Príloha č. 1 k Zmluve o dielo

Podrobná špecifikácia predmetu zmluvy
(opis predmetu zákazky)

Názov zákazky: „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS – Národné lesnícke centrum

Zoznam skratiek

IB	informačná bezpečnosť
KB	kybernetická bezpečnosť
ITVS	informačné technológie verejnej správy
AR	analýza rizík
VS	verejná správa
BIA	Business Impact Analysis
CSIRT	Computer Security Incident Response Team Slovakia – vládna jednotka pre riešenie kybernetických bezpečnostných incidentov
SK-CERT	Národné centrum kybernetickej bezpečnosti
BCM	Business Continuity Management - riadenie kontinuity činností
BCP	Business Continuity Plan - plán Kontinuity činností
DRP	Disaster Recovery Plan - plán obnovy
VISKB	vládny informačný systém kybernetickej bezpečnosti
OVM	orgán verejnej moci
SW	softvér

Verejný obstarávateľ v oblasti informačnej a kybernetickej bezpečnosti informačných technológií verejnej správy (ďalej len „IB a KB ITVS“) z dôvodu potreby plnenia požiadaviek stanovených najmä 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 č. 95/2019 Z. z.“) a zákonom č. 69/2018 Z. z o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“)., 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 podsektore VS – Národné lesnícke centrum.

Predmetom zákazky je poskytovanie služieb súvisiacich so zavedením procesu riadenia IB a KB ITVS v súlade s projektom Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS – Národné lesnícke centrum na základe schválenej žiadosti o poskytnutie nenávratného finančného príspevku č. NFP311070BUD8 a v súlade s výzvou OPII-2021/7/16-DOP - Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS a v súlade so zákonom č. 95/2019 Z. z. a so zákonom č. 69/2018 Z. z.

Verejný obstarávateľ zamestnáva približne 250 zamestnancov, spravuje a prevádzkuje približne 400 osobných počítačov, 125 mobilných telefónov, 205 pevných stolových telefónov, digitálnu telekomunikačnú ústredňu, 15 informačných systémov, 50 krabicových počítačových programov, 10

pevných a 20 virtuálnych serverov, 6 lokálnych sietí z toho 2 hlavné nadradené a 4 expozitúry. Všetky tieto siete sú prepojené šifrovaným spojením a tvoria ako celok rozľahlú komunikačnú sieť, ktorá sa skladá z kabeláže a 84 aktívnych prvkov.

A. Predmetom zákazky bude poskytovanie služieb minimálne v rozsahu:

1. analýza aktuálneho stavu v oblasti riadenia IB a KB ITVS a jeho súladu s požiadavkami príslušných právnych predpisov;
2. vypracovanie analýzy rizík (ďalej len „AR“) a analýzy dopadov (Business Impact Analysis – ďalej len „BIA“) vrátane:
    a. identifikácie aktív a ohodnotenia ich kritickosti,
    b. klasifikácie aktív a kategorizácie informačných systémov a sietí,
    c. identifikácie hrozieb a vektorov útokov,
    d. analýzy potenciálnych dopadov,
    e. identifikácie rizík, na základe pravdepodobností výskytu hrozieb a možných dopadov,
    f. identifikácie existujúcich opatrení a reziduálnych rizík,
    g. návrhu opatrení,
3. vypracovanie stratégie informačnej a kybernetickej bezpečnosti vrátane plánu/ harmonogramu na implementáciu navrhnutých opatrení;
4. zabezpečiť formálne rozhodnutie o riadení rizík (o ich akceptácii alebo prijatí adekvátnych opatrení na ich zníženie alebo úplnú elimináciu),
5. vytvorenie požadovaných interných bezpečnostných dokumentov a smerníc pre relevantné oblasti riadenia IB a KB ITVS,
6. Implementácia, testovanie a uvedenie do produkčnej prevádzky SW nástroja, pre procesno-organizačné riadenie IB a KB ITVS.

Výsledkom bude nový efektívny spôsob procesného ako aj organizačného riadenia a udržiavania základných bezpečnostných dokumentov ako i rámca riadenia informačnej a kybernetickej bezpečnosti, klasifikácie informačných aktív a informácií a kategorizácie informačných systémov a sietí, realizácie AR/BIA a zavedenie formalizovaného a opakovaného procesu riadenia rizík, vrátane podpory IKT nástrojom.

Dodávateľ je pri vypracovaní bezpečnostných dokumentov, na základe tohto opisu predmetu zákazky povinný používať jednotné termíny na pomenovávanie rovnakých javov a tvoriť formulácie tak, aby bola jednoznačná a nezameniteľná výpovedná hodnota pomenovaných javov. Na tento účel bude podľa potreby vytvorená v dokumentoch časť/článok „Vymedzenie základných pojmov, zoznam skratiek“.

<u>1. Analýza aktuálneho stavu v oblasti riadenia IB a KB a jeho súladu s požiadavkami príslušných právnych predpisov</u>

Požadujeme analýzu aktuálneho stavu prijatých a zabezpečovaných bezpečnostných opatrení v oblasti IB a KB ITVS z pohľadu procesného a organizačného zabezpečenia verejného obstarávateľa voči povinnostiam vyplývajúcim z platných právnych predpisov, najmä zákona č. 95/2019 Z. z. a vyhlášky 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 (ďalej len „vyhláška č. 179/2020 Z. z.“). Analýzu aktuálneho stavu podľa zákona č. 69/2018 Z. z. a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) má verejný obstarávateľ vypracovanú vo forme Správy z auditu, ktorá bude dodávateľovi sprístupnená po podpise zmluvného vzťahu.
Výstupom bude analýza realizovaná minimálne v rozsahu:

- sumarizáciu všetkých povinnosti uložených príslušným právnym predpisom vo vzťahu k IB a KB ITVS, ktoré je verejný obstarávateľ povinný dodržiavať a ich úroveň plnenia zo strany verejného obstarávateľa,
- návrh opatrení na odstránenie príčin vzniku neplnenia týchto povinností,
- časový harmonogram prijímania všetkých bezpečnostných opatrení verejného obstarávateľa vyplývajúcich z príslušných právnych predpisov z oblasti IB a KB ITVS vzhľadom na prioritu a potenciálnu príčinu vzniku kybernetického bezpečnostného incidentu.

2. Vypracovanie analýzy rizík (ďalej len „AR“) a analýzy dopadov (Business Impact Analysis – ďalej len „BIA“) vrátane identifikácie aktív a ohodnotenia ich kritickosti, klasifikácie aktív a kategorizácie informačných systémov 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 a návrhu opatrení

Požadujeme vypracovanie AR a BIA v nasledovnom rozsahu:
- identifikácia všetkých informačných aktív, informácií, informačných systémov a sietí, od ktorých závisí prevádzkovanie základnej služby, vrátane podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie,
- určenie vlastníkov, správcov a používateľov informačných aktív, informácií, informačných systémov a sietí,
- kategorizácia informačných aktív,
- klasifikácia informácií, kategorizácia informačných systémov a sietí na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť,
- ohodnotenie kritickosti informačných aktív, informácií, informačných systémov a sietí,
- identifikácia hrozieb, zraniteľností a vektorov útokov,
- identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,
- určenia vlastníka rizika,
- analýzy potenciálnych funkčných dopadov,
- hodnotenie a kategorizácia rizík vyplývajúcich z hrozieb, zraniteľností a možných dopadov,
- identifikácia existujúcich opatrení verejného obstarávateľa,
- identifikácia reziduálnych rizík,
- vzorce/modely/matice/definície/metódy/postupy na určovanie klasifikácie a kategorizácie informačných aktív, informácií, informačných systémov a sietí, hrozieb a rizík,
- návrh opatrení na odstránenie rizík a časový harmonogram ich implementácie vzhľadom na kategóriu rizík.

Výstupom tejto AR A BIA bude:
- zoznam informačných aktív, informácií, informačných systémov a sietí verejného obstarávateľa a k nim priradené identifikované a určené údaje podľa požiadaviek na rozsah AR a BIA (vlastníci informačných aktív, klasifikácia informačných aktív, kategorizácia informačných systémov a sietí, hodnota kritickosti informačných aktív, informačných systémov a sietí, identifikovaná hrozba a zraniteľnosť, vektorový útok, hodnoty a kategórie rizík a všetky ostatné relevantné údaje),
- katalóg rizík,
- zoznam a formalizovaná úprava použitých vzorcov/modelov/matíc/definícií/metód/postupov na určovanie klasifikácie a kategorizácie informačných aktív, informácií, informačných systémov a sietí, hrozieb a rizík,
- návrh plánu preskúmavania a aktualizácie informačných aktív, informácií, informačných systémov a sietí a k nim príslušných identifikovaných a určených údajov,
- zoznam opatrení na odstránenie rizík a časový harmonogram ich implementácie vzhľadom na kategóriu rizík.

Uvedené je predpokladom na zavedenie efektívneho spôsobu na kvalifikované vykonávanie analýzy rizík a dopadov na strategickej aj operatívnej úrovni prostredníctvom interných personálnych kapacít verejného obstarávateľa.

3. Na základe AR a BIA vypracovanie stratégie IB a KB ITVS vrátane plánu/harmonogramu na implementáciu navrhnutých opatrení

Na základe vykonaných analýz, identifikovaných a kategorizovaných rizík a taktiež na základe existujúcich opatrení a navrhnutých opatrení požadujem vypracovať stratégiu IB a KB ITVS.
Výstupy - Stratégie IB a KB ITVS budú obsahovať minimálne:
- stanovenie bezpečnostných cieľov z hľadiska informačnej a kybernetickej bezpečnosti, ktoré je potrebné na základe výsledkov analýzy rizík, spolu s uvedením základných princípov na ich dosiahnutie a určenie právomocí a zodpovedností za riadenie IB a KB ITVS, riadenie rizík IB a KB ITVS,
- stanovenie spôsobu vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov,
- určenie všeobecných a špecifických zodpovedností a povinností v oblasti IB a KB ITVS a určenie príslušných bezpečnostných rolí potrebných na riadenie IB a KB ITVS vrátane určenia rozsahov činností, kompetencií a úloh; rozdelenie rolí na riadiacu zložku, výkonnú zložku a kontrolnú zložku, pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami,
- rozsah základného rámca na riadenie aktív podľa § 6 vyhlášky č. 362/2018 Z. z., od ktorých závisí činnosť sietí a informačných systémov,
- rozsah základného rámca riadenia rizík podľa § 6 vyhlášky č. 362/2018 Z. z. v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov a určenie bezpečnostných opatrení podľa oblastí v zmysle § 20 ods. 3 zákona č. 69/2018 Z. z. v závislosti od identifikovaných rizík,
- rozsah a periodicitu overovania stavu informačnej a kybernetickej bezpečnosti prostredníctvom auditu informačnej a kybernetickej bezpečnosti vrátane zhodnotenia súladu bezpečnostnej stratégie a bezpečnostných politík s požiadavkami najmä zákona č. 69/2018 Z. z., č. 95/2019 Z. z. alebo iného všeobecne záväzného právneho predpisu,
- postup a zodpovednosti pri revízii bezpečnostnej dokumentácie schvaľovanej prevádzkovateľom základnej služby vrátane periodicity pravidelných revízií a jej aktualizácií po každej zmene majúcej na ňu vplyv, ako aj z dôvodov mimoriadnych revízií.

4. Zabezpečenie formálneho rozhodnutia o riadení rizík (o ich akceptácii alebo prijatí adekvátnych opatrení na ich zníženie alebo úplnú elimináciu).

Na základe identifikovaných rizík vypracovať verejnému obstarávateľovi metodiku a spôsob vypracovania adekvátnych opatrení na zníženie rizika na prijateľnú úroveň alebo úplnú elimináciu rizika a mechanizmus akceptácie prijatých opatrení a následnú kontrolu dodržiavania prijatých opatrení v príslušnom časovom intervale.

5. Vytvorenie požadovaných interných bezpečnostných dokumentov a smerníc pre relevantné oblasti riadenia IB a KB

Na základe vykonaných analýz, identifikovaných rizík a taktiež na základe existujúcich opatrení a navrhnutých opatrení požadujem vypracovať interné bezpečnostné dokumenty – výstupy v súlade s vypracovanou stratégiou IB a KB ITVS v rozsahu:
a) **Bezpečnostná politika**, ktorá bude obsahovať:
   - organizáciu informačnej bezpečnosti - riadenie bezpečnostnej architektúry, systém riadenia kybernetickej bezpečnosti, riadenie identít a prístupových práv, riadenie privilegovaných prístupov, bezpečnostný monitoring a správa, bezpečnostných záznamov,

- politiku IB a KB ITVS - určenie povinnosti, zodpovednosti a právomoci manažéra kybernetickej bezpečnosti a manažéra informačnej bezpečnosti a všetkých zamestnancov v oblasti riadenia, správy a prevádzky IB a KB ITVS, základné zásady a opatrenia kybernetickej a informačnej bezpečnosti v štruktúre oblastí definovaných minimálne vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z.,
- riadenie bezpečnostných rizík - testovanie a bezpečnostná certifikácia informačných systémov, metodika posudzovania vplyvu na ochranu údajov a osobných údajov, metodika posudzovania rizík, fyzická bezpečnosť a bezpečnosť prostredia, riadenie a riešenie bezpečnostných incidentov, vrátane určenia postavenia štatutárneho orgánu verejného obstarávateľa a jeho podpory pri riadení rizík, pri ich akceptácii alebo prijímaní adekvátnych opatrení na ich zníženie na prijateľnú úroveň alebo úplnú elimináciu,
- riadenie informačných aktív - klasifikácia informácií a kategorizácia informačných systémov a sietí, návrh aktualizácie platného registratúrneho poriadku a registratúrneho plánu,
- pravidlá správania a dobrej praxe - práca na diaľku a používanie mobilných zariadení, riadenie personálnej bezpečnosti, pravidlá komunikácie,
- riadenie dodávateľských vzťahov - riadenie dodávateľských služieb, akvizícia informačných systémov,
- riadenie vývoja a údržby v oblasti informačno-komunikačných technológií - vývoj a testovanie informačných systémov, postupy údržby informačných systémov, riadenie technických zraniteľností a manažment záplat,
- riadenie a prevádzka informačno-komunikačných technológií - pravidlá prepájania informačných systémov a prenosu, elektronických informácií, riadenie bezpečnosti sietí, riadenie zmien infraštruktúry, riadenie kapacity informačných systémov a služieb, riadenie kryptografických opatrení,
- riadenie prístupov,
- riadenie súladu - audit kybernetickej bezpečnosti, spracúvanie údajov, osobných údajov a klasifikovaných informácií, poskytovanie súčinnosti tretím stranám,
- riadenie kontinuity procesov a činností - plány kontinuity prevádzkových činností, plány obnovy prevádzky, metodika zálohovania a obnovy údajov, testovacie plány/scenáre;

b) **Smernica pre riadenie informačnej bezpečnosti,** ktorá bude obsahovať určenie povinnosti, zodpovednosti a právomoci manažéra kybernetickej bezpečnosti a informačnej bezpečnosti a všetkých zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti a základné zásady a opatrenia kybernetickej a informačnej bezpečnosti ITVS;

c) **Smernica o klasifikácií informácií, kategorizácií aktív, sietí a informačných systémov**, ktorá sa vykonáva v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov minimálne podľa prílohy č. 2 vyhlášky č. 362/2018 Z. z.;

d) **Smernica na vykonávanie analýzy rizík a analýzy dopadov**, ktorá obsahuje postupy na určenie pravdepodobnosti vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva a pozostáva z hodnotenia dopadu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby a spôsobiť ohrozenie alebo narušenie kontinuity jeho poskytovanej základnej služby;

e) **Smernica o bezpečnej prevádzke informačných systémov a sietí**, ktorá bude obsahovať pravidlá a postupy na riadenie zmien, riadenie záplat a aktualizácií, riadenie kapacít, pravidelné zálohovanie a testovanie obnovy informácií/informačných systémov alebo ich komponentov zo záloh, ochranu pred škodlivým kódom/počítačovým programom, inštaláciu počítačových programov v sieťach a informačných systémoch, inštaláciu zariadení v sieťach a informačných systémoch a zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov;

f) **Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov,** ktorá bude minimálne obsahovať:
   - základné pravidlá ako identifikovať kybernetický bezpečnostný incident,

- postup pri hlásení kybernetických bezpečnostných incidentov,
- postup evidencie kybernetických bezpečnostných incidentov,
- postupy a princípy riešenia kybernetických bezpečnostných incidentov,
- zoznam preventívnych a nápravných opatrení,
- zoznam informačných systémov verejného obstarávateľa vrátane aktuálnych kontaktných údajov zamestnancov určených na správu jednotlivých informačných systémov,
- zoznam zástupcov tretích strán zodpovedných za správu alebo podporu ITVS potrebných pri riešení kybernetických bezpečnostných incidentov vrátane aktuálnych kontaktných údajov,
- kontaktné údaje na príslušnú jednotku pre riešenie kybernetických bezpečnostných incidentov (CSIRT) a Národné centrum kybernetickej bezpečnosti SK-CERT (SK-CERT),
- povinnosti a zodpovednosti verejného obstarávateľa voči CSIRT a SK-CERT,
- preukázateľné oboznámenie s povinnosťou ohlasovania kybernetických bezpečnostných incidentov všetkých používateľov ITVS vrátane správcov jednotlivých komponentov, ako aj zamestnancov tretích strán, ktorí vykonávajú správu alebo podporu ITVS;

g) **Politika BCM riadenia kontinuity procesov, vrátane stratégie obnovy a návrh predvyplnenej šablóny pre BCP a DRP** - bude obsahovať krízové plány na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu na základnú službu, plány havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu, postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej:
   - frekvenciu a rozsah jej dokumentovania a schvaľovania,
   - určenie osoby zodpovednej za zálohovanie,
   - časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní,
   - požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom,
   - požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
   - požiadavku na vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov;
h) **Smernica pre bezpečný vývoj a údržbu aplikácií a informačných systémov,** ktorá bude obsahovať povinnosti zamestnancov a tretích strán pri prevádzke, údržbe, rozvoji informačných systémov ako aj bezpečnostné opatrenia pri ich prevádzke, údržbe a rozvoji.

6. Implementácia, testovanie a uvedenie do produkčnej prevádzky SW nástroja, pre procesno-organizačné riadenie IB a KB ITVS

V rámci implementácie SW nástroja pre procesno-organizačné riadenie IK a KB ITVS požadujeme integráciu na vládny informačný systém kybernetickej bezpečnosti (ďalej len „VISKB“) a implementáciu príslušných klientskych modulov pre OVM – online aj offline do aplikačno-technologického prostredia verejného obstarávateľa a jeho testovanie v technologickom prostredí verejného obstarávateľa. Pod pojmom implementácia sa rozumie uvedenie VISKB - klientskych modulov pre OVM – online aj offline do produkčnej prevádzky v aplikačno-technologickom prostredí verejného obstarávateľa, jeho customizácia, čiže parametrizácia, konfigurácia a integrácia s príslušnými IS verejného obstarávateľa, v prípade potreby aj inštalácia modulov alebo častí VISKB - klientskych modulov pre OVM – online aj offline do aplikačno-technologického prostredia verejného obstarávateľa a nastavenie jeho funkcionalít tak aby spĺňal všetky požiadavky a skutočné potreby, ktoré vyplynú verejnému obstarávateľovi z vykonaných analýz na základe tejto zákazky a poskytoval požadované výstupy pre podporu riadenia IB a KB ITVS.

VISKB bude vyhotovený pre Ministerstvo investícií, regionálneho rozvoja a informatizácie SR na základe „Rámcovej dohody č. 622/2022 o implementácii informačného systému“ dostupnej na webovej adrese https://www.crz.gov.sk/zmluva/6613632/, kde v prílohe č. 1 predmetnej zmluvy je jeho technická špecifikácia.
Súčasťou predmetu zákazky podľa tohto bodu je:

- vypracovanie a dodanie používateľských príručiek pre administrátora a používateľa - aplikačné príručky, používateľské príručky, inštalačné príručky a pokyny na inštaláciu/reinštaláciu, konfiguračné príručky a pokyny pre diagnostiku, integračné príručky, a prevádzkový opis a pokyny pre servis a údržbu, realizačná dokumentácia v zmysle požiadaviek definovaných v návrhových dokumentoch;

Požiadavky na zabezpečenie školení
Zhotoviteľ je povinný navrhnúť rozsah a štruktúru školení vrátane harmonogramu a v súlade so schválenou Žiadosťou o poskytnutie nenávratného finančného príspevku č. NFP311070BUD8. Rozsah jednotlivých školení musí zodpovedať pokrytiu potrieb všetkých používateľov systému, ktorý je súčasťou Diela/ dodávky. V rámci dodávky je potrebné pokryť minimálne nasledujúci rozsah:

- Všeobecné funkcionality z pohľadu používateľov
- Prevádzka, obsluha a dohľad z pohľadu prevádzkovateľa

Zaškolenie pracovníkov Objednávateľa je požadované v slovenskom jazyku, miesto konania preferenčne v priestoroch Zhotoviteľa a to v rozsahu:

- obsah školenia
- trvanie školenia
- miesto
- maximálny počet účastníkov na školení, požadované predpoklady pre účasť na školení

Školenia sa vykonávajú v školiacom prostredí, ktoré pripraví Zhotoviteľ. Školiace prostredie obsahuje školiace dáta. Zmeny, ktoré účastník školenia vykoná v školiacom systéme, môže administrátor odvolať a obnoviť prednastavené školiace prostredie. Alternatívne je možné využiť na školenie testovacie prostredie.
Súčasťou dodávky školení je dodávka školiacich materiálov a výstupov.

Testovanie bude pozostávať z funkčného testovania, systémového a integračného testovania, záťažového a výkonnostného testovania, bezpečnostného a používateľského testovania. Výstupom z testovania bude zoznam chýb a ich návrh na odstránenie.
Testovanie pozostáva z testovania samostatného VISKB - klientskych modulov pre OVM – online aj offline tak, aby bolo preukázané jeho bezporuchové a bezpečné prevádzkovanie v aplikačno-technologickom prostredí verejného obstarávateľa.

Za nasadenie sa považuje implementácia a uvedenie do produkčnej prevádzky po celkovom testovaní s výsledkom testov bez chýb VISKB - klientskych modulov pre OVM – online aj offline.

B. Financovanie

Predmet zákazky bude financovaný zo zdrojov poskytnutých verejnému obstarávateľovi na základe zmluvy o nenávratný finančný príspevok z projektu:
Kód Projektu a ISVS z MetaIS: projekt_1925

Názov projektu:	**Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS – Národné lesnícke centrum**
Kód projektu:	311070BUD8
Kód ŽoNFP:	NFP311070BUD8
Operačný program:	311000 - Operačný program Integrovaná infraštruktúra
Spolufinancovaný z:	Európsky fond regionálneho rozvoja

Prioritná os: 311070 - Informačná spoločnosť
(ďalej spoločne označené ako „projekt“)

Dodávateľ je povinný nim vyhotovovanú dokumentáciu súvisiacu s predmetom plnenia zákazky (napr. faktúry, dodacie listy, preberacie protokoly a pod.), ktorú špecifikuje verejný Obstarávateľ v závislosti od programov EÚ, podľa pokynov verejného Obstarávateľa, viditeľne označovať odkazom na Európsku úniu a znak Európskej únie v súlade s grafickými normami podľa prezentácie na adrese: http://europa.eu/about-eu/basic-information/symbols/flag/index_sk.htm, odkazom na príslušný fond Európskej únie, logami verejného Obstarávateľa a logami jednotlivých programov EÚ a príslušným textom podľa znenia poskytnutého verejným Obstarávateľom. Takéto označenie sa uplatní na každý špecifikovaný vyhotovený dokument od začiatku plnenia zmluvného vzťahu.

Dodávateľ poskytne potrebnú súčinnosť verejnému Obstarávateľovi a oprávneným kontrolným zamestnancom pri vykonávaní kontroly obchodných dokumentov a vecnú a finančnú kontrolu v súvislosti s realizáciou a plnením predmetu tejto zákazky, ako aj v súvislosti s aktivitami financovanými zo zdrojov príslušného programu EÚ, a to aj po ukončení zmluvného vzťahu v trvaní 5 rokov.

Dodávateľ stanoví výšku nákladov za predmet zákazky v nasledovnom členení a pri fakturácii bude povinný rozčleniť fakturovanú sumu Objednávateľovi v prílohe faktúry:

Skupina výdavkov	Názov výdavku	MJ	Počet jednotiek	Komentár
013 Softvér	IT analytik	človekodeň	16,00	Vypracovanie analýzy rizík. Rola realizuje definované projektové výstupy okrem vývoja.
013 Softvér	IT/IS konzultant (napr. SAP)	človekodeň	14,00	Vypracovanie analýzy rizík. Rola realizuje definované projektové výstupy okrem vývoja.
013 Softvér	Špecialista pre bezpečnosť IT	človekodeň	7,00	Vypracovanie analýzy rizík. Rola realizuje definované projektové výstupy okrem vývoja.
013 Softvér	IT programátor/vývojár	človekodeň	34,00	Rola realizuje customizáciu SW nástroja pre procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti.
013 Softvér	IT/IS konzultant (napr. SAP)	človekodeň	6,00	Rola realizuje customizáciu SW nástroja pre procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti.
013 Softvér	IT tester	človekodeň	12,00	Rola realizuje testovanie customizovaného SW nástroja pre procesno-organizačné riadenie Informačnej a kybernetickej bezpečnosti.
013 Softvér	Školiteľ pre IT systémy	človekodeň	4,00	Rola realizuje školenia pre technických pracovníkov/administrátorov a školenia pre pracovníkov odboru kybernetickej bezpečnosti
013 Softvér	Špecialista pre infraštruktúrny/HW špecialista	človekodeň	17,00	Rola realizuje nasadenie customizovaného offline klienta.

C. Termín realizácie predmetu zákazky/zmluvy

Poskytovanie služieb podľa tohto predmetu zákazky požadujeme v lehote najneskôr **do 8 mesiacov od nadobudnutia účinnosti zmluvného vzťahu** v zmysle záväzného harmonogramu a to v nasledovných termínoch:

1. Názov aktivity: Analýza a dizajn od nadobudnutia účinnosti zmluvy s dodávateľom do 05/2023,
2. Názov aktivity: Implementácia a testovanie od 04/2023 do 06/2023,
3. Názov aktivity: Nasadenie od 04/2023 do 08/2023.

Hranice medzi jednotlivými aktivitami predstavujú body, kedy dodávateľ odovzdá čiastkové výstupy predmetu zákazky dohodnutým spôsobom Verejnému obstarávateľovi a zároveň odberateľ vyhlási ukončenie jednej aktivity a začiatok nasledovnej aktivity v zmysle harmonogramu.

Fakturácia za predmet zákazky prebehne po odovzdaní celého predmetu zákazky spôsobom stanoveným v zmluvnom vzťahu verejnému obstarávateľovi v zmysle časti B. bodu 3.

Harmonogram aktivít

Hlavné aktivity projektu		
Typ aktivity	43231107009 – Q. Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti	
Hlavné aktivity projektu	**Začiatok realizácie**	**Koniec realizácie**
432BUD800001 – Analýza a dizajn	od nadobudnutia účinnosti zmluvy	5.2023
432BUD800002 – Implementácia a testovanie	4.2023	6.2023
432BUD800003 - Nasadenie	4.2023	8.2023