projektu je realizácia primárnych aktivít, konkrétne:

- Analyzovať aktuálny stav v oblasti riadenia informačnej bezpečnosti (ďalej len „**IB**“) a kybernetickej bezpečnosti (ďalej len „**KyB**“) a jeho súladu s požiadavkami legislatívy, a to najmä so zákonom o KyB.
- Vykonať dôkladnú analýzu rizík a analýzu dopadov (AR/BIA) vrátane:
  - identifikácie aktív a ohodnotenia ich kritickosti,
  - klasifikácie aktív a kategorizácie IS a sietí,
  - identifikácie hrozieb a vektorov útokov,
  - analýzy potenciálnych dopadov,
  - identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,

- identifikácie existujúcich opatrení a reziduálnych rizík,
- návrhu opatrení.

- Na základe analýzy rizík spracovať stratégiu informačnej a kybernetickej bezpečnosti vrátane plánu na implementáciu navrhovaných opatrení.
- Zabezpečiť formálne rozhodnutia o riadení rizík (o ich akceptácii alebo prijatí adekvátnych opatrení na ich zníženie alebo úplnú elimináciu) vedením NEDU.
- Vytvoriť požadované interné dokumenty a smernice pre relevantné oblasti riadenia informačnej bezpečnosti a kybernetickej bezpečnosti.
- Zaviesť do prostredia NEDU SW nástroj pre procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti.
- Zaviesť do prostredia NEDU SW nástroj pre bezpečnostné testovania zamestnancov NEDU.
- Vykonanie bezpečnostných testovaní zameraných na:
  - identifikovanie zraniteľností SW a HW,
  - zistenie podozrivých aktivít v infraštruktúre organizácie.

Požadované aktivity:

ID	Aktivita/prevádzková dokumentácia (výstup)	Popis
1.1	Posúdenie súladu s bezpečnostnými požiadavkami, zákonom č. 69/2018 Z.z. (vyhlášky NBÚ č. 362/2018 Z. z.) ako aj 95/2019 (vyhlášky č. 179/2020 Z.z.) a návrh strategického akčného plánu úloh na zabezpečenie súladu	"Pred-audit", resp. posúdenie stavu kybernetickej bezpečnosti. Príprava NEDU na oficiálny audit kybernetickej bezpečnosti. Výstupom aktivity je kontrolný zoznam legislatívnych požiadaviek a ich súladu s aktuálnym stavom NEDU a návrh akčného plánu strategických úloh pre jednotlivých členov tímu.
1.2	Vypracovanie interných smerníc a prevádzkovej dokumentácie riadenia informačnej bezpečnosti a kybernetickej bezpečnosti	Výstupom aktivity bude interná dokumentácia a smernice.
1.2.1.	Stratégia informačnej a kybernetickej bezpečnosti	Definuje jednoznačné a merateľné strategické ciele, pričom po ich naplnení bude možné zhodnotiť ich dopad na zlepšenie systému informačnej a kybernetickej bezpečnosti. Výstupom bude dokument definujúci požiadavky a ciele na strategickej úrovni v oblasti informačnej a kybernetickej bezpečnosti. Predmetná stratégia musí spĺňať štruktúru a byť v súlade s obsahovými požiadavkami podľa prílohy č. 1 vyhlášky č. 362/2018 Z. z. Dokument musí taktiež obsahovať roadmapy na implementáciu navrhovaných bezpečnostných opatrení.
1.2.2.	Bezpečnostná politika	Smernica upravuje bezpečnostnú politiku v NEDU. NEDU musí zabezpečiť aj prijatie politiky.

ID	Aktivita/prevádzková dokumentácia (výstup)	Popis
1.2.3.	Smernica pre riadenie informačnej bezpečnosti	Smernica Systému riadenia informačnej bezpečnosti sa uplatňuje pri plnení všetkých úloh, pri ktorých je nevyhnutné zabezpečiť vysokú ochranu informačných aktív a na všetky prevádzkované informačné aktíva. NEDU musí zabezpečiť schválenie smernice.
1.2.4.	Klasifikácia informácií a kategorizácia sietí a informačných systémov	Smernica sa riadi podľa § 20 ods. 2 zákona č. 69/2018 Z.z. Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa odseku 1 sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.
1.2.5.	Smernica výkonu analýzy rizík a analýzy dopadov (AR/BIA)	Smernica upravuje základnú AR/BIA, ktorá riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti.
1.2.6.	Smernica o bezpečnej prevádzke informačných systémov (IS) a sietí	Cieľom smernice je zabezpečiť správnu a bezpečnú prevádzku prostriedkov spracúvajúcich informácie v prevádzke IS.
1.2.7.	Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov	Smernica na základe §20 ods. 3 písm. j) zákona o riešení kybernetických bezpečnostných incidentov.
1.2.8.	Politika riadenia kontinuity činností - Business Continuity Management (BCM) vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP	BCM predstavuje súbor plánovaných a vzájomne prepojených aktivít, ktoré je odporúčané vykonať v prípade, ak nastane neplánované prerušenie bežnej činnosti organizácie ako havária alebo iná krízová situácia. (DRP – Disaster Recovery Plan) - Plán obnovy je dokument opisujúci činnosti, úlohy, zdroje a údaje potrebné na obnovu infraštruktúry organizácie. (BCP – Business Continuity Plan) - Plány obnovy sú podmnožinou plánov kontinuity činností. NEDU požaduje aby BCM bola priamo realizovaná a ďalej spravovaná v SW nástroji na procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti.
1.3	Inventarizácia, klasifikácia a kategorizácia	Realizácia inventarizácie a klasifikácie informačných aktív, kategorizácie IS a sietí na základe klasifikácie. Cieľom je dosiahnuť a udržiavať primeranú ochranu informačných aktív, aktív IS a sietí. NEDU požaduje aby inventarizácia, klasifikácia a kategorizácia bola priamo realizovaná a ďalej spravovaná v SW nástroji na procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti.
1.4	Vykonanie technických testov (skenov) aktív a zraniteľností aktív na zistenie	Testovanie metódou „white-box“. NEDU zabezpečí dostupnosť testovaných aktív počas testovacieho okna.

ID	Aktivita/prevádzková dokumentácia (výstup)	Popis
	známych zraniteľností v internej sieťovej infraštruktúre organizácie.	Posúdené budú jednotlivé identifikované aktíva, služby, ich účel a verzie.
1.4.1	Report technických testov (skenov) zraniteľností v internej sieťovej infraštruktúre organizácie.	Výstupom z technických testov (skenov) zraniteľností bude zoznam aktív a identifikovaných zraniteľností aktív a zoznam odporúčaní pre zníženie rizika v súvislosti s identifikovanými zraniteľnosťami. Report z testov bude podkladom pre podrobnú inventarizáciu a klasifikáciu informačných aktív.
1.5	Vykonanie technických testov (skenov) sieťovej komunikácie na zistenie podozrivých aktivít v infraštruktúre organizácie.	Testovanie prostredníctvom neinvazívnej kontroly všetkých typov sieťovej prevádzky – „počúvaním" prostredníctvom span portu. Cieľom testovania je odhalenie škodlivého obsahu, škodlivej komunikácie, či správania, ktoré môžu naznačovať činnosť škodlivého softvéru alebo činnosť útočníkov naprieč všetkými úrovňami útoku. Hrozby APT a cielené útoky. Oblasti analýzy: • malware a exploity zneužívajúce dokumenty • Sieťová aktivita útočníka • Webové hrozby (exploity, nevedomé downloady) • E-mailové hrozby (phishing, spear phising) • Krádeže dát • Botnety, trójske kone, červy, keyloggery • Nebezpečné (disruptívne) aplikácie • Iné podozrivé aktivity
1.5.1	Report technických testov (skenov) sieťovej komunikácie organizácie.	Výstupom z technických testov (skenov) bude zoznam zariadení, kde bola identifikovaná podozrivá alebo škodlivá aktivita a zoznam odporúčaní pre zníženie rizika v súvislosti s identifikovanými podozrivými alebo škodlivými aktivitami. Report z testov bude podkladom pre podrobnú analýzu rizík organizácie.
1.6	Vykonanie analýzy rizík a analýzy dopadov	Výstupom bude vykonaná AR/BIA podľa jednotnej smernice (metodiky) pre dátovo-procesné aktíva (biznis agendy) a IKT zdroje, ktoré tieto agendy podporujú. V rámci procesu tvorby AR/BIA vykonať fyzicky objektovú obhliadku vo všetkých priestoroch NEDU súvisiacich s predmetom zákazky pre zmapovanie rizík a zraniteľností. Vypracovanie akčného plánu vrátane technických návrhov a časovým harmonogramom pre odstránenie identifikovaného nesúladu a zníženia rizík. NEDU požaduje aby analýza rizík a analýza dopadov bola priamo realizovaná a ďalej spravovaná v SW

ID	Aktivita/prevádzková dokumentácia (výstup)	Popis
		nástroji na procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti.
1.7	Návrh katalógu rizík a spôsobov ich riadenia	V zozname rizík je potrebné uviesť najmä základné informácie o riziku, informácie pre analýzu rizík, informácie o odozve na vyhodnotenie rizika. NEDU požaduje aby plán riadenia rizík bola priamo vytvorený a ďalej spravovaný v SW nástroji na procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti.
1.8	Implementácia, customizácia a konfigurácia SW nástroja pre evidenciu informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov	Implementácia, customizácia a konfigurácia SW nástroja pre evidenciu informačných aktív.
1.9	Implementácia, customizácia a konfigurácia SW nástroja pre procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti	Implementácia, customizácia a konfigurácia SW nástroja pre procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti.
1.10	Implementácia, customizácia a konfigurácia SW nástroja pre Riadenie tretích strán	Implementácia, customizácia a konfigurácia SW nástroja pre evidenciu tretej strany ich prístupových oprávnení a časové obmedzenia týchto oprávnení.
1.11	Implementácia, customizácia a konfigurácia SW nástroja pre riadenie Personálnej bezpečnosti	Implementácia, customizácia a konfigurácia SW nástroja pre vedenie údajov o zamestnancoch, realizované vzdelávanie a školenia zamestnancov v oblasti kybernetickej bezpečnosti, zvýšenie zručností biznis vlastníkov, zodpovednosť za jednotlivé aktíva a ich klasifikácia, priradené licencie a zariadenia.
1.12	Implementácia, customizácia a konfigurácia SW nástroja pre riadenie procesu Analýzy rizík	Implementácia, customizácia a konfigurácia SW nástroja pre riadenie procesu riadenia rizík a bezpečnostných opatrení
1.13	Implementácia, customizácia a konfigurácia SW nástroja pre automatický výkon auditu súladu.	Implementácia, customizácia a konfigurácia SW nástroja pre zabezpečenie vykonania auditu súladu či už z pohľadu dokumentácie, procesov alebo rizík a to na základe naplnenia opatrení definovaných legislatívou ako i smernicami NEDU.
1.14	Bezpečnostný projekt	Vytvorenie bezpečnostného projektu pre systém NIS v súlade so zákonom o ITVS.
1.15	Plán zálohovania	Vytvorenie dokumentu popisujúceho plán, spôsob a periódu zálohovania tak aby novo navrhnutý proces bol v súlade s požiadavkami predmetnej legislatívy.

ID	Aktivita/prevádzková dokumentácia (výstup)	Popis
1.16	Implementácia, customizácia a konfigurácia platformy pre bezpečnostné testovania zamestnancov	Implementácia, customizácia a konfigurácia platformy pre bezpečnostné testovania zamestnancov pre potreby rozvoja bezpečnostného povedomia zamestnancov NEDU v zmysle požiadaviek predmetnej legislatívy.

Špecifické požiadavky na SW nástroj procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti:

- Centrálna konzola pre používateľov systému prístupná cez web prehliadače (Chrome, Firefox, Safari alebo Edge).
- Centrálna konzola lokalizovaná v Slovenskom jazyku.
- Centrálna správa musí byť prevádzkovaná ako SaaS.
- Podpora požiadaviek legislatívy SR.
- Centrálny dashboard pre rýchle vyhodnotenie aktív (primárne a podporné), rizík podľa kategórie, rizík podľa hrozieb a zraniteľností, aktuálne dosahovaná úroveň súladu s požiadavkami zákona č. 69/2018 Z. z. a vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- Podpora prihlásenia prostredníctvom multi-faktorovej autentifikácie.
- Podpora tvorby klasifikácie informácií a kategorizácie sietí a informačných systémov podľa zákona č. 69/2018 Z.z. a doporučení vyhlášky č. 362/2018, vytváranie registrov aktív, hrozieb.
- Parametrizácia systému:
  - Definovanie metódy na výpočet hodnotenie aktív,
  - Definovanie metódy na kategorizáciu rizík,
  - Definovanie bezpečnostnej štruktúry spoločnosti (osoby, organizačné jednotky, role),
  - Definovanie druhov aktív,
  - Definovanie typov aktív,
  - Definovanie vlastných atribútov aktív,
  - Definovanie stupnice pre hodnotenie dôvernosti, dostupnosti, integrity, dopadov, hrozieb a zraniteľností,
  - Definovanie bezpečnostných opatrení ,
  - Register dodávateľov,
  - Definovanie kritérií na hodnotenie dodávateľov.
- Register rizík prostredníctvom, ktorého je možné definovať kombinácie hrozba/zraniteľnosť na konkrétne typy aktív.
- Evidencia aktív (manuálne alebo prostredníctvom importu z dátového súboru):
  - Všeobecné (druh, typ, lokalita, garant, administrátor, dodávateľ, prevádzkovateľ, závislosť aktíva na iných aktívach
  - Hodnotenie aktíva (dôvernosť, dostupnosť a integrita),
  - Identifikácia hrozieb/zraniteľnosti manuálne alebo priamo z registra rizík,

- Spôsob používania a manipulácie,
- Vlastné atribúty.

- Mapa aktív pre grafické zobrazenie závislostí medzi jednotlivými aktívami:
  - Zobrazenie priameho vzťahu aktíva a jeho podriadených a nadriadených aktív,
  - Komplexné zobrazenie mapy všetkých aktív,
  - Filtrácia zobrazených aktív (druh alebo kategória aktíva).
- Hodnotenie rizík:
  - Možnosť stiahnuť súbor pdf s identifikovanými rizikami pre jedno alebo viaceré aktíva,
  - Hodnotenie dopadu identifikovaných rizík,
  - Návrh bezpečnostných opatrení pre zníženie rizika na úrovni aktíva,
  - Výpočet rizika pred a po opatrení bezpečnostného opatrenia,
  - Rozhodnutie o akceptovaní alebo neakceptovaní rizika.
- Hodnotenie opatrení:
  - Zoznam rizík, ktoré bezpečnostné opatrenie rieši,
  - Aplikovateľnosť bezpečnostného opatrenia,
  - Zavedenie bezpečnostného opatrenia a jeho riadenie
    - ľudské a finančné zdroje, časový harmonogram
    - evidencia komunikácie riešiteľského tímu
- Plán zvládania rizík pre riadenie implementácie bezpečnostných opatrení:
  - Evidencia požiadaviek na ľudské a finančné zdroje,
  - Dátum začatia a ukončenie implementácie,
  - Diskusný priestor pre riešiteľský tím.
- Hodnotenie dodávateľov:
  - Hodnotenie atribútov dodávateľov aktív,
  - Mapovanie dodávateľov na konkrétne aktíva,
  - Možnosť evidencie podpornej dokumentácie k dodávateľov (zmluvy, SLA,..).
- Hodnotenie plnenie požiadaviek legislatívy:
  - Evidencia plnenia požiadaviek legislatívy
    - ZoKB (zákon č.69/2018 Z. z. a vyhláška č.362/2018 Z. z)
    - ITVS (zákon č.95/2019 Z. z. a vyhláška č. 179/2020 Z. z.)
    - ISO 27001 SOA
  - Jednotlivé požiadavky môžu byť v stave zavedené, v procese zavádzania, neaplikované alebo nezavedené,
  - Ku každej požiadavke je možné pripojiť komentár a záznam zo zoznamu bezpečnostných opatrení,
  - Hodnotenie je možné exportovať do súboru pdf.
- Plán kontinuity:
  - Všeobecné údaje o pláne kontinuity (názov, popis, dotknuté aktíva),
  - Definovanie členov analytického, výkonného a riadiaceho tímu,
  - Popis procesu a dokumentácia,
  - Export plánu obnovy do súboru.
- Auditný log pre zaznamenávanie aktivít v systéme:

- Systém zaznamenáva aktivitu používateľa (pridanie, zmena, vymazanie) pre konkrétne časti systému (aktívum, atribút aktíva, riziko, ..),
- Možnosť pozrieť stav pred vykonanou zmenou a po zmene.

- Vzdelávanie - E-learning:
  - Vytváranie kurzov, vzdelávacích aktivít s definovaním rôznych platností a podmienok pre splnenie.
  - Podpora práce používateľov na základe preddefinovaných rolí (lektor, účastník kurzu)
  - Synchronizácia kontaktov účastníkov kurzov, vzdelávacích aktivít cez MS Active Directory
  - Pre účastníkov kurzov, vzdelávacích aktivít sa z dôvodu absolvovania nevyžaduje registrácia.
  - Pozvanie účastníkov kurzov, vzdelávacích aktivít pomocou definovaných skupín a taktiež výberom konkrétneho účastníka.
  - Notifikovanie účastníkov kurzov, vzdelávacích aktivít v minimálnom rozsahu:
    - Nutnosť absolvovania kurzu, vzdelávacej aktivity
    - Blížiaci sa termín pre splnenie kurzu, vzdelávacej aktivity
  - Vytvorenie prehľadu absolvovaných kurzov a prehľad kurzov, ktoré účastníci musia absolvovať.
  - Vytvorenie prehľadu pre lektorov o absolvovaní kurzov a vzdelávacích aktivít, úspešnosti účastníkov a vyhodnotení priebežného stavu plnenia kurzu.
  - Evidencia dokumentov, s ktorými sa následne účastníci kurzov, vzdelávacích aktivít oboznamujú.
  - Vytváranie kontrolných testov pre overenie znalostí zamestnancov organizácie.
  - Štruktúra testovacích otázok musí byť bez obmedzení a v minimálnom rozsahu:
    - Odpoveď áno/nie
    - Výber z odpovedí
    - Odpoveď voľným textom
    - Správna odpoveď jedna až všetky
  - Testy sú možné automaticky vyhodnocovať a exportovať výsledky kurzov, vzdelávacích aktivít do tabuľkových výstupov.
- Všetky vyššie uvedené funkcionality a požiadavky kladené na SW nástroj musia byť súčasťou dodaného riešenia ako celku bez potreby využívania iných SW nástrojov.

Špecifické požiadavky na platformu pre bezpečnostné testovania zamestnancov NEDU:

- Platforma musí umožňovať vytváranie phishingových kampaní.
- Platforma obsahuje predpripravené email šablóny a stránky najčastejšie sa vyskytujúcich podvodov.
- Phishigová kampaň sa môže realizovať manuálne alebo prostredníctvom plánovača.
- Minimálne ukazovatele pre vyhodnocovanie phishigových kampaní je:
  - Počet odoslaných emailov,
  - Počet doručených emailov,
  - Počet otvorených emailov,

- Počet kliknutí na odkaz,
- Počet kliknutí na prílohu,
- Počet odpovedí na email.

- Reporting pre vyhodnocovanie úspešnosti phishingových kampaní.
- Platforma podporuje import používateľov z Active Directory
- Možnosť nastaviť akciu po úspešnom phishingu používateľa. (Napr. po kliknutí na podozrivú linku sa objaví vysvetlenie čo nesprávne používateľ vykonal.).
- Možnosť vytvorenia skupín používateľov, ktorý budú účastníkmi phishingovej kampane.
- Možnosť nastavenia školenia po absolvovaní phishingovej kampane.
- Zrealizovanie 2 samostatných phishingových kampaní zameraných na preverenie aktuálnej úrovne bezpečnostného povedomia zamestnancov NEDU, vytvorenie reportov z phishingových kampaní s podrobným výstupom.

Požiadavky pri realizácii primárnych aktivít:

- V rámci analýzy rizík (ďalej len „AR") vykonanie fyzickej objektovej obhliadky vo všetkých relevantných priestoroch NEDU súvisiacich s predmetom zákazky pre zmapovanie rizík a zraniteľností.
- Pravidelné osobné stretnutia v priestoroch NEDU s projektovým tímom pre prezentovanie priebežných výstupov a napredovanie v rámci projektu (minimálne 1x za 2 týždne).
- NEDU požaduje po ukončení analýzy rizík aj vypracovanie akčného plánu vrátane technických návrhov a časovým harmonogramom pre odstránenie identifikovaného nesúladu a zníženia rizík.
- Služby podpory počas projektu:
  - nahlásenia vád riešenia a konzultácii týkajúcich sa bežnej prevádzky riešenia,
  - dotazy na obchodnú podporu,
  - knowledge database, Q&A,
  - konzultácie licenčného modelu,
  - komunikácia s výrobcom.

B) Cieľom predkladaného projektu je realizácia sekundárnych aktivít, konkrétne:

- B.1 Nasadenie bezpečnostného monitoringu spojeného s riadením bezpečnosti prevádzky, ochrany koncových staníc a serverov.
  - Servre a kritické zariadenia
  - Pracovné stanice
  - Bezpečnostná konzola pre vyšetrovanie kybernetických incidentov
- B.2 Nasadenie systému na riadenie bezpečnosti sieti
  - Perimetrový firewall
  - Mailová brána
  - Swtich
  - Access Point
- B.3 Nasadenie Dvojfaktorovej autentifikácie
- B.4 Nasadenie technológie pre zálohovanie a obnovu dát.

B.1 Špecifikácia pre nasadenie bezpečnostného monitoringu spojeného s riadením bezpečnosti prevádzky, ochrany koncových staníc a serverov.

Servre a kritické zariadenia (ďalej len „**SP**").

ID	**Požiadavka**	**Konkrétne a zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
SP-1	SP musí podporovať nasledujúce operačné systémy na inštaláciu agenta: • Windows 2000 a novšie • Linux: • Red Hat 5 a novšie • Ubuntu 10 a novšie • CentOS 5 a novšie • Debian 6 a novšie • Amazon Linux • Oracle Linux 5 a novší • SUSE Linux 10 a novší • CLoud Linux 5 a novší • Solaris 10 a novší • AIX 5.3, 6.1, 7.1 a 7.2	Agentská aplikácia podporuje operačné systémy: Windows 2000, Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11 Windows Server 2003, Windows Server 2008 a 2008R2, Windows Server 2012 a 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 RedHat 5 - 9 Ubuntu 10.04 – 22.04 CentOS 5 – 8 Rocky Linux 8 Debian 6 - ++ Amazon Linux, Amazon Linux2 Oracle Linux 5 – 8 SUSE Linux 11, 12, 15 Cloud Linux 5 – 8 AlmaLinux 8 Solaris 10 – 11.4 AIX 6.1 – 7.3
SP-2	SP centrálna správa môže byť implementované onpremise alebo poskytovaná ako služba formou cloudu výrobcu.	Áno, riešenie môže byť implementované on-premise, alebo ako služba formou cloudu výrobcu.
SP-3	SP umožňuje jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému,	Áno, systém umožňuje prideľovanie prístupových práv ku uloženým udalostiam a ovládacím komponentom na základe priraďovaných rolí. Systém umožňuje vytváranie vlastných.
SP-4	SP obsahuje funkcionalitu antimalware pre detekciu a blokovanie škodlivého kódu na koncovom zariadení.	Áno, funkcia Anti-malware umožňuje detekciu a blokovanie škodlivého kódu (vírusy, trójske

		kone, spyware, grayware) na koncovom zariadení. Ochrana prebieha v reálnom čase (Real-time) a umožňuje plánovanie skenov pre vyhľadávanie škodlivého kódu a ručné spustenie vyhľadávania škodlivého kódu. Systém podporuje aj funkcionalitu prediktívneho Machine Learning, behaviorálny monitoring, ochranu pred exploitmi v dokumentoch
SP-5	SP podporuje funkcionalitu pre detekciu a blokovanie správania sa používateľa/útočníka pre detekciu podozrivých aktivít na koncovom zariadení.	Áno, systém podporuje funkcionalitu detekcie a blokácia správania sa používateľa / útočníka za účelom detekcie podozrivých aktivít na koncovom zariadení vrátane mapovania na MITRE ATT&CK.
SP-6	SP podporuje funkcionalitu web reputácie url pre detekciu a blokovanie komunikácie na potenciálne škodlivú / podozrivú cieľovú adresu	Áno, systém podporuje web reputáciu URL pre detekciu a blokovanie komunikácie na potenciálne škodlivú / podozrivú cieľovú adresu. Napr. servery Command & Control.
SP-7	SP podporuje funkcionalitu aplikačného monitorovania a blokovania spustenia podozrivého softvéru na koncovom zariadení.	Áno, systém podporuje aplikačný monitoring a blokovanie / povolenie podozrivého, alebo zmeneného softvéru na koncovom bode (PHP, Java, Python, ...), pričom je možné definovať časové okná potrebné pre plánované aktualizácie aplikácií.
SP-8	SP podporuje monitorovanie integrity súborov koncového zariadenia prostredníctvom vytvorenia baseline (stav integrity súborov definovanom čase)	Áno, systém podporuje monitorovanie integrity koncového zariadenia prostredníctvom vytvorených baseline (stav v danom čase). Monitoring obsahuje najmä kontrolu verzií súborov a ich HASH, stav služieb, hodnoty registrov.
SP-9	SP podporuje funkcionalitu inšpekcie logov a udalostí (log manažment) na koncovom zariadení. Podporuje natívne typy zdrojov udalostí	Áno, systém podporuje inšpekciu logov a udalostí (log manažment) koncového zariadenia. Podporuje natívne typy zdrojov udalostí logov

	(windows event log) ako aj vlastné zdroje logov vrátane parsovania zdrojových dát.	operačného systémov windows (windows event log) a natívneho typu zdrojov systémov linux, vrátane iných zdrojov logov (aplikačné logy) a parsovanie zdrojových dát.
SP-10	SP podporuje funcionalitu firewall pre detekciu a blokovanie škodlivej sieťovej komunikácie. Podporovaný je **režim odposluchu** - sieťová komunikácia nie je rušená, firewall funguje len v režime detekcie/logovania, vhodný na testovanie alebo **Inline režim** - sieťová komunikácia prechádza cez definované pravidlá a na prevádzku sa aplikujú definované akcie na základe zásad a nastavených pravidiel	Áno, firewall umožňuje detekciu a blokovanie škodlivej sieťovej komunikácie. V móde odposluchu (TAP) pre detekciu a v móde in-line, kde sieťová komunikácia môže byť okrem detekcia aj blokovaná. Systém obsahuje množstvo predvolených firewallových pravidiel a umožňuje tvorbu vlastných firewallových pravidiel.
SP-11	SP podporuje detekciu a blokovanie pokusov o skenovanie siete aleboportov alebo techník ako TCP SYNFIN,TCP XMAS, TCP null a podobných.	Áno, detekcia pokusov o skenovanie siete, portov, alebo techník je podporovaná: OS Fingerprint Probe, TCP Null Scan, TCP SYNFIN Scan, TCP XMAS Scan, Network Scan, Port Scan
SP-12	SP podporuje detekciu a prevenciu prienikov (IDS resp IPS) pre podozrivú sieťovú komunikáciu.	Áno, systém podporuje detekciu a prevenciu (IDS a IPS) podozrivej sieťovej komunikácie koncového bodu.
SP-13	SP podporuje automatické skenovanie, ktoré skenuje operačný systém, zisťuje verziu operačného systému, zisťuje nainštalované aktualizácie, zisťuje nainštalované programy a ich verzie a odporúča príslušné pravidlá IPS (tzv. virtuálne záplaty).	Áno, systém podporuje automatizované skeny operačného systému, jeho verzie, nainštalované aplikácie, spustené služby a programy 3tích strán, pričom chýbajúce aktualizácie operačného systému, nainštalovaných aplikácií, spustených služieb a programov 3tích strán sú zdrojom pre automatizovaný výber príslušných IDS / IPS pravidiel (virtuálne záplaty).
SP-14	SP podporuje kontrolu sieťovej komunikácie SSL/TLS (nahraním certifikátu so súkromným kľúčom,	Áno, systém podporuje SSL/TLS inšpekciu sieťovej komunikácie

	ktorý sa používa na dešifrovanie obsahu)	koncového bodu nahratím certifikátu so súkromným kľúčom, ktorý sa používa na dešifrovanie obsahu.
SP-15	SP obsahuje funkcionalitu tzv. virtual patching prostredníctvom IPS pravidiel pre blokovanie zneužitia známych zraniteľností (log4shell, ..)	Áno, funkcionalitu virtual patchingu pre známe zraniteľnosti systém realizuje prostredníctvom IPS pravidiel (log4shell, log4j, MS Exchange, ...)
SP-16	SP podporuje inbound a outbound aplikačné integračné rozhranie API	Áno, integračné rozhranie RESTful API pre inbound a outboud.
SP-17	SP podporuje tvorbu vlastník politík pre všetky funkcionality a ich aplikovanie na jednotlivé koncové zariadenia alebo skupiny zariadení.	Áno, systém umožňuje tvorbu vlastných politík pre všetky funkcionality. Politiky je možné prideľovať hromadne pre viacero koncových zariadení, a/alebo jednotlivo pre dané koncové zariadenie. Tvorba politík a stromovej štruktúry politík obsahuje aj funkcionalitu dedenia.

Pracovné stanice (ďalej len „**EP**").

ID	**Požiadavka**	**Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
EP-1	EP musí podporovať nasledujúce operačné systémy na inštaláciu agenta: Windows 7 a novšie MacOS 10.13 a novšie.	Áno, systém podporuje operačné systémy: Windows 7, Windows 8.1, Windows 10 Windows 11, Windows Server 2008R2, Windows Server 2012, Windows Server 2016, Windows Server 2019 Windows Server 2022 macOS 10.13, mcOS 10.14, macOS 10.15, macOS 11, macOS 12
EP-2	EP umožňuje prepojenie s Active Directory	Áno, systém umožňuje integráciu s Active Directory.
EP-3	EP obsahuje funkcionalitu antimalware pre detekciu a blokovanie škodlivého kódu na koncovom zariadení.	Áno, funkcionalita Anti-malware umožňuje detekciu a blokovanie škodlivého kódu (vírusy, trójske

		kone, spyware, grayware) na koncovom zariadení. Ochrana prebieha v reálnom čase (Real-time) a umožňuje plánovanie skenov pre vyhľadávanie škodlivého kódu a ručné spustenie vyhľadávania škodlivého kódu. Systém podporuje aj funkcionalitu prediktívneho Machine Learning, behaviorálny monitoring, ochranu pred exploitmi v dokumentoch.
EP-4	EP podporuje funkcionalitu pre detekciu a blokovanie správania sa používateľa/útočníka pre detekciu podozrivých aktivít na koncovom zariadení.	Áno, systém podporuje funkcionalitu detekcie a blokácie správania sa používateľa / útočníka za účelom detekcie podozrivých aktivít na koncovom zariadení.
EP-5	EP podporuje funkcionalitu web reputácie url pre detekciu a blokovanie komunikácie na potenciálne škodlivú / podozrivú cieľovú adresu	Áno, systém podporuje web reputáciu URL pre detekciu a blokovanie komunikácie na potenciálne škodlivú / podozrivú cieľovú adresu. Napr. servery Command & Control.
EP-6	EP podporuje funkcionalitu aplikačného monitorovania a blokovania spustenia podozrivého softvéru na koncovom zariadení. Aplikáciám je možné definovať: • povoliť/zakázať iba konkrétnu verziu aplikácie alebo novšiu/staršiu verziu. • Typ aplikácie (web. Prehliadač, hra, vývojárske nástroje, ovládače, ...) • Či aplikácia môže spustiť inú aplikáciu (ďalšia úroveň) alebo ľubovoľný počet aplikácií (ľubovoľná úroveň) • Cesta k súboru (reťazec alebo regulárny výraz) • Certifikát (platný / vypršal /nedôveryhodný a dotazovanie akejkoľvek časti C, L, CN, O, OU, ...) • Hodnota hash (SHA1, SHA-256) Riešenie obsahuje vlastnú databázu aplikácií, ktorú možno použiť na nastavenie politiky	Áno, systém podporuje aplikačný monitoring a blokovanie / povolenie podozrivého, alebo zmeneného softvéru. Vytvárať inventáre softvéru a a vytvárať politiky.

	povolených/zakázaných aplikácií. Podpora nastavení dedičnosti, možnosť definovať, či povolená aplikácia môže alebo nemôže spúšťať iné (nedefinované) aplikácie.	
EP-7	EP podporuje funkcionalitu Anti-ransomware (blokuje proces vykonávajúci neoprávnené šifrovanie a obnovenie dátových súborov zo zálohy)	Áno, funkcionalita Anti-Ransomware blokuje proces/procesy vykonávajúce neoprávnené šifrovanie súborov a vykonáva obnovu dátových súborov zo zálohy.
EP-8	EP podporuje funkcionalitu Data Lost prevention/application contro: • Blokovanie funkcie AutoRUN na USB • Môže povoliť/zakázať prístup k jednotkám USB na základe výrobcu jednotky, modelu i • špecifické sériové číslo. Riešenie obsahuje nástroj, ktorý poskytuje tieto informácie o • každý disk. Možno zablokovať/povoliť: • Bluetooth • COM • LPT • IEEE 1394 • Infračervené zariadenia • Modemy • Bezdrôtové sieťové adaptéry • Mobilné zariadenia Môžete povoliť práva (FULL, Modify, ReadExecute, Read, Block) pre nasledujúce položky, • Programy, ktoré pristupujú k úložisku, aj programy, ktoré pristupujú k • úložisko: • CD/DVD • Sieťové jednotky • Úložné zariadenia USB	Áno, agentská aplikácia podporuje funkcionalitu DLP a Device control so správou prístupu ku externým zariadeniam. Blokovanie funkcionality AUTORUN na USB jednotkách s možnosťou povolenia / blokovania na základe zoznamov (výrobca, model, sériové číslo). Prípadne zariadeniach, ktoré nie sú USB úložiská. Systém obsahuje nástroj pre umožňujúci zobrazenie zoznamu práve pripojených zariadení. Ochrana zariadení, ktoré nie sú úložiskom je podporovaná pre nasledovné zariadenia: Bluetooth adaptéry, COM a LPT porty (sériové a paralelné), FireWire (IEEE 1394, skenery/kamery, infračervené zariadenia, modemy, čítačky/karty PCMCIA, klávesu Print screen a bezdrôtové sieťové adaptéry. Ochrana zariadení, ktoré sú úložiskom je podporovaná pre nasledovné zariadenia: USB, CD/DVD, Floppy disk, Sieťové disky Riadenie prístupu ku zariadeniam, ktoré sú úložiskom umožňujú

		nastaviť oprávnenia: Full access, Modify, Read&Execute, Read, List device content only, Block.
EP-9	EP podporuje detekciu a prevenciu prienikov (IDS resp. IPS) pre podozrivú sieťovú komunikáciu.	Áno, systém podporuje funkcionalitu IDS/IPS pre podozrivú sieťovú komunikáciu.

Bezpečnostná konzola pre vyšetrovanie kybernetických incidentov (ďalej len „**IM**").

ID	**Požiadavka**	**Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
IM-1	Centrálna jednotná konzola pre vyšetrovanie incidentov/SoC s podporou napojenia a zdieľania podozrivých objektov minimálne pre - Servery - Pracovné stanice - Perimetrový firewall - Email	Áno. Podporuje. Konzola je dostupná cez webový prehliadač. Je možné integrovať pracovné, stanice, servery a cez api rozhranie aj perimetrový firewall a email (napr. Pre výmenu suspicious object.
IM-2	Riešenie pre účely detekcie obsahuje nasledujúce funkcionality: - Analýza prostredníctvom sandbox s možnosťou automatizovaného alebo manuálneho nahrávania vzoriek - Detekčné modely ktoré korelujú logy z koncových staníc a serverov - Detekcia na základe IOC (Indicator of Compromise) - Detekcia zraniteľností na koncovom zariadeniach	Áno. Riešenie má k dispozícii sandbox prostredie,ktoré umožňuje analýzun manuálne nahraním napr. Súboru alebo prostredníctvom integrácie alebo API. Detekčné modely korelujú telemetrické dát z pracovných staníc a serverov. Je možné taktiež importovať IOC a prehliadať koncové body na ich prítomnosť. Na podporovaných zariadeniach dú detegované zraniteľnosti.
IM-3	Podporuje vyhľadávanie nasledujúcich objektov z hladiska detekcie indikátorov kompromitácie • Doména • EndpointID • Názov hostiteľa • IP adresa (v4 a v6) • Cesta k súboru na disku • MD5, SHA1, SHA2 súboru • Názov súboru • Prístav	Podpoorujeme vyhľadávanie cez aplikáciu Search pre uvedené ale aj dalšie objekty.

	• Cesta k spracovaniu • Názov procesu • Kľúč registra • Hodnota v registri • Údaje v registri • Taktiky spoločnosti MITRE • Technika MITRE • ADRESA URL • Používateľské konto • Príkaz z príkazového riadku	
IM-4	Možnosť manuálneho zadávania objektov IOC a iných spravodajských informácií o hrozbách, ktoré sa potom môžu použiť na prehľadávanie. Podpora pre: - STIX . - CSV - TAXII - MISP	Podporujeme. Manuálne alebo prostredníctvom importu.
IM-5	Z hľadiska vyšetrovanie riešenie poskytuje - Vypracovanie analýzy hlavných príčin (profil vykonania) - Zobrazenie profilu objektu (ako bol vykonaný, kde bol dotazovaný, čo spustil atď...) - Identifikácia dopadu, informácie o výskyte detekcie v sieti - Zobrazenie podrobných informácií o objekte, napríklad parametrov príkazu z príkazového riadku	Ano. Workbench, Incident a Execution Profile.
IM-6	Z hladiska reakcie na incident alebo udalosť podporuje nasledujúce možnosti vykonať akciu na koncovom zariadení: • Ukončenie (bežiaceho) procesu • Stiahnutie súboru z koncového bodu (napríklad na ďalšiu analýzu) • Pridanie objektu do zoznamu blokovaných • Odstránenie objektu zo zoznamu blokovaných • Izolácia koncového bodu (Endpoint) • Obnovenie pripojenia k izolovanému zariadeniu	Podporujeme. Pre každý typ integrovaného zariadenia sú k dispozícii relevantné zdroje.

	• Pripojenie k príkazovému riadku stanice • Spustenie skriptu PowerShell/Bash • Odoslanie súboru/priečinka do služby Sandbox	
IM-7	Riešenie podporuje aj automatizáciu ako napr. - Nastavenie automatických reakcií na základe detekcie (napríklad automatická izolácia agenta v sieti) - Automatické vykonávanie skriptov na definovaných staniciach - Upozornenie pri zistení novej kritickej zraniteľnosti	Áno. Prostredníctvom Security Playbooks.

B.2 Nasadenie systému na riadenie bezpečnosti sieti

Perimetrový firewall (ďalej len „**NGFW**").

ID	**Požiadavka**	**Konkrétne a zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
	HW appliance NGFW/UTM firewallu v režime vysokej dostupnosti (dve fyzické zariadenia rovnakého typu zapojené do funkčného clustra); Platforma postavená na HW akcelerovanej architektúre (t.j. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií ; HW appliance do racku s veľkosťou 1RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu; Možnosť doplniť druhý napájací zdroj (interný alebo externý), alebo zariadenie vybavené dvoma zdrojmi;:	Áno. Spĺňa. Riešenie je dodávané vo forme HW applince vo formáte 1RU.
NGFW-1	Rozhrania na každom firewalle využiteľné pre management: min. 1x GE RJ45	Áno. 1x GE RJ45, 16 x GE RJ45, 8x GESFP Slots, 4x 10 GE SFP+ Slots. Podpora Active-Active akko aj Active- Passive
	Rozhrania na každom firewalle využiteľné pre spracovanie komunikácie: min. 16x GE RJ45 Ports, 8x GE SFP Slots, 4x 10 GE SFP+ Slots	
	Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý	

	cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky.:	
	Podpora VLAN: min. 4000	
	Podpora LACP	
NGFW-2	Počet FW pravidel: min. 8000	Podporuje.
NGFW-3	Možnosť definície FW pravidel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je::min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.	Podporuje
NGFW-4	Celková priepustnosť firewallu: min. 27/27/11 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B)	Podporuje uvedenú priepustnosť.
NGFW-5	Latencia firewallu: nepresahuje 5 µs (merané na malých UDP paketoch (64B))	Áno
NGFW-6	Počet nových spojení za sekundu (setup-rate): min. 270000	Podporuje
NGFW-7	Celkový počet súčasných TCP spojení firewallu: min. 3000000	Podporuje
NGFW-8	PPS (počet spracovaných paketov za 1 sekundu):min. 16000000	Podporuje
NGFW-9	Funkcia detekcie aplikácií na L7 (Application Control)	Zariadenie deteguje aplikácie nielen na úrovni portov ale aj služieb resp. Aplikácií,ktoré tieto spojenia realizujú
NGFW-10	Detekcia známych aplikácií na základe signatúr: min 3500 preddefinovaných aplikácií/signatúr	Áno.
NGFW-11	pre populárne cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii)	Áno.
NGFW-12	aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu	Áno
NGFW-13	priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response): min. 12 Gbps	Podporuje

NGFW-14	podpora použitia Application control aj formou profilov priradených k pravidlám	Podporuje
NGFW-15	Funkcie detekcie a zamedzenia narušení (IPS/IDS)	Podporuje. Systém ma modul Intrusion Detection Systém (neblokuje ale len deteguje) alebo Intrusion Prevention System (aj blokácia)
NGFW-16	počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom: min. 11000	Podporuje
NGFW-17	funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám	Podporuje
NGFW-18	možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS	Podporuje tvorbu vlastných IPS pravidiel.
NGFW-19	priepustnosť funkcie IPS vrátane logovania: min. 5 Gbps	Áno. Podporuje.
NGFW-20	Funkcie antivírovej kontroly	Podporuje kontrolu prstredníctvom AV jadra výrobcov.
NGFW-21	Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom:	Podporuje
NGFW-22	AV kontrola rozšírená o inšpekciu tzv. sandbox technikou:Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky	Podporuje. Bud Cloud alebo OnPremise sandbox
NGFW-23	Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním: min. 3 Gbps	Ano. Podporuje
NGFW-24	Podpora služby výrobcu umožňujúca detekovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hash-ov:	Podporuje
NGFW-25	Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky:	Podporuje
NGFW-26	Podpora SSL dešifrovania/SSL inšpekcie: min. 4 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou)	Podpora SSL inšpekcie
NGFW-27	Funkcia DNS filtra:	

NGFW-28	Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii	Podporuje
NGFW-29	Možnosť definovať vlastný tzv. blacklist domén	Podporuje
NGFW-30	Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL	Podporuje
NGFW-31	Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos	Podporuje
NGFW-32	Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri	Podporuje
NGFW-33	Podpora SSL VPN	Ánp. Je možné sa pripojiť cez SSL portál
NGFW-34	Priepustnost SSL VPN:min. 2 Gbps	Podporuje
NGFW-35	Popora IPSEC VPN v režime site-2-site aj client-2-site:	Podporuje
NGFW-36	Priepustnosť IPSEC VPN (AES256-SHA256, UDP packet size 512B):min. 12 Gbps	Áno. Je monžé sa pripojiť cez IPSEC VPN.

Mailová brána (ďalej len „**MGW**“).

ID	**Požiadavka**	**Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
MGW-1	minimálne 4x GE RJ45	Zariadenie obsahuje 4 x GE RJ45
MGW-2	Kapacita úložného priestoru minimálne 1TB	Úložná kapacita 1 x 1TB
MGW-3	Počet chránených e-mailových domén minimálne 20	Minimálne 20 podporuje.
MGW-4	Počet e-mail schránok minimálne 150	Podporuje
MGW-5	Minimálny počet politík na doménu 60	Podporuje
MGW-6	Minimálny počet politík na systém 300	Podporuje
MGW-7	Kapacita spracovania minimálne 45000 e-mailov za hodinu	Podporuje
MGW-8	Kapacita spracovania e-mailov pri nasadení antivírusovej a antispamovej kontroly 40000 za hodinu	Podporuje
MGW-9	Maximálna spotreba elektrickej energie 65 W	Podporuje

MGW-10	Požadovaná montáž do racku veľkosti 1U	Riešenie je dodávané v rackovom formáte 1U
MGW-11	Požadovaný je výkonný anti-malware zahŕňajúci heuristické a behaviorálne techniky s prevenciou šírenia vírusov	Podporuje
MGW-12	Požadovaná je viacvrstvová ochrana proti spamu, analýza reputácie, filtrovanie pripojení, autentifikácia a metódy overovania príjemcov. Kontroly zahŕňajúce IP, doménu, odosielateľa, SPF, DKIM, DMARC a geografické obmedzenia.	Podporuje
MGW-13	Požiadavka je kladená na súbor funkcií na prevenciu straty údajov, šifrovanie e-mailov bezpečnosť doručenia citlivých e-mailov, ochrana proti neúmyselnej strate údajov.	Podporuje
MGW-14	Sledovanie prehľadov činností v reálnom čase, používateľské rozhranie umožňujúcu prehľadnú jednoduchú kontrolu nad e-mailovou prevádzkou.	Podporuje

Switch typ A (ďalej len „**SW1**") – odhadovaný počet 3 ks.

ID	**Požiadavka**	**Konkrétne a zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
SW1-1	minimálne 48x GE RJ45	Zariadenie obsahuje 48 x GERJ45
SW1-2	minimálne 4x 10 GE SFP+, ktoré sú však zároveň kompatibilne aj s 1 GE SFP	Zariadenie obsahuje 4 x 10 GE SFP
SW1-3	Minimálna prepínacia kapacita (Duplex) 176 Gbps	Ano. Podporuje
SW1-4	Minimálne spracovanie počtu paketov za sekundu 262 Mpps	Ano. Podporuje
SW1-5	Latencia menej ako 1µs	Ano. Podporuje
SW1-6	Minimálny počet podporovaných VLAN: 4096	Podporuje
SW1-7	Podpora spájania zariadení do logického celku	Podporuje
SW1-8	Možnosť zapojenia redundantného napájacieho zdroja	Zariadenie podporje zapojenie redundantného zdroja.
SW1-9	Smer prúdenia a odvod vzduchu zo strany do zadu (side-to-back)	Podporuje
SW1-10	Podpora Auto-negotiation	Podporuje
SW1-11	Podpora Jumbo Frame	Podporuje
SW1-12	Podpora DHCP Relay	Podporuje
SW1-13	Podpora DHCP snooping	Podporuje

SW1-14	Podpora RBAC	Podporuje
SW1-15	Podpora QoS 802.1p	Podporuje
SW1-16	Podpora 802.3ad Link Aggregation	Podporuje
SW1-17	Podpora 802.1q VLAN tagging	Podporuje
SW1-18	Podpora STP, RSTP, MSTP vrýtane rozšírenia BPDU guard, Root guard, Loop guard	Podporuje
SW1-19	Podpora IEEE 802.1ab LLDP-MED	Podporuje
SW1-20	Zrkadlenie sieťových rozhraní	Podporuje
SW1-21	Podpora Radius CoA (Change of Authority)	Podporuje
SW1-22	Podpora 802.1x Radius	Podporuje
SW1-23	Podpora Radius Accounting	Podporuje
SW1-24	Podpora ACL	Podporuje
SW1-25	Podpora SNMP a syslog	Podporuje
SW1-26	SSH a HTTPS management	Podporuje
SW1-27	Podpora REST API pre konfiguráciu a monitorovanie prvkov	Podporuje
SW1-28	prepínače musia byť plne integrovateľné s firewall platformou ako na funkčnej, tak na riadiacej úrovni	Podporuje
SW1-29	plnou funkčnou integráciou je myslené minimálne:	Podporuje
SW1-30	jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu	Ano. Riesenie je mozne doplnit o spravovanie cez centrálnu konzulo manager.
SW1-31	vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používateľa (firewally, prepínače, Wireless Prístupové body, koncové stanice/užívatelia)	Podporuje
SW1-32	koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice	Podporuje
SW1-33	možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno	Podporuje

SW1-34	vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií	Podporuje
SW1-35	možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme	Podporuje
SW1-36	vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia	Podporuje
SW1-37	integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo užívateľského mena	Podporuje
SW1-38	možnosť hromadnej aktualizácie (upgrade) firmware-u prepínačov z centrálnej konzoly	Podporuje
SW1-39	podpora spájania niekoľkých fyzických prepínačov do jedného logického prepínača	Podporuje

Switch typ B (ďalej len „**SW2**") – odhadovaný počet 10 ks.

ID	**Požiadavka**	**Konkrétne a zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
SW2-1	minimálne 24 x GE RJ45	Zariadenie obsahuje 24 x GE RJ45
SW2-2	minimálne 4 x 10 GE SFP+, ktoré sú však zároveň kompatibilne aj s 1 GE SFP	Zariadenie obsahuje 4 x 10 GE SFP
SW2-3	Minimálna prepínacia kapacita (Duplex) 128 Gbps	Podporuje
SW2-4	Minimálne spracovanie počtu paketov za sekundu 204 Mpps	Podporuje
SW2-5	Latencia menej ako 1µs	Podporuje
SW2-6	Minimálny počet podporovaných VLAN: 4096	Podporuje
SW2-7	Podpora spájania zariadení do logického celku	Podporuje
SW2-8	Možnosť zapojenia redundantného napájacieho zdroja	Podporuje zapojenie redundatného napájacieho zdroja

SW2-9	Smer prúdenia a odvod vzduchu zo strany do zadu (side-to-back)	Podporuje
SW2-10	Podpora Auto-negotiation	Podporuje
SW2-11	Podpora Jumbo Frame	Podporuje
SW2-12	Podpora DHCP Relay	Podporuje
SW2-13	Podpora DHCP snooping	Podporuje
SW2-14	Podpora RBAC	Podporuje
SW2-15	Podpora QoS 802.1p	Podporuje
SW2-16	Podpora 802.3ad Link Aggregation	Podporuje
SW2-17	Podpora 802.1q VLAN tagging	Podporuje
SW2-18	Podpora STP, RSTP, MSTP vrátane rozšírenia BPDU guard, Root guard, Loop guard	Podporuje
SW2-19	Podpora IEEE 802.1ab LLDP-MED	Podporuje
SW2-20	Zrkadlenie sieťových rozhraní	Podporuje
SW2-21	Podpora Radius CoA (Change of Authority)	Podporuje
SW2-22	Podpora 802.1x Radius	Podporuje
SW2-23	Podpora Radius Accounting	Podporuje
SW2-24	Podpora ACL	Podporuje
SW2-25	Podpora SNMP a syslog	Podporuje
SW2-26	SSH a HTTPS management	Podporuje
SW2-27	Podpora REST API pre konfiguráciu a monitorovanie prvkov	Podporuje
SW2-28	prepínače musia byť plne integrovateľné s firewall platformou ako na funkčnej, tak na riadiacej úrovni	Podporuje
SW2-29	plnou funkčnou integráciou je myslené minimálne:	Podporuje

SW2-30	jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu	Podporuje
SW2-31	vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používatela (firewally, prepínače, Wireless Prístupové body, koncové stanice/užívatelia)	Podporuje
SW2-32	koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice	Podporuje
SW2-33	možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno	Podporuje
SW2-34	vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií	Podporuje
SW2-35	možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme	Podporuje
SW2-36	vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia	Podporuje
SW2-37	integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo užívatelského mena	Podporuje
SW2-38	možnosť hromadnej aktualizácie (upgrade) firmware-u prepínačov z centrálnej konzoly	Podporuje
SW2-39	podpora spájania niekoľkých fyzických prepínačov do jedného logického prepínača	Podporuje

Access Point (ďalej len „**AP**").

ID	Požiadavka	**Konkrétne** a **zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
AP-1	AP musí byť plne integrované s firewall platformou dopytovanou v tomto výberovom konaní ako na funkčnej, tak na manažment úrovni.	Podporuje. Riešenie je priamo manžovatelné cez firewall platformu
AP-2	plnou funkčnou integráciou je myslené najmä:	
AP-3	automatická alebo manuálna autorizácia AP na základe auto discovery mechanizmu	Podporuje
AP-4	jednotné manažment rozhranie, z ktorého je možné spravovať AP aj firewally	Podporuje
AP-5	vizualizácie logickej i fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/užívateľa (firewally, switche, koncové stanice/užívatelia)	Podporuje
AP-6	koncové zariadenia musia byť v jednotnom manažment rozhraní graficky zobrazené vrátane minimálne nasledujúcich informácií: názov zariadenia, verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia k sieti, počet otvorených spojení, množstvo prenesených dát, počet paketov, aktuálne využitá šírka pásma	Podporuje
AP-7	možnosť vyhľadávania konkrétnych zariadení alebo užívateľa na základe minimálne nasledujúcich parametrov: IP adresa, MAC adries, užívateľské meno	Podporuje
AP-8	vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií	Podporuje
AP-9	možnosť manuálneho alebo automatického vloženia zariadenia do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme	Podporuje
AP-10	vizualizácia množstva prenesených dát na jednotlivých AP. Možnosť konfigurácie časového intervalu tohto zobrazenia.	Podporuje
AP-11	možnosť hromadného upgrade firmware AP z centrálnej konzoly	Podporuje
AP-12	Formát AP: indoor	Podporuje

AP-13	Počet rádií: 3+1 BLE	Podporuje
AP-14	Minimálne 2x2 MU-MIMO	Podporuje
AP-15	Bleutooth rádio pre lokalizačné služby	Podporuje
AP-16	Súčasná podpora 2,4 GHz a 5GHz pásma	Podporuje
AP-17	Podpora štandardu 802.11ax	Podporuje
AP-18	2x 10/100/1000 Base-T RJ45, 1x Type 2.0 USB, 1x RS- 232 RJ45 Serial Port	Podporuje
AP-19	Počet SSID: 14	Podporuje
AP-20	Cellular Co-existencia	Podporuje
AP-21	Kapacita množstva klientov pre jednotlivé rádio minimálne do 512	Podporuje
AP-22	Maximálna spotreba energie 17W	Podporuje
AP-23	Podpora BSS Coloring	Podporuje
AP-24	Podpora TWT (Target Wake Time)	Podporuje
AP-25	Spektrálna analýza	Podporuje
AP-26	Kensigton lock	Podporuje

B.3 Nasadenie Dvojfaktorovej autentifikácie (ďalej len „**MFA**").

ID	**Požiadavka**	**Konkrétne a zrozumiteľne** popíšte akým spôsobom napĺňate uvedenú požadovanú funkcionalitu.
MFA-1	Virtual appliance poskytujúci funkcionality pre manažment identít, Plnohodnotná AAA funkcionalita, Integrované funkcie AAA pre pripojenie z VPN.	Riešenie dodávané formou VM appliance. Podporuje požadovanú funkcionalitu.
MFA-2	Podpora pre 200 používateľov	Podporuje
MFA-3	Autorizácia prístupu do siete kombináciou minimálne nasledujúcich parametrov - identita (meno/heslo, certifikát) pripájajúceho sa používateľa, identita (MAC adresa, certifikát) pripájajúceho sa zariadenia, čas pripojenia do siete a spôsob pripojenia do siete (wifi/LAN/VPN).	Podporuje
MFA-4	Podpora RADIUS, RADIUS CoA, RADIUS Accounting proxy s možnosťou úpravy atribútov a s možnosťou statického alebo dynamického vkladania hodnôt do atribútov	Podporuje
MFA-5	Možnosť využitia Radius Accounting proxy v režime kedy je jeden Radius MSG pomocou proxy rozosielaný na viacero zariadení	Podporuje
MFA-6	Podpora TACACS+ s možnosťou autorizácie príkazov alebo služieb	Podporuje

MFA-7	Podpora viacerích databáz identít.	Podporuje
MFA-8	Možnosť automatického importovania užívateľov zo vzdialených LDAP serverov	Podporuje
MFA-9	Podpora LDAP cez SSL.	Podporuje
MFA-10	Podpora Kerberos	Podporuje
MFA-11	Podpora EAP metód - EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-GTC	Podporuje
MFA-12	Podpora autentifikácie pre klientov nepodporujúcich 802.1x	Podporuje
MFA-13	Podpora REST API pre väčšinu základných úkonov AAA platformy	Podporuje
MFA-14	Logovanie činností, úspešných aj neúspešných pokusov o prihlásenie v reálnom čase.	Podporuje
MFA-15	Podpora LAN a WLAN portálu pre hostí s HTTP/HTTPS autentizáciou. Možnosť vytvárania dočasných užívateľských účtov pre návštevníkov prostredníctvom prispôsobiteľného užívateľského rozhrania oddeleného od hlavného administratívneho rozhrania.	Podporuje
MFA-16	Guest portál musí podporovať možnosť prihlasovania prostredníctvom účtov minimálne týchto sociálnych sietí – LinkedIn, Facebook, Twitter, Google+. Portál musí umožňovať bohatú grafickú úpravu vrátane možnosti pridávania videí a ďalšieho dynamického obsahu. Možnosť samoobslužnej registrácie hosťa do siete so SMS alebo email overením.	Podporuje
MFA-17	Podpora BYOD, možnosť bezpečnej registrácie súkromných zariadení do internej siete na základe užívateľských údajov z externej autentizačnej databázy ako napr. AD či LDAP. Užívateľ musí byť schopný jednoduchým užívateľským wizardom nainštalovať osobný certifikát na svoje súkromné zariadenie.	Podporuje
MFA-18	Certifikačná autorita na vydávanie certifikátov pre súkromné zariadenia musí byť súčasťou AAA platformy.	Podporuje
MFA-19	Podpora protokolu SCEP.	Podporuje
MFA-20	Hostia alebo interní užívatelia musia mať možnosť prístupu do samoobslužného portálu na správu svojich nastavení alebo zmenu hesla.	Podporuje
MFA-21	Podpora viacfaktorovej autentifikácie pomocou OTP tokenov	Podporuje
MFA-22	Podpora HW aj SW tokenov	Podporuje

MFA-23	Podpora SW tokenov pre mobilné platformy Android, iOS, Windows Mobile	Podporuje
MFA-24	Podpora OAUTH, SAML IdP	Podporuje
MFA-25	Podpora SSO na základe informácií získaných z SAML, Windows Event Log, Radius Accounting a Syslog	Podporuje

C) **Rámcové konzultačné práce na obdobie 1 roka v predpokladanom objeme:**

- pravidelná kontrola funkčnosti nástrojov,
- poskytnutie updatov, upgradov a patchov pre riešenia,
- pravidelná kontrola funkčnosti zberu dát,
- pravidelná kontrola konfiguračných nastavení a aktuálneho stavu komponentov,
- podpora pri riešení kybernetických bezpečnostných incidentov,
- aktualizácia smerníc.

Vyššie je uvedený minimálny rozsah požiadaviek na produkty, ktoré projekt dodáva. Uchádzač má možnosť rozšíriť spektrum ponúknutých a v prípade úspechu uchádzača aj dodanie produktov nad rámec týchto minimálnych požiadaviek. Produktom nad rámec minimálnych požiadaviek sa rozumie dokument alebo software, ktorý tematicky rozširuje dodávané produkty na základe skúsenosti dodávateľa z historicky realizovaných projektov obdobného charakteru, tak by verejný obstarávateľ dosiahol ďalšie kroky potrebné k realizácii auditu kybernetickej bezpečnosti. Cieľom je, aby verejný obstarávateľ dostal produkt so zvýšenou hodnotou za ekonomicky najlepších podmienok (ekvivalentné plnenie predmetu zákazky musí spĺňať ten istý účel použitia a musia mať kvalitatívne rovnaké alebo lepšie vlastnosti a technické parametre, ako je požadované pri pôvodnom predmete zákazky, tzn. spĺňajú úžitkové, prevádzkové a funkčné charakteristiky).

Verejný obstarávateľ požaduje, aby realizáciu predmetu zákazky úspešný uchádzač zabezpečoval prostredníctvom osôb, ktoré sú technicky a odborne spôsobilé na jeho realizáciu. Verejný obstarávateľ požaduje, aby úspešný uchádzač vykonal fyzickú obhliadku priestorov a konkrétnych zariadení výpočtovej techniky verejného obstarávateľa za účelom zistenia skutkového stavu a určenia potencionálnych fyzicko-objektových rizík.

Pri návrhu ceny je potrebné zohľadniť nasledovné skutočnosti:
• kompatibilita navrhovaných riešení s existujúcim HW a SW vybavením verejného obstarávateľa,
• spolupráca s personálom verejného obstarávateľa pri implementovaní zákazky.

1. Formy spolupráce a súčinnosti

Miestom realizácie predmetu zákazky je sídlo verejného obstarávateľa.
V prípade technologických opatrení verejný obstarávateľ požaduje konkrétny technologický návrh na základe technickej špecifikácie a parametrov informačnej siete verejného obstarávateľa. Uchádzač vytvorí dokument s presným technickým popisom riešenia a špecifikáciami hardvéru resp. softvéru.
Vedeniu verejného obstarávateľa budú na schválenie predložené vypracované smernice, a najmä spôsob riadenia (mitigácie) identifikovaných rizík z aktualizovanej AR/BIA, čo zabezpečí formálne zadefinovanie procesov pre oblasť riadenia IB a KyB.

Z pohľadu technických opatrení budú do praxe zavedené bezpečnostné informačné systémy, aplikácie a riešenia, ktoré prispejú najmä k včasnej identifikácii bezpečnostných incidentov, ich efektívnemu a rýchlemu riešeniu a k celkovému zvýšeniu úrovne IB a KyB v rámci verejného obstarávateľa.
Hardvérové vybavenie predmetu zákazky požaduje verejný obstarávateľ dodať vrátane dopravy a so zapojením a spustením v serverovni za prítomnosti administrátora IT verejného obstarávateľa.
Projekt je realizovaný s cieľom rozšíriť spôsobilosti v oblasti informačnej a kybernetickej bezpečnosti v rámci verejného obstarávateľa a zabezpečiť súlad so zákonom o ITVS a zákonom o KyB.

Financovanie aktivít predmetu zákazky bude realizované formou projektu podporeného z dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach".
Implementáciou bezpečnostných opatrení a následným ukončením realizácie predmetu zákazky bude verejný obstarávateľ spĺňať legislatívne požiadavky vyplývajúce z informačnej a kybernetickej bezpečnosti a legislatívy k ITVS. Zároveň bude verejný obstarávateľ pripravený na úspešný audit v kybernetickej bezpečnosti.

2. Záruka a záručná doba

Záručná doba na poskytnuté služby
Všetky skutočnosti, ktoré budú počas realizácie predmetu zákazky vyhodnotené ako nezhody, sú predmetom záruky a úspešný uchádzač je povinný navrhnúť opatrenia na ich odstránenie.

Záruka a záručná doba a podpora softvérového vybavenia predmetu zákazky
- Softvérové licencie z predmetu zákazky požaduje verejný obstarávateľ s podporou min. 24 mesiacov

Záruka a záručná doba hardvérového vybavenia predmetu zákazky
- Záruka pre hardvérové vybavenie z predmetu zákazky min. 24 mesiacov

3. Termín realizácie predmetu zákazky/zmluvy

Ukončenie realizácie hlavných aktivít projektu požaduje verejný obstarávateľ v lehote najneskôr **do 7 mesiacov od nadobudnutia účinnosti zmluvného vzťahu, najneskôr však do 31.12.2023, podľa toho, ktorá lehota nastane skôr.**

Príloha č. 2

Zoznam subdodávateľov

podľa ustanovenia § 41 ods. 3 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Por. č.	Subdodávateľ *obchodné meno/názov, sídlo/miesto podnikania, IČO*	Osoba oprávnená konať za subdodávateľa *meno a priezvisko, adresa pobytu, dátum narodenia*
1.	**Sicurio s.r.o.** Gagarinova 10A, 821 05 Bratislava IČO: 54911559	Ing. Marek Majka, konateľ Zemianske Sady 27, 92554 Zemianske Sady 30.05.1995
2.	**iseco s. r. o.** Bodíky 705, 930 31 Bodíky IČO: 45485615	Ľubomír Kopáček, konateľ Bodíky 205, 930 31 Bodíky 15.07.1977

Ak úspešný uchádzač nemá v úmysle zadať časť plnenia subdodávateľom, pod tabuľku uvedie nasledovné: „**Predmet zákazky nebudem plniť prostredníctvom subdodávateľov a celé plnenie vykonám vlastnými kapacitami**".

V Bratislave dňa 23.10.2023

iServices
iServices s.r.o., Zadunajská cesta 8, 851 01 Bratislava
tel.: +421 2 6224 4226, email: iservices@iservices.sk
IČO: 43872930, IČ DPH: SK2022500524

.....

Ing. Pavol Šimák
konateľ
iServices s. r. o.

Príloha č. 3

Harmonogram

Harmonogram realizácie Projektu

Zhotoviteľ je povinný dodržiavať harmonogram aktivít, ktorý si Zmluvné strany dohodnú na úvodnom stretnutí, a ktorý bude vychádzať z harmonogramu realizácie Projektu existujúceho v súvislosti so Zmluvou o poskytnutí NFP (viď nižšie). V každom prípade však platí, že konečný termín odovzdania a prevzatia celého Diela, vrátane všetkých jeho častí, resp. poslednej z jeho častí, je najneskôr **do 31.12.2023**.

	Aktivita	Začiatok aktivity Mesiac/rok	Koniec aktivity Mesiac/rok
Hlavné aktivity	Analýza a dizajn	6/2023	12/2023
	Nákup technických prostriedkov, programových prostriedkov a služieb	6/2023	09/2023
	Implementácia a testovanie	10/2023	12/2023
	Nasadenie	10/2023	12/2023

Príloha č. 4

Návrh na plnenie kritérií

Cena celkom v EUR bez DPH	DPH 20% v EUR	Cena celkom v EUR s DPH
144 966,42 €	28 993,28 €	173 959,70 €

Realizácia primárnych aktivít:

Popis	Počet (ks, MD)	Cena v EUR bez DPH	DPH v EUR	Cena v EUR s DPH
1. **Posúdenie súladu s bezpečnostnými požiadavkami, zákonom č. 69/2018 Z.z. (vyhlášky NBÚ č. 362/2018 Z. z.) ako aj 95/2019 (vyhlášky č. 179/2020 Z.z.) a návrh strategického akčného plánu úloh na zabezpečenie súladu.** 2. **Inventarizácia, klasifikácia a kategorizácia aktív** 3. **Vykonanie analýzy rizík a analýzy dopadov s návrhom katalógu rizík a spôsobov ich riadenia** 4. **Vypracovanie interných smerníc a prevádzkovej dokumentácie riadenia IB a KyB v rozsahu:** ▪ Stratégia informačnej a kybernetickej bezpečnosti ▪ Bezpečnostná politika ▪ Smernica pre riadenie informačnej bezpečnosti ▪ Klasifikácia informácií a kategorizácia sietí a informačných systémov	20	11 600,00 €	2 320,00 €	13 920,00 €

▪ Smernica výkonu analýzy rizík a analýzy dopadov (AR/BIA) ▪ Smernica o bezpečnej prevádzke IS a sietí ▪ Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov ▪ Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP ▪ Plán zálohovania				
5. Vykonanie technických testov/skenov: ▪ aktív a zraniteľností aktív na zistenie známych zraniteľností v internej sieťovej infraštruktúre organizácie, vyhodnotených reportom ▪ sieťovej komunikácie na zistenie podozrivých aktivít v infraštruktúre spoločnosti, vyhodnotených reportom	4	2320,00 €	464,00 €	2 784,00 €
6. SW nástroj pre procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti na obdobie 24 mesiacov • evidenciu informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov • riadenie tretích strán • personálnej bezpečnosti • analýzy rizík • automatický výkon auditu súladu. • e-learning	6	3 480,00 €	696,00 €	4 176,00 €
7. Platforma pre bezpečnostné testovania zamestnancov na obdobie 12 mesiacov • Realizácia 2 samostatných phishingových kampaní	4	2320,00 €	464,00 €	2 784,00 €

8. Implementačné a konfiguračné práce pre zavedenie: • SW nástroja pre procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti • Platformy pre bezpečnostné testovania zamestnancov	6	3 480,00 €	696,00 €	4 176,00 €
CENA CELKOM ZA PRIMÁRNE AKTIVITY		**23 200,00 €**	**4 640,00 €**	**27 840,00 €**

Realizácia sekundárnych aktivít:

Popis	Počet (ks, MD)	Cena v EUR bez DPH	DPH v EUR	Cena v EUR s DPH
Licencie a Hardvér na obdobie 24 mesiacov	1	99 146,42 €	19 829,28 €	118 975,70 €
Konzultačné a implementačné práce	15	8 700,00 €	1 740,00 €	10 440,00 €
CENA CELKOM ZA SEKUNDÁRNE AKTIVITY		**107 846,42 €**	**21 569,28 €**	**129 415,70 €**

Rámcové konzultačné práce

Popis	Počet (ks, MD)	Cena v EUR bez DPH	DPH v EUR	Cena v EUR s DPH
Rámcové konzultačné práce na obdobie 1 roka	24 MD	13 920,00 €	2 784,00 €	16 704,00 €

CENA CELKOM ZA RÁMCOVÉ KONZULTAČNÉ PRÁCE	**13 920,00 €**	**2 784,00 €**	**16 704,00 €**

*MD: Man-Day (Človekodeň) je pracovný čas jednej osoby zodpovedajúce jednému pracovnému dňu, teda typicky 8 hodín.

V prípade, ak hospodársky subjekt nie je platca DPH, uvedie celkovú cenu s poznámkou, že nie je platca DPH.

Príloha č. 5

Zoznam odborníkov a požiadaviek na odborníkov

Odborník	Požiadavky na odborníka	Meno a priezvisko odborníka/ odborníkov
IT Analytik	a) minimálne 3 roky preukázateľnej odbornej praxe v oblasti analýzy a dizajnu informačných systémov a návrhu architektúry riešenia bezpečnostných informačných technológií; b) minimálne 2 preukázateľné praktické skúsenosti s vypracovaním analýz a dizajnu pre realizáciu IT bezpečnostných riešení; c) držiteľ platného certifikátu minimálne na úrovni CISSP alebo ekvivalent;	Ľubomír Kopáček
IT konzultant	a) minimálne 2 roky preukázateľnej odbornej praxe v oblasti predmetu zákazky a požiadaviek na činnosti uvedené v tejto pozícii, kľúčový expert preukáže v štruktúrovanom profesijnom životopise.	Ľudovít Maruniak
Odborník pre IT dohľad/ Quality Assurance	a) preukázateľná profesionálna praktická skúsenosť, a to preukázaním účasti na minimálne jednom projekte v pozícii odborník pre IT dohľad, kľúčový expert preukáže v štruktúrovanom profesijnom životopise.	Ing. Marek Majka
Špecialista pre IT bezpečnosť	a) minimálne 2 roky preukázateľnej odbornej praxe v oblasti kybernetickej a informačnej bezpečnosti; b) minimálne 1 preukázateľná praktická skúsenosť v oblasti kybernetickej a informačnej bezpečnosti, kľúčový expert preukáže v štruktúrovanom profesijnom životopise; c) držiteľ platného certifikátu CISSP alebo CISA alebo ekvivalent;	Ing. Peter Rejta

Zhotoviteľ nemôže využiť jednu osobu na účely splnenia požiadaviek súčasne na viacero druhov odborníkov vo vyššie uvedenej tabuľke.