Opis predmetu zákazky

(Vzdelávacie materiály pre školenie zamestnancov verejnej správy – e-learning)

Obsah

1. Úvod a účel

Účelom tohto verejného obstarávania, realizovaného v rámci implementácie Reformy č. 5 Skvalitnenie vzdelávania a zabezpečenie odbornej spôsobilosti v oblasti KIB (Plán obnovy a odolnosti, Komponent 17: Digitálne Slovensko, je zabezpečiť zvýšenie úrovne znalostných štandardov v oblasti kybernetickej bezpečnosti špecifikovaných skupín zamestnancov verejnej správy na požadovanú úroveň vzdelania v oblasti kybernetickej bezpečnosti definovanú v kapitole 3 tohto dokumentu. Tento cieľ požadujeme dosiahnuť a naplniť prostredníctvom vytvorenia a zároveň dodania príslušných vzdelávacích materiálov v elektronickej (digitálnej) forme, bližšie špecifikovaných v kapitole 2.2 tohto dokumentu.

Tento dokument slúži pre záujemcu /dodávateľa na identifikáciu požiadaviek, týkajúcich sa obsahových náležitostí predmetných vzdelávacích materiálov, ktoré sú určené na zvýšenie znalostných štandardov u vybraných špecifických skupín zamestnancov verejnej správy špecifikovaných v kapitole 2.1 (Cieľová skupina zamestnancov verejnej správy) tohto dokumentu.

Tento dokument slúži zároveň ako odborný podklad pre realizáciu verejného obstarávania, ktorého cieľom je vysúťažiť dodávateľa, ktorý vytvorí na základe požiadaviek verejného obstarávateľa vzdelávacie materiály, pre definovaný okruh zamestnancov verejnej správy.

1.1 Východiskový stav

Aktuálne verejná správa nedisponuje dostupnými vzdelávacími materiálmi, ktoré by boli komplexne zamerané na praktické zavedenie, implementáciu a zvýšenie znalostných štandardov v oblasti kybernetickej bezpečnosti u definovanej cieľovej skupiny zamestnancov verejnej správy na požadovanú úroveň.

1.2 Cieľ zákazky

Hlavným cieľom reformy Skvalitnenie vzdelávania a zabezpečenie spôsobilosti v oblasti KIB v aktivite SK2 je v zmysle projektového zámeru zvýšiť znalostné štandardy v oblasti kybernetickej a informačnej bezpečnosti u definovanej cieľovej skupiny zamestnancov verejnej správy na požadovanú úroveň, a to prostredníctvom vytvorenia a dodania príslušných vzdelávacích materiálov. Následná realizácia školení prostredníctvom dodaných vzdelávacích materiálov u zamestnancov verejnej správy prakticky zavedie a implementuje zvýšenie základného povedomia v oblasti kybernetickej a informačnej bezpečnosti.

1.3 Definície a skratky

- EÚ - Európska únia
- IKT - informačno-komunikačné technológie
- KB - kybernetická bezpečnosť
- KBI – kybernetický bezpečnostný incident
- KIB - kybernetická a informačná bezpečnosť
- MIRRI SR - Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
- OVM - orgán verejnej moci
- SR - Slovenská republika

2. Celkový opis predmetu zákazky

Verejný obstarávateľ má záujem v oblasti kybernetickej bezpečnosti zvýšiť úroveň znalostných štandardov u definovanej skupiny zamestnancov verejnej správy špecifikovaných v kapitole 2.1 (Cieľová skupina zamestnancov verejnej správy) tohto dokumentu na požadovanú úroveň vedomostí v oblasti kybernetickej bezpečnosti a to prostredníctvom nasledovných aktivít:

- vytvorenie vzdelávacích materiálov zo strany úspešného uchádzača pre cieľové skupiny zamestnancov verejnej správy (formou e-learningu),
- dodanie vytvorených vzdelávacích materiálov/obsahov verejnému obstarávateľovi elektronickou formou v niektorom zo štandardizovaných formátov pre výukový obsah (napr. video obsah, SCORM alebo ekvivalent špecifikovaný v kapitole VI), a zároveň dodanie vytvorených vzdelávacích materiálov/obsahov, najmä scenárov k jednotlivým kapitolám vzdelávacích modulov verejnému obstarávateľovi vo formátoch ako .PDF aj .DOC alebo kompatibilných vo forme editovateľnej pre verejného obstarávateľa(vrátane ich aktualizácie, ako je definované nižšie v tomto dokumente), video objekty musia byť v štandardne používanom video formáte (napr.: H.264 alebo ekvivalent špecifikovaný v kapitole 2.2.3.3), zvukové objekty musia byť v štandardne používanom audio formáte (napr.: mp3 alebo ekvivalent špecifikovaný v kapitole 2.2.3.4)
- pravidelná aktualizácia dodaných vzdelávacích materiálov/obsahov z hľadiska legislatívnych zmien, ktoré sú odsúhlasené verejným obstarávateľom podľa harmonogramu v kapitole 3.3 tohto opisu po dobu 25 mesiacov od účinnosti zmluvy, ktorá bude výsledkom verejného obstarávania

2.1 Cieľová skupina zamestnancov verejnej správy

Cieľová skupina zamestnancov verejnej správy pôsobiacich v ústredných orgánoch verejnej správy a rozpočtových organizáciách a príspevkových organizáciách je koncipovaná nasledovne:

- základná kategória používateľov: „laický používateľ“ a „kvalifikovaný zamestnanec“,
- riadiaca kategória používateľov: „riadiaci zamestnanec“ a „špecializovaný riadiaci zamestnanec“.

Používateľ		**Charakteristika kategórie**	**Cieľ vzdelávania**
základná kategória používateľov	laický používateľ **modul č. 1 až č. 4**	používateľ informačno-komunikačných technológií mimo vykonávania konkrétneho povolania	1. pochopiť význam vybraných základných pojmov kybernetickej bezpečnosti, 2. pochopiť význam osobných údajov a citlivých informačných aktív v mimopracovnej oblasti a osvojiť si základné pravidlá bezpečnej manipulácie a používania IKT.
	kvalifikovaný zamestnanec **modul č. 1 až č. 4**	Zamestnanec používajúci informačno-komunikačných technológií, ktorý pri výkone povolania využíva sieť alebo informačný systém	1. pochopiť význam vybraných základných pojmov kybernetickej bezpečnosti, 2. pochopiť úlohu používateľa a z nej vyplývajúcu zodpovednosť v systéme kybernetickej bezpečnosti, 3. porozumieť významu informačných aktív s ktorými zamestnanec pracuje,

			4. pochopiť potrebu ochrany informácií a informačných aktív, 5. naučiť sa základné pravidlá bezpečnej práce s IKT, 6. rozoznať incident a vedieť naň správne a včas reagovať, 7. pochopiť bezpečnostné politiky a používanie bezpečnostných mechanizmov v pracovných procesoch.
riadiaca kategória používateľov	riadiaci zamestnanec **modul č. 5**	riadiaci zamestnanec, ktorý do značnej miery zodpovedá za príslušný proces alebo skupinu procesov a v rámci nich zodpovedá aj za plnenie úloh v oblasti riadenia rizík kybernetickej bezpečnosti a zároveň nie je manažérom IT alebo manažérom KB	1. pochopiť význam vybraných základných pojmov kybernetickej bezpečnosti, 2. pochopiť riziká kybernetickej bezpečnosti v riadených procesoch, 3. získať znalosť analyzovať požadovanú úroveň ochrany informačných aktív, 4. získať znalosť integrovať požiadavky kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov, 5. osvojiť si znalosť určiť a dozerať na plnenie požiadaviek kybernetickej bezpečnosti pri obstaraní produktov a služieb a pri procesoch podporovaných tretími stranami.
	špecializovaný riadiaci zamestnanec **modul č. 6**	riadiaci zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, vlastníci bezpečnostných procesov	1. získať znalosť vytvoriť rámec riadenia kybernetickej bezpečnosti v organizácii, 2. získať znalosť riadiť procesy súvisiace s informačnou a kybernetickou bezpečnosťou v organizácii, 3. získať znalosť formulovať návrhy a odporúčania na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení a navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti, 4. získať znalosť navrhovať, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia, 5. získať znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív, 6. získať znalosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru, 7. získať a osvojiť si znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a

			schopnosť uplatňovať ich v procesoch organizácie, 8. získať znalosť o presadzovaní bezpečnostných opatrení.

2.2 Požiadavky na vzdelávacie materiály

Vzdelávacie materiály budú dostupné pre každú definovanú cieľovú skupinu (kategóriu používateľov, ktorá obsahuje samostatné pozície) a to v elektronickej forme, pričom obsah a spôsob vyhotovenia vzdelávacích materiálov musí byť v takej podobe, ktorá umožňuje vkladať vytvorené vzdelávacie materiály vytvorené úspešným uchádzačom do e-learningovej platformy verejného obstarávateľa.

Samotná realizácia školiacich aktivít v kontexte e-learningového systému určenom verejným obstarávateľom nie je súčasťou tohto verejného obstarávania, t. j. tieto aktivity nebudú realizované úspešným uchádzačom v rámci procesu vytvorenia a dodania vzdelávacích materiálov. Súčasťou predmetného verejného obstarávania nie je výroba e-learningovej platformy. E-learningová platforma je vo vlastníctve, v správe a prevádzke verejného obstarávateľa a je postavená na open source produkte moodle.

Vzdelávacie materiály budú rozdelené do šiestich modulov - moduly č. 1 až č. 6 vrátane ich variant dodávaných počas účinnosti zmluvy, budú dodané:

- v elektronickej podobe v e-learningovej forme, ktoré sú uvedené v kapitole 2, pričom vzdelávacie materiály budú dodané na zvolenom nosiči informácií podľa požiadaviek verejného obstarávateľa (napr. USB nosič alebo DVD nosič), a zároveň
- v elektronickej podobe ako .PDF a .DOC súbory alebo v kompatibilných formátoch, ktoré umožňujú editáciu verejným obstarávateľom (vrátane ich aktualizácie, ako je definované nižšie v tomto dokumente), najmä scenáre a obsah kapitol v moduloch, dodané na verejným obstarávateľom zvolenom nosiči informácií (napr. USB nosič alebo DVD nosič)

Vzdelávacie materiály musia obsahovať všetky informácie nevyhnutné pre dosiahnutie špecifických cieľov potrebné na zvyšovanie znalostných štandardov tak, ako sú definované v kapitole 3.1 (Všeobecné požiadavky na vzdelávacie moduly) tohto dokumentu.

Vzdelávacie materiály budú rozdelené do viacerých logických celkov - kapitol, ktoré sa budú nachádzať v každom požadovanom module, pričom moduly č. 1 až č. 4 sú povinné pre všetkých zamestnancov verejnej správy a majú charakter náučno-popularizačný, modul č. 5 je určený špecificky len pre kategóriu používateľov „riadiaci zamestnanec“ a modul č. 6 je určený špecificky len pre kategóriu používateľov „špecializovaný riadiaci zamestnanec“ z definovanej cieľovej skupiny. Obsahová špecifikácia jednotlivých modulov a kapitol je zahrnutá v kapitole 3.1 (Všeobecné požiadavky na vzdelávacie moduly) tohto dokumentu.

2.2.1 Požiadavky na testovanie

Pri každom jednotlivom module, ktorý pozostáva z kapitol, požadujeme zaradiť minimálne v polovici z celkového počtu kapitol rozhodovací mikro test – vyklikávací formulár počas trvania aktuálnej kapitoly s výberom dvoch odpovedí – v prípade nesprávnej odpovede nasleduje vysvetlenie, prečo bola odpoveď nesprávna, v prípade správnej odpovede nasleduje pokračovanie videa s ocenením správnej odpovede.

Na záver každej kapitoly požadujeme zaradiť krátke testy (nerozumie sa v zmysle záverečného testu) ale na pochopenie obsahu prezentovanej kapitoly. Test by mal obsahovať tri otázky formou vyklikávacieho formuláru - v prípade nesprávnej odpovede možnosť zopakovať výber.

Súčasťou vzdelávacích materiálov musí byť po ukončení každého individuálneho modulu (modul č. 1 až modul č. 6) aj záverečný test na zhrnutie učiva, ktorým sa zhodnotia nadobudnuté vedomosti a znalosti individuálne pre každého používateľa podľa definovanej cieľovej skupiny. Test musí byť koncipovaný spôsobom, aby priemerný používateľ so znalosťami získanými z e-learningového školenia vedel získať minimálne 70% úspešnosť inak musí test opakovať v novej vygenerovanej variante, teda neopakuje rovnaký test. Po úspešnom absolvovaní systém vygeneruje osvedčenie o absolvovaní daného modulu.

Záverečný test po absolvovaní každého modulu pozostáva z 20 otázok (otázky z každej kapitoly), verejný obstarávateľ požaduje vyhotoviť tri varianty záverečného testu – spolu 60 otázok. Preto požadujeme vytvoriť databázu , ktorá bude tvoriť 360 otázok pre 6 modulov. Pre moduly č. 1 až 5 je na každú otázku záverečného testu správna iba jedna odpoveď. Pre modul č. 6 musí každá otázka záverečného testu pozostávať zo 4 možností odpovedí, pričom správna môže byť jedna, dve, alebo tri odpovede prípadne žiadna. Pred začiatkom záverečného testu bude pre absolventov modulu vopred uvedená informácia o viacerých možnostiach odpovedí.

Vzdelávacie materiály musia obsahovať všetky informácie nevyhnutné pre dosiahnutie špecifických cieľov zvyšovania znalostných štandardov, ako sú definované v kapitole 3.1 (Všeobecné požiadavky na vzdelávacie moduly) tohto dokumentu.

2.2.2 Požiadavky na vzdelávacie moduly

Verejný obstarávateľ požaduje od úspešného uchádzača dodanie vzdelávacích modulov v oblasti kybernetickej bezpečnosti. Tvorca vzdelávacích materiálov e-learningu zabezpečí skladbu vzdelávania v súlade s didaktickými zásadami vzdelávania požadovaných cieľových skupín. Každý modul bude rozdelený do tematicky uzatvorených kapitol. Verejný obstarávateľ požaduje vytvorenie a nasadenie do e-learningovej platformy verejného obstarávateľa min. nasledujúce typy e-learningových prístupov, ktoré budú v každej kapitole jednotlivých modulov:

I. Video obsah – podľa rozpisu schváleného scenára – obsahuje audiovizuálny obsah vzdelávacej časti, sprevádzanej jedným moderátorom doplnené napr. grafickými prvkami a názornými ukážkami formulárov/podkladov; a vysvetľujúci rozhovor s odborníkom na riešenú tému. Môže obsahovať vlastné vyrobené videá, stockové videá, podmazovú hudbu a pod.

II. Interaktívna časť - obsahujú videá, animácie a prezentácie spolu s rôznymi interaktívnymi cvičeniami, ktoré používatelia musia dokončiť, aby si osvojili poznatky z prezentovaného učiva. Môže slúžiť ako rozhodovací mikro test – vyklikávací formulár počas trvania kapitoly s výberom dvoch odpovedí – v prípade nesprávnej odpovede nasleduje vysvetlenie prečo bola odpoveď nesprávna, v prípade správnej odpovede nasleduje pokračovanie videa s ocenením správnej odpovede, ktorej vizuál (napr. text, zvuk, obraz, atď.) pripraví úspešný uchádzač., tzn. navrhne akou formou bude používateľ informovaný o správnej odpovedi. Táto požiadavka je v réžii úspešného uchádzača. V každej kapitole požadujeme jednu interaktívnu časť kvalitou zodpovedajúcou tvorbe tímu grafika alebo animátora v min. trvaní 3 minúty. Interaktívna časť má za cieľ preveriť pochopenie prezentovanej látky v danej kapitole.

III. Simulácie - poskytujú používateľom príležitosť absolvovať v rámci vzdelávacieho procesu konkrétnej kapitoly napr. formou kybernetického útoku alebo špecifický malware útok a zistiť, ako sa môžu chrániť pred rôznymi typmi hrozieb. Realizácia simulácie prostredníctvom audiovizuálneho obsahu alebo animovanou grafikou alebo vyklikávacím testom možností ako by používateľ reagoval. Simulácie majú za cieľ v každej kapitole dať používateľom školenia príležitosť vyskúšať si simulovanú vysvetľovanú situáciu alebo vtiahnuť do riešeného obsahu kapitoly používateľa tak, aby sa stal súčasťou riešeného obsahu kapitoly, uplatní sa podľa vhodnosti riešenej kapitoly. Verejný obstarávateľ požaduje 2 simulácie kvalitou zodpovedajúca tvorbe tímu grafika alebo animátora v min. trvaní 5 minút, v každom požadovanom module (odporúčané umiestnenie: prvá simulácia v prvej polovici z celkového počtu kapitol a druhá simulácia v druhej polovici z celkového počtu kapitol).

IV. Komentovaný čítaný text – vysvetlenie pojmov s vizualizáciou/ animáciou, obsah v textovej podobe s grafickou úpravou zjednocujúcou kapitoly modulu, slúži ako komentár k prezentovanej látke. Pod pojmom komentovaný čítaný text verejný obstarávateľ má na mysli vložené učebné texty (vytvorené požadovaným expertom) ktoré sú bližšie komentované osobou, ktorá sa bude podieľať na tvorbe zvukového záznamu, ktorá prečíta, prípadne opíše (situáciu, obraz, animáciu, grafiku, uvedený text..), osoba zodpovedná za komentovaný čítaný text bude zároveň moderátorom v zmysle požiadavky na moderátora, ktorý je uvedený v tomto opise.
Komentovaný čítaný text k prezentovanej látke, môže byť aj vyskladaním viacerých komentárov v min. trvaní 5 minút celkovo na jednu kapitolu – uplatní sa podľa potreby jednotlivých kapitol, nie je podmienkou mať v každej kapitole komentár ak túto časť nahrádza moderátor na obraze. Cieľom je v častiach kapitoly, uľahčiť pochopenie prezentovaného obsahu na celú obrazovku ak nie je na obraze moderátor.

V. Študijné materiály - zaradená časť na vypublikovanie a sťahovanie komunikovaných pracovných podkladov – súborov napr. v PDF/DOC/XLSX/JPG a pod. alebo vo forme aktívnych linkov, z ktorých je možné sťahovanie voľne dostupných materiálov alebo vo vzdelávacej časti odporúčané linky na webové lokality na samostatnom okne/slide. Vytvorenie študijných materiálov nie je v kompetencii úspešného uchádzača, ide o rozšírenie študijného obsahu o voľne dostupné materiály nachádzajúce sa na webovom rozhraní (príklad: odkazy na slovlex, webové portály relevantných inštitúcií a pod.)

VI. Testovanie vedomostí - pozostáva z krátkych kvízov počas samotného vzdelávania (animované a/alebo grafické znázornenie zábavnou formou) alebo testov, ktoré používateľov testujú na ich znalosti v oblasti kybernetickej bezpečnosti. Požiadavky definované v kap. 2.2.1

2.2.3 Požiadavky na zloženie modulov, formáty, technická špecifikácia

Verejný obstarávateľ požaduje dodanie každého z definovaných modulov č. 1 až č. 6, definovaných v kap. 3.1.1 až 3.1.5 rozdelených na kapitoly. Realizácia vzdelávania bude nastavená v platforme verejného obstarávateľa pre používateľa spôsobom, aby mohol vzdelávanie absolvovať samostatne po kapitolách, naraz aj prerušovane, pričom pokračuje od naposledy zastaveného času, riešenie je optimalizované na rozhranie desktop/mobilné zariadenie/tablet.

Každá kapitola má trvanie min. 30 – max. 45 minút, video obsah v zmysle bodu I. kap. 2.2.2 obsahuje 4 videá podľa schváleného scenára, pričom:

- 1 video - dĺžka videa min. 7 – max. 14 minút je formou vysvetľujúceho štúdiového rozhovoru moderátora s odborníkom na riešenú tému (za odborníka považuje verejný obstarávateľ minimálne certifikovaného audítora KB v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, podľa NBÚ certifikačnej schémy overovania odbornej spôsobilosti audítora kybernetickej bezpečnosti , kt. zároveň disponuje 2 ročnou praxou v audite KB alebo minimálne certifikovaného manažéra KB v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, podľa NBÚ certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti, kt. zároveň disponuje 2 ročnou praxou ako manažér KB). Zdrojové informácie odporúčame čerpať napr. zo Správ o kybernetickej bezpečnosti v Slovenskej republike za jednotlivé roky od NBÚ. 3 videá - s dĺžkou jedného videa min. 3 – max. 6 minút je formou vysvetľovacieho videa prezentovaním/ vysvetľovaním riešeného problému/látky. Realizované jedným moderátorom sprievodným hlasom, doplnené napr. grafickými prvkami a názornými ukážkami formulárov/podkladov,

Celkový počet videí pre všetky moduly je 200, po schválení verejným obstarávateľom je možné meniť umiestnenie z požadovaného počtu videí (1 video) v každej kapitole, medzi rôzne kapitoly, pričom celkový počet videí musí byť dodržaný. V praxi to znamená, že ak v danej kapitole nebude možné vytvoriť videá na základe riešenej problematiky, tém, učebného textu a pod. sa tento požadovaný počet môže použiť v inej kapitole, kde sú témy v určitej kapitole rozsiahlejšie a je možné vytvoriť a použiť viacero videí v jednej kapitole.

Celkový počet interaktívnych častí je 50, po schválení verejným obstarávateľom je možné meniť umiestnenie z požadovaného počtu interaktívnych častí (1 interaktívna časť) v každej kapitole medzi rôzne kapitoly, pričom celkový počet interaktívnych častí musí byť dodržaný. V praxi to znamená, že ak v danej kapitole nebude možné vytvoriť interaktívnu časť na základe riešenej problematiky, tém, učebného textu a pod. sa tento požadovaný počet môže použiť v inej kapitole, kde sú témy v určitej kapitole rozsiahlejšie a je možné vytvoriť a použiť viacero interaktívnych častí v jednej kapitole.

Celkový počet simulácií pre všetky moduly je 12, (2 požadované simulácie v jednom module) po schválení verejným obstarávateľom je možné meniť požadované umiestnenie simulácií medzi modulmi, pričom celkový počet simulácií musí byť dodržaný.

Z hľadiska realizácie video obsahu požaduje verejný obstarávateľ, na základe schváleného návrhu scenára, dodanie profesionálnych moderátorov (osoba zodpovedná za tvorbu vzdelávacej aktivity prostredníctvom tvorby audiovizuálneho alebo zvukového záznamu) moderovaného video obsahu s obsadením jeden muž a jedna žena (primerané striedanie moderátorov po moduloch resp. po kapitolách) tak aby dramaturgicky zapadli do celkovej realizácie vzdelávacích modulov. Verejný obstarávateľ požaduje predložiť zoznam 2

moderátorov v obsadení jeden muž a jedna žena. Profesionálny moderátor/moderátorka musí mať profesionálne skúsenosti s moderovaním audiovizuálnych diel televíznej produkcie alebo v oblasti audiovizuálnych vzdelávacích programov (TV programy, Online programy, vzdelávacie audiovizuálne diela, TV dokumenty, hrané vzdelávacie a informačné spoty).

Z hľadiska realizácie audiovizuálnej časti e-learningu profesionálnym tímom požadujeme minimálne zastúpenie týchto profesií – režisér, scenárista, produkčný výrobného tímu, strihač, grafický dizajnér, animátor. Uvedené profesie musia mať skúsenosti s výrobou audiovizuálnych diel televíznej produkcie alebo v oblasti audiovizuálnych vzdelávacích programov (TV programy, Online programy, vzdelávacie audiovizuálne diela, TV dokumenty, hrané vzdelávacie a informačné spoty) na úrovni ich špecializácie. Úspešný uchádzač preukáže disponibilitu týchto profesií obsadených za každú profesiu jednou osobou menným zoznamom do 5 pracovných dní od účinnosti zmluvy. Zoznam podlieha schváleniu verejným obstarávateľom, s možnosťou výmeny osoby priradenej k požadovanej profesií.

2.2.3.1 Detailná špecifikácia jednotlivých modulov

Základom bude schválený návrh realizácie, priebežne konzultovaný a schvaľovaný verejným obstarávateľom - v súlade s harmonogramom, ktorý musí obsahovať:

2.2.3.1.1 Prvá fáza do 3 mesiacov

- úspešný uchádzač dodá do 3 mesiacov od účinnosti zmluvy Návrh scenárov všetkých kapitol modulu č. 1, plánované časové trvanie jednotlivých scén, návrhy grafiky, návrh animácie a návrh moderátorského a hlasového obsadenia na základe výberu konzultované s verejným obstarávateľom vo video obsahoch ako zapadnú do konkrétneho vzdelávacieho modulu, návrh obsadenia odborníkov ako bude celý vzdelávací modul vyzerať ako celok.
- úspešný uchádzač uvedie ako budú zakomponované infografiky, animácie, resp. iné číselné, textové alebo inak graficky spracované informácie v súlade s dizajnom špecifikovaným v kapitole 2.2.3.5.
- návrhy v rámci prvej fázy bude uchádzač s verejným obstarávateľom konzultovať vo 4. a 8. týždni prvej fázy od účinnosti zmluvy, finálne schválenie návrhov bude realizované v 12. týždni realizácie prvej fázy

2.2.3.1.2 Druhá fáza do 6 mesiacov

- úspešný uchádzač v súlade s verejným obstarávateľom schválenou prvou fázou v kap. 2.2.3.1.1 dodá detailný scenár všetkých kapitol modulov č. 1 až č. 6, opis scén, časové trvanie jednotlivých scén, grafiky, animácie a konkrétne moderátorské obsadenie vo video obsahoch konkrétneho vzdelávacieho modulu, konkrétne obsadenie odborníkov ako bude celý vzdelávací obsah vyzerať ako celok.
- úspešný uchádzač uvedie konkrétny sprievodný hlas komentárov, ktoré môžu komentovať dianie na obrazovke, resp. číselné a/alebo textové údaje, infografiky alebo animácie kvôli lepšiemu znázorneniu informácií - sprievodný hlas vo vzdelávacích obsahoch zabezpečuje moderátor príslušnej kapitoly.
- návrhy v rámci druhej fázy bude úspešný uchádzač s verejným obstarávateľom konzultovať v 16. a 20. týždni druhej fázy od účinnosti zmluvy, finálne schválenie návrhov bude realizované v 24. týždni realizácie druhej fázy

Všetky kapitoly v jednotlivých moduloch, budú spĺňať kritéria prístupnosti aj pre určitým spôsobom znevýhodnených používateľov so zdravotným postihnutím (napr. zrakovo, sluchovo postihnuté osoby a pod.) podľa Vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie SR č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy.

V súlade s uvedeným požadujeme minimálne:

- slovenské titulky s možnosťou nastavenia veľkosti písma, ako vypínateľnú funkcionalitu
- možnosť nastaviť rýchlosť prehrávania vzdelávania/video obsahu (vyššou alebo nižšou rýchlosťou)
- v súvislých textových častiach neobsahuje viac ako 10 riadkov, ak je riadkov viac, tieto oddeliť odrážkami, grafikou a pod.
- dodržiavať rovnaké ikonky na ovládanie
- text, ktorý nie je hyperlinkom, nesmie byť podčiarknutý
- ak je potrebné text vyznačiť, neodporúčame použiť modrú farbu
- možnosť vrátiť sa k jednotlivým častiam kapitoly, história pozretého/absolvovaného

2.2.3.2 Minimálne požadované formáty vzdelávacích modulov e-learningu

Verejný obstarávateľ požaduje dodanie výukových kapitol v rámci jednotlivých modulov v jednom zo štandardne používaných formátoch, video formáty definované v kap. 2.2.3.3 a textové časti (napr. formuláre) v jednom zo štandardných formátov napr.: SCORM, xAPI, AICC alebo ekvivalent.

Cieľom zákazky je aby bol verejný obstarávateľ schopný vo svojej platforme po uplynutí rámcovej dohody upraviť prípadné textové časti kapitoly, ktoré sa zmenili vplyvom vonkajších okolností (napr. zmena vyhlášky, zákona a pod.) aby bola zachovaná správnosť a aktuálnosť vzdelávacieho obsahu.

2.2.3.3 Minimálne požiadavky na realizáciu video obsahu a výstupný formát

Verejný obstarávateľ požaduje realizáciu nakrúcania v profesionálnom štúdiu s minimálnym vybavením:

- štúdio o rozmere min. 25 m^2
- tri štúdiové kamery na statívoch, čítacie zariadenie
- osvetľovacia technika závesná na rampovom systéme alebo samostatných statívoch
- zvuková technika – min. 3 mikroporty, v prípade potreby mikrofón
- zelená kľúčovacia stena a iné vhodné štúdiové pozadie
- strihová réžia, alebo postprodukcia v strižni
- profesionálny personál na obsluhu techniky (kameraman, zvukár, osvetľovač)

Verejný obstarávateľ si vyhradzuje právo účasti na výrobe osobne – určenou zodpovednou osobou, resp. osobami.

Video obsah požadujeme dodávať v kvalite používateľmi školenia nepostrehnuteľnej kompresie zobrazeného videa a zvuku. Požadované video formáty: H.264,alebo H.265 alebo WebM alebo ekvivalent - vzdelávacie materiály vo formátoch súborov podľa vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov.

2.2.3.4 Minimálne požadované formáty zvuku

Verejný obstarávateľ požaduje dodanie zvukového obsahu v štandardne používanom formáte s podmienkou zachovania kompatibility s vybraným formátom vzdelávacích modulov úspešným

uchádzačom. Zvukový obsah požadujeme dodávať v kvalite používateľmi školenia nepostrehnuteľnej kompresie použitej zvukovej stopy v stereo kvalite. Požadované zvukové formáty: MP3 alebo WAV alebo AAC alebo ekvivalent - vzdelávacie materiály vo formátoch súborov podľa vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov.

2.2.3.5 Minimálne požadované štandardy dizajnu e-learningu

Jednotný dizajn vytvorených školiacich modulov vrátane obrazovej, zvukovej, grafickej podoby, typu, veľkosti prípadne sklonu písma prispôsobené požiadavkám pre zdravotne znevýhodnené osoby vytvorí úspešný uchádzač a po schválení verejným obstarávateľom implementuje vo vzdelávacom obsahu. Na základe schválenej vizuálnej identity verejným obstarávateľom spracuje úspešný uchádzač dodávané vzdelávacie moduly a jednotlivé druhy používaného obsahu – najmä písmo, vizualizácie, infografiky, grafiky, animácie, mapy, zvuky, videá a pod.

Verejný obstarávateľ požaduje od úspešného uchádzača dodržanie Záväzného usmernenia NIKA v súvislosti s informovaním, komunikáciou a viditeľnosťou opatrení Plánu obnovy a odolnosti SR (https://www.planobnovy.sk/realizacia/dokumenty/ , časť Vizibilita);

2.3 Požiadavky na ďalší audiovizuálny obsah

Verejný obstarávateľ požaduje dodanie ďalšieho audiovizuálneho obsahu formou upútavky, ktorý bude nasadená v prostredí e-learningovej platformy, internetu, vlastných zobrazovacích jednotiek (digitálne outdoorové a indoorové obrazovky) alebo vo vysielaní audiovizuálnych služieb TV a rádií. Nie je úlohou úspešného uchádzača realizovať propagáciu audiovizuálneho obsahu v online priestore, na sociálnych sieťach alebo v TV, obsah len vyrobí a dodá v požadovaných formátoch verejnému obstarávateľovi. Cieľom je využiť kapacitu odborníkov vystupujúcich v jednotlivých vzdelávacích moduloch a technické kapacity dodávateľa. Všeobecné požadované technické špecifikácie, ktoré nie sú bližšie špecifikované v jednotlivých podkapitolách 2.3.1, 2.3.2 a 2.3.3 sú zadefinované v kap. VI.

2.3.1 Upútavky

Upútavky požadujeme dodať pre potreby propagácie pripravených vzdelávacích modulov podľa špecifikácie verejného obstarávateľa. Dodávateľ môže použiť vyrobený materiál počas prípravy a realizácie vzdelávacích modulov. Požadovaná technická špecifikácia:

- audiovizuálny TV spot – forma: hraný alebo stockové video s grafickou úpravou podľa vizuálnej identity; dĺžka 30 sekúnd; formát: HDCam; pomer strán: 16:9; rozlíšenie 1920x1080
- audiovizuálny Web spot – forma: hraný alebo stockové video s grafickou úpravou podľa vizuálnej identity; dĺžka 20 sekúnd; formát: MP4; pomer strán: 16:9; rozlíšenie 1920x1080
- audio spot – formát: *.wav alebo *.mp3, 0db, 44,1 alebo 48 kHz, non variable bit rate 16 alebo 24Bit, stereo; dĺžka 30 sekúnd;

2.3.1.1 Upútavka na vzdelávacie moduly ako celok

Upútavka na vzdelávacie moduly ako celok bude propagovať dodávané e-learningové vzdelávanie v oblasti kybernetickej bezpečnosti a to spôsobom, ako vhodne zaujať a informovať používateľa o školení.

Požadovanými výstupmi vrátane všetkých prípravných (predprodukčných), produkčných a postprodukčných prác (ako grafická výroba, zvukovýroba, až po výstup podľa požiadavky verejného obstarávateľa) na základe scenárov, ktoré schváli verejný obstarávateľ sú:

- 1 audiovizuálny TV spot, jedna 30 sekundová verzia
- 1 audiovizuálny Web spot, jedna 20 sekundová verzia
- 1 audio spot, jedna 30 sekundová verzia

Spoty budú použité ako reklamné spoty pre TV vysielanie, pre webové portály v online v prostredí internetu, sociálne siete, online televízie, podcastové aplikácie, rádiá a digitálne outdoorové a indoorové obrazovky.

2.3.1.2 Upútavka na jednotlivé vzdelávacie moduly

Upútavka na jednotlivé vzdelávacie moduly bude propagovať témy jednotlivých modulov dodávaného e-learningového vzdelávania v oblasti kybernetickej bezpečnosti.

Požadovanými výstupmi vrátane všetkých prípravných (predprodukčných), produkčných a postprodukčných prác (ako grafická výroba, zvukovýroba, až po výstup podľa požiadavky verejného obstarávateľa) na základe scenárov, ktoré schváli verejný obstarávateľ sú:

- 6 audiovizuálnych TV spotov, pre každý modul jeden, spolu šesť rôznych spotov každý po 30 sekúnd
- 6 audiovizuálnych Web spotov, pre každý modul jeden, spolu šesť rôznych spotov každý po 20 sekúnd
- 6 audio spotov, pre každý modul jeden, spolu šesť rôznych spotov každý po 30 sekúnd

Spoty budú použité ako reklamné spoty pre TV vysielanie, pre webové portály v online v prostredí internetu, sociálne siete, online televízie, podcastové aplikácie, rádiá a digitálne outdoorové a indoorové obrazovky.

2.3.2 Rozhovory s odborníkmi

Rozhovory s odborníkmi požadujeme dodať pre potreby zrozumiteľnejšieho a rozsiahlejšieho porozumenia danej problematiky a obsiahlejšie informácie na konkrétnych 10 tém vybrané úspešným uchádzačom po konzultácií s verejným obstarávateľom, v oblasti kybernetickej a informačnej bezpečnosti – vychádzajúcich z riešenej problematiky v rámci jednotlivých modulov dodávaného e-learningového vzdelávania. Dodávateľ môže použiť vyrobený materiál počas prípravy a realizácie vzdelávacích modulov.
Požadovaná technická špecifikácia:

- audiovizuálny TV obsah – forma: štúdiový rozhovor moderátora s odborníkom s grafickou úpravou podľa vizuálnej identity; dĺžka 26 minút; formát: HDCam; pomer strán: 16:9; rozlíšenie 1920x1080
- audiovizuálny Web obsah – forma: štúdiový rozhovor moderátora s odborníkom s grafickou úpravou podľa vizuálnej identity; dĺžka 26 minút; formát: MP4; pomer strán: 16:9; rozlíšenie 1920x1080
- audio obsah – formát: *.wav alebo *.mp3, 0db, 44,1 alebo 48 kHz, non variable bit rate 16 alebo 24Bit, stereo; dĺžka 26 minút; primárne určené pre podcastovú aplikáciu

Požadovanými výstupmi vrátane všetkých prípravných (predprodukčných), produkčných a postprodukčných prác (ako grafická výroba, zvukovýroba, až po výstup podľa požiadavky verejného obstarávateľa) na základe scenárov, ktoré schváli verejný obstarávateľ sú:

- 10 audiovizuálnych TV a Web obsahov, z ktorých bude vyrobených 10 audio obsahov ako zvuková verzia rozhovorov s odborníkmi, spolu 10 rôznych rozhovorov vyrobených v troch formátoch (TV, Web, Audio)

Obsahy budú použité ako odborné rozhovory pre TV vysielanie, pre webové portály v online v prostredí internetu, sociálne siete, online televízie, podcastové aplikácie, rádiá a digitálne outdoorové a indoorové obrazovky.

2.3.3 Bonusový obsah

Bonusový obsah požadujeme dodať pre potreby popularizácie tematiky KB, ktoré na konkrétnych 10 témach v oblasti kybernetickej a informačnej bezpečnosti predstaví rebríček TOP zaujímavostí. Cieľom je vytvoriť 10 rozhovorov v nižšie navrhovaných kategóriách, obsah pred realizáciou bude predmetom konzultácie a schválenia verejným obstarávateľom.

1. TOP zaujímavosti a trendy v KB;
2. Princípy a príklady sociálneho inžinierstva (najmä: p. presviedčania, p. autority, p. náklonnosti, p. spoločenského schválenia, p. odplaty, p. nedostatku, p. záväzkov a zásadovosti)
3. Typy útokov sociálneho inžinierstva (najmä: baiting, smishing, phising, spear phishing, whaling, vishing, trashing, pharming a pod.)
4. Výber najzaujímavejších svetových prípadov KBI;
5. Výber najzaujímavejších európskych prípadov KBI;
6. Výber najzaujímavejších slovenských prípadov KBI;
7. Hodnotenie a aktuálny stav KB - štátna a súkromná sféra;
8. Vektory útokov – typy, popis, praktické príklady, prevencia, najnovšie technologické trendy v oblasti detekcie a ochrany pred útokmi;
9. Minimálny štandard KB pre bežného užívateľa;
10. Minimálny štandard KB pre bežného užívateľa – technológie budúcnosti (napr.: AI)

Dodávateľ môže použiť vyrobený materiál počas prípravy a realizácie vzdelávacích modulov. Požadovaná technická špecifikácia alebo ekvivalent:

- audiovizuálny TV obsah – forma: štúdiový rozhovor moderátora s odborníkom s grafickou úpravou podľa vizuálnej identity; dĺžka 13 minút; formát: HDCam; pomer strán: 16:9; rozlíšenie 1920x1080
- audiovizuálny Web obsah – forma: štúdiový rozhovor moderátora s odborníkom s grafickou úpravou podľa vizuálnej identity; dĺžka 13 minút; formát: MP4; pomer strán: 16:9; rozlíšenie 1920x1080
- audio obsah – formát: *.wav alebo *.mp3, 0db, 44,1 alebo 48 kHz, non variable bit rate 16 alebo 24Bit, stereo; dĺžka 13 minút; primárne určené pre podcastovú aplikáciu

Požadovanými výstupmi vrátane všetkých prípravných (predprodukčných), produkčných a postprodukčných prác (ako grafická výroba, zvukovýroba, až po výstup podľa požiadavky verejného obstarávateľa) na základe scenárov, ktoré schváli verejný obstarávateľ sú:

- 10 audiovizuálnych TV a Web obsahov, z ktorých bude vyrobených 10 audio obsahov ako ich zvuková verzia, spolu 10 rôznych rozhovorov vyrobených v troch formátoch (TV, Web, Audio)

Obsahy budú použité ako odborno-popularizačné rozhovory pre TV vysielanie, pre webové portály v online v prostredí internetu, sociálne siete, online televízie, podcastové aplikácie, rádiá a digitálne outdoorové a indoorové obrazovky.

3. Požiadavky na vzdelávacie moduly

3.1 Všeobecné požiadavky na vzdelávacie moduly

Vzdelávacie materiály **pre moduly č. 1 až 4** pre základnú kategóriu používateľov musia obsahovať všetky informácie, ktoré sú nevyhnutné pre:

- zabezpečenie realizácie vzdelávacích cieľov a získania znalostných štandardov pre kategóriu používateľov „laický používateľ“ a „kvalifikovaný zamestnanec“,

Vzdelávacie materiály **pre modul č. 5** je špecifický modul vzdelávacích materiálov, určený špecificky len pre kategóriu používateľov „riadiaci zamestnanec“ z definovanej cieľovej skupiny, musí obsahovať všetky informácie, ktoré sú nevyhnutné pre:

- zabezpečenie realizácie vzdelávacích cieľov pre kategóriu používateľov „riadiaci zamestnanec“, t. j. zabezpečenie získania príslušných vedomostí a nadobudnutia príslušných znalostí.

Vzdelávacie materiály **pre modul č. 6** je špecifický modul vzdelávacích materiálov, určený špecificky len pre kategóriu používateľov „špecializovaný riadiaci zamestnanec“ z definovanej cieľovej skupiny, musí obsahovať všetky informácie, ktoré sú nevyhnutné pre:

- zabezpečenie realizácie vzdelávacích cieľov pre kategóriu používateľov „špecializovaný riadiaci zamestnanec“, t. j. zabezpečenie získania príslušných vedomostí a nadobudnutia príslušných znalostí.

Cieľom vzdelávania pre všetky moduly je zabezpečiť zvýšenie úrovne základných vedomostí v oblasti kybernetickej a informačnej bezpečnosti a znalostných štandardov u definovanej cieľovej skupiny zamestnancov verejnej správy formou e-learningového vzdelávania.

Minimálne požiadavky na zloženie modulov a ich kapitol uvádzame v nasledovných podkapitolách 3.1.1 až 3.1.5:

3.1.1 Modul č. 1

Minimálne požadované kapitoly modulu:

Kapitola č. 1:
Úvod do základných vybraných pojmov a ich význam v kybernetickej bezpečnosti, znalosti týkajúce sa najčastejších spôsobov útokov realizovaných cez používateľov a základné typy a príklady bezpečnostných incidentov a možná obrana voči nim; vybrané príklady sociálneho inžinierstva a najčastejšie spôsoby útokov; schopnosti identifikácie a nahlásenia bezpečnostného incidentu, best practice používania internetu, sociálnych sietí, emailu, telefónu/smartphone

Kapitola č. 2:
Tvorba hesiel a používanie password manažéra; rizík verejných wifi; princípov bezpečného prehliadania stránok internetu; rozpoznávania hoaxov; kontrola správnej funkčnosti nástrojov defender/antivírus; možné dôsledky bezpečnostného incidentu pre typickú organizáciu štátnej správy/samosprávy a ďalšie, moderné trendy AI

Celkový rozsah na 1 osobu: absolvovanie modulu v minimálnej časovej dĺžke 60 minút

3.1.2 Modul č. 2

Minimálne požadované kapitoly modulu:

Kapitola č. 1:
Základné vybrané pojmy v kybernetickej bezpečnosti, napr. informačná bezpečnosť, kybernetická bezpečnosť, dôvernosť, integrita, dostupnosť, autentickosť, identita, informačný systém verejnej správy, aktívum, hrozba, zraniteľnosť, riziko, opatrenie, audit, bezpečnostný manažér,

Kapitola č. 2:
Vymenovanie a úvod a stručné vysvetlenie právnych predpisov v oblasti KB

Kapitola č. 3:
Základné pojmy v oblasti osobných údajov a citlivých informačných aktivít vrátane bezpečnej manipulácie a používania IKT, napr. spracúvanie osobných údajov, prevádzkovateľ, sprostredkovateľ, špecificky navrhnutá a štandardná ochrana osobných údajov, profilovanie, pseudonymizácia alebo anonymizácia, účel spracúvania osobných údajov, porušenie ochrany osobných údajov, doba uchovania osobných údajov.

Kapitola č. 4:
Vplyv súčasných technológií na bezpečnosť, AI technológie

Kapitola č. 5:
Znalosti týkajúce sa typických hrozieb a kategórií hrozieb, vrátane hrozieb týkajúcich sa mobilných zariadení, napr. fyzické hrozby, kompromitácia funkcií alebo služieb, ľudské konanie, organizačné hrozby, porucha infraštruktúry,

Kapitola č. 6:
Aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby, nedostatok (finančných, ľudských) zdrojov,

Kapitola č. 7:
Stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity,

Celkový rozsah na 1 osobu: absolvovanie modulu v minimálnej časovej dĺžke 210 minút

3.1.3 Modul č. 3

Minimálne požadované kapitoly modulu:

Kapitola č. 1:
Procesy identifikácie, autentizácie, autorizácie, napr. účely a náväznosť procesov, typy autentizácie, heslá/tokeny, paswordless autentifikácia, single sign-on, , prípady zneužitia, autorizácia, identifikácia, verifikácia, rola, identita,

Kapitola č. 2:
Spôsoby overenia digitálnej totožnosti a významu viacfaktorovej autentizácie, napr. autentizačné prvky, prípady použitia MFA, obmedzenia MFA v praxi, riadenie digitálnej identity (IAM), prípady zneužitia, typy autentizačných faktorov,

Kapitola č. 3:
Základné princípy tvorby a používania hesiel, napr. bezpečnostné parametre hesla (dĺžka, skladba, ...), ochrana hesla, obnova hesla, odolnosť/sila hesla a najčastejšie chyby pri jeho používaní, prípady zneužitia, hygiena hesiel, význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom,

Kapitola č. 4:
Základné riziká používania zariadení IKT, napr. neoprávnené použitie , infiltrácia, zanedbaná údržba, zneužitie oprávnení, riziká dodávateľských vzťahov, vendor-lock, obstaranie IKT služieb a ich rizika,

Kapitola č. 5:
Základné princípy vzdialeného prístupu a bezpečnostných zásad pri práci z domu a práci na diaľku, napr. používanie silných hesiel, používanie VPN pre zabezpečenie komunikácie, zabezpečenie sieťovej infraštruktúry a zariadení, používanie firewallu a antivírusového softvéru, používanie 2-faktorovej autentifikácie, pravidelné zálohovanie dôležitých dát, šifrovanie zariadení, oddelenia úložiska zariadenia (sandboxing),

Kapitola č. 6:
Bezpečnostné riziká cloud computingu,

Kapitola č. 7:
Podstaty šifrovania a kryptografických mechanizmov, napr. symetrické/asymetrické šifrovanie, odolnosť šifrovania, typy útokov na tieto mechanizmy, rozdiely medzi šifrovaním a kódovaním, prípady použitia, verejné/privátne kľúče, PKI,

Kapitola č. 8:
Pojmy - digitálny popis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka, napr. vzťah podpisu a elektronického podpisu, KEP/ZEP, scenáre použitia, aktuálna slovenská a európska právna úprava a právne účinky, využitie pri elektronických službách, hashovanie,

Celkový rozsah na 1 osobu: absolvovanie modulu v minimálnej časovej dĺžke 240 minút

3.1.4 Modul č. 4

Minimálne požadované kapitoly modulu:

Kapitola č. 1:
Bezpečnostné riziká a riziká ochrany súkromia pri telekonferenciách a online rokovaniach/stretnutiach, napr. zneužívanie zaznamenaných videokonferencií, špionáž prostredníctvom webkamery, uniknutie osobných údajov používateľov, útoky na zabezpečenie videokonferencie, zneužívanie zdieľaných súborov a informácií, phishing a sociálne inžinierstvo využívajúce videokonferencie,

Kapitola č. 2:
Bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí, napr. únik osobných údajov, phishing a sociálne inžinierstvo, šírenie klamlivých informácií a dezinformácií, cyberstalking, zneužívanie dôverných informácií, riziko porušenia firemných pravidiel a tajomstva, zneužívanie profilu na kriminalitu,

Kapitola č. 3:
Podstata útokov formou sociálneho inžinierstva, napr. (phising, vishing, smishing, vydávanie sa za inú osobu, prezentácia falošných príležitostí, vymáhanie dôverných informácií, prezentácia falošných správ, imitácia bezpečnostných inštitúcií, Business Email Compromise),

Kapitola č. 4:
Základy trestného práva v kontexte kybernetického priestoru, napr. vzťah medzi bezpečnostným incidentom a počítačovým trestným činom, taxonómia incidentov pre orgány činné v trestnom konaní, trestné právo a GDPR, OČTK, forenzné dôkazy,

Kapitola č. 5:
Znalosti týkajúce sa bezpečnej manipulácie s prostriedkami IKT, napr. zabezpečenie hesiel, dodržiavanie firemných politík bezpečnosti, používanie softvéru na ochranu proti malware, používanie sieťových

bezpečnostných opatrení, bezpečné vyraďovanie IKT, firewalling / riadenie sieťových prestupov, CMDB, hardenig, logy, bezpečnostný monitoring, Nástroj na riadenie servisných požiadaviek, dodávateľ,

Kapitola č. 6:
Znalosti týkajúce sa bezpečným zaobchádzaním s osobnými údajmi, podľa činností definovaných v nariadení GDPR,

Kapitola č. 7:
Znalosti týkajúce sa používania bezpečnostných mechanizmov v pracovných procesoch, napr. správa hesiel, využívanie firewall/EDR/VPN, mechanizmy riadenia prístupu, šifrovanie, zálohovanie, testovanie bezpečnosti, reportovanie bezpečnosti, nastavenie zodpovedností, vzdelávanie zamestnancov,

Kapitola č. 8:
Znalosti týkajúce sa rozpoznania bezpečnostného incidentu a správnej reakcie na incident, napr. identifikácia bezpečnostných incidentov, kontrola škôd, kontrola dôkazov, koordinácia s bezpečnostnými tímami, kontrola opatrení na ochranu, CSIRT/CERT, SOC, SIEM, bezpečnostný monitoring,

Kapitola č. 9:
Znalosti týkajúce sa dodržiavania bezpečnostných zásad a platných politík, napr. používanie firemných počítačov a sietí, používanie osobných zariadení na prácu, používanie firemných aplikácií a služieb, zdieľanie informácií a súborov, dodržiavanie pravidiel pre elektronickú komunikáciu, bezpečnostné povedomie a vzdelávanie, bezpečnostná dokumentácia, úroveň/typ/forma/úložisko bezpečnostnej dokumentácie,

Celkový rozsah na 1 osobu: absolvovanie modulu v minimálnej časovej dĺžke 270 minút

3.1.5 Modul č. 5

Špecifický modul vzdelávacích materiálov, určený špecificky len pre kategóriu používateľov „riadiaci zamestnanec“ z definovanej cieľovej skupiny.

Minimálne požadované kapitoly modulu:

Kapitola č. 1:
Porozumenie rizikám kybernetickej bezpečnosti v riadených procesoch vrátane zásad riadenia fyzickej a objektovej bezpečnosti, procesu riadenia rizík, postupov a metodiky analýzy rizík,

Kapitola č. 2:
Postupy analýzy požadovanej úrovne ochrany informačných aktív,

Kapitola č. 3:
Tvorba podmienok pre riadenie bezpečnosti informácií v organizácii,

Kapitola č. 4:
Integrácia požiadaviek kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov, metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie,

Kapitola č. 5:

Definícia a dohľad na plnenie požiadaviek kybernetickej bezpečnosti pri obstaraní produktov a služieb a pri procesoch podporovaných tretími stranami

Kapitola č. 6:
Odporúčania na ďalšie vhodné informačné zdroje umožňujúce prehĺbiť si znalosti v oblasti kybernetickej bezpečnosti – verejne prístupné informačné zdroje, odborná literatúra, dostupné kurzy.

Celkový rozsah na 1 osobu: absolvovanie modulu v minimálnej časovej dĺžke 180 minút

3.1.6 Modul č. 6

Špecifický modul vzdelávacích materiálov, určený špecificky len pre kategóriu používateľov „špecializovaný riadiaci zamestnanec“ z definovanej cieľovej skupiny.

Minimálne požadované kapitoly modulu:

Kapitola č. 1:
Postupy pre tvorbu rámca riadenia kybernetickej bezpečnosti v organizácii – časť I.,

Kapitola č. 2:
Postupy pre tvorbu rámca riadenia kybernetickej bezpečnosti v organizácii – časť II.,

Kapitola č. 3:
Riadenie procesov súvisiacich s informačnou a kybernetickou bezpečnosťou v organizácii– časť I.,

Kapitola č. 4:
Riadenie procesov súvisiacich s informačnou a kybernetickou bezpečnosťou v organizácii– časť II.,

Kapitola č. 5:
Tvorba návrhov a odporúčaní na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení. Navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti – časť I.,

Kapitola č. 6:
Tvorba návrhov a odporúčaní na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení. Navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti – časť II.,

Kapitola č. 7:
Tvorba návrhov a odporúčaní na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení. Navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti – časť III.,

Kapitola č. 8:
Princípy návrhov, implementácie, údržby a prevádzky bezpečnostných mechanizmov a riešenia – časť I.,

Kapitola č. 9:
Princípy návrhov, implementácie, údržby a prevádzky bezpečnostných mechanizmov a riešenia – časť II.,

Kapitola č. 10:
Právne a etické požiadavky na zaručenie bezpečnosti informačných aktív – časť I.,

Kapitola č. 11:
Právne a etické požiadavky na zaručenie bezpečnosti informačných aktív – časť II.,

Kapitola č. 12:
Tvorba bezpečnostných stratégii, bezpečnostnej politiky a bezpečnostnej architektúry – časť I.,

Kapitola č. 13:
Tvorba bezpečnostných stratégii, bezpečnostnej politiky a bezpečnostnej architektúry – časť II.,

Kapitola č. 14:
Tvorba bezpečnostných stratégii, bezpečnostnej politiky a bezpečnostnej architektúry – časť III.,

Kapitola č. 15:
Techniky a metódy vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie – časť I.,

Kapitola č. 16:
Techniky a metódy vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie – časť II.,

Kapitola č. 17:
Zásady pri presadzovaní bezpečnostných opatrení – časť I.,

Kapitola č. 18:
Zásady pri presadzovaní bezpečnostných opatrení – časť II.,

Celkový rozsah na 1 osobu: absolvovanie modulu v minimálnej časovej dĺžke 540 minút

3.2 Autorské práva k dodaným vzdelávacím materiálom

Verejný obstarávateľ bude oprávnený použiť dodané vzdelávacie materiály v zmysle kapitoly 2 a kapitoly 3 tohto dokumentu nasledovne: použitie autorského diela vo forme výhradnej, bezodplatnej, vecne, časovo a územne neobmedzenej licencie na všetky spôsoby použitia, najmä v súlade s § 19 ods. 4 autorského zákona, bez akýchkoľvek ďalších obmedzení; verejný obstarávateľ bude najmä oprávnený aj na zverejnenie diela, označenie diela svojim názvom, na zmenu diela alebo ktorejkoľvek jeho časti, na akékoľvek iné zásahy do diela a na dokončenie diela, vždy po odovzdaní a akceptovaní každej verzie vzdelávacích materiálov.

3.3 Periodická aktualizácia dodaných vzdelávacích materiálov

Vzdelávacie materiály vytvorené a dodané úspešným uchádzačom bude pravidelne aktualizovať, a to v 4-mesačnej aktualizačnej lehote, počas celej doby trvania projektu alebo aj častejšie v prípade relevantnej legislatívnej zmeny.

Dodanie vytvorených vzdelávacích materiálov bude teda prebiehať nasledovne:

— Prvá verzia vzdelávacích materiálov musí byť dodaná najneskôr do 9 mesiacov odo dňa nadobudnutia účinnosti zmluvy,
— Druhá až štvrtá verzia vzdelávacích materiálov musí byť dodaná v lehote do 4-mesiacov od dodania predchádzajúcej verzie vzdelávacích materiálov,
— Piata verzia vzdelávacích materiálov musí byť dodaná na konci projektu a to v lehote do 25 mesiacov od účinnosti zmluvy,
— Úspešný uchádzač sa zaväzuje dodať aktualizáciu vzdelávacích materiálov aj v prípade relevantnej zmeny legislatívy a to najneskôr do 30 dní odo dňa nadobudnutia účinnosti príslušného zákona. Túto povinnosť nemá v prípade, ak legislatívna zmena nadobudla účinnosť tesne pred dodaním nasledujúcej verzie (t. j. bezprostredne pred začiatkom plynutia 30-tich dní), pričom uvedené zmeny musí zapracovať do najbližšej verzie vzdelávacích materiálov. V prípade, ak legislatívna zmena nadobudla účinnosť menej ako 30 dní pred dátum dodania najbližšej aktualizácie vzdelávacích materiálov, môže úspešný uchádzač požiadať o predĺženie lehoty na dodanie novej verzie vzdelávacích materiálov, maximálne však o 14 dní.

Úhrada odmeny úspešného uchádzača za dodanie jednotlivých verzií vzdelávacích materiálov bude realizovaná nasledovne:

— 70% z celej výšky odmeny bude uhradených po dodaní prvej verzie vzdelávacích materiálov a po ich akceptácii zo strany verejného obstarávateľa,
— 30% z celej výšky odmeny bude uhradených po dodaní poslednej (piatej) verzie vzdelávacích materiálov a po ich akceptácii zo strany verejného obstarávateľa.

Každá aktualizácia vzdelávacích materiálov musí reflektovať aktuálne zmeny a trendy týkajúce sa obsahových požiadaviek špecifikovaných v kapitole 3.1 tohto dokumentu, a to najmä (ale nie len) v kontexte aktuálneho vývoja:

— typických zraniteľností a hrozieb a kategórií hrozieb,
— bezpečnostných rizík a rizík ochrany súkromia v súvislosti s používaním zariadení IKT, elektronických služieb, cloud computingu, telekonferencií / online rokovaní / stretnutí, používaním sociálnych sietí,
— útokov formou sociálneho inžinierstva,
— rozpoznania bezpečnostného incidentu a správnej reakcie na incident,
— zmeny vyžiadané zmenou príslušných právnych aktov, metodických usmernení, štandardov alebo súvisiacich relevantných dokumentov.

Aktualizáciou sa na účely tohto dokumentu myslí taká aktualizácia vzdelávacích materiálov, ktorá zahrňuje ich primerané prepracovanie, zohľadnenie aktuálneho stavu, ako aj doplnenie vzdelávacích materiálov o nové skutočnosti v kontexte aktuálneho vývoja stavu kybernetickej a informačnej bezpečnosti.

4. Legislatívne požiadavky

Vzdelávacie materiály špecifikované v kapitolách 2.2 a 3.1 tohto dokumentu musia primerane zohľadňovať legislatívny rámec pre oblasť kybernetickej bezpečnosti v Slovenskej republike, ktorý je daný najmä nasledovnými právnymi aktami a ďalšími súvisiacimi dokumentami:

a) Právne akty sekundárneho práva Európskej únie

- Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Smernica NIS) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky,
- Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu,
- Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) – aj v kontexte jej transpozície do právneho poriadku Slovenskej republiky,

b) Všeobecne záväzné právne predpisy právneho poriadku Slovenskej republiky
   - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
   - Vyhláška 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,
   - Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a doplnení niektorých zákonov v znení neskorších predpisov,
   - Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
   - Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
   - Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
   - Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
   - Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti,
   - Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov,
   - Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov,
   - Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov,
   - Zákon č. 185/2015 Z. z. Autorský zákon
   - Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti,
   - Vyhláška č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov

c) Ostatné relevantné akty a dokumenty

- medzinárodné normy rady ISO/IEC 27000 „Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti“ alebo iný obdobný bezpečnostný rámec, spolu s jeho premapovaním na normy rady ISO/IEC 27000.
- Záväzné usmernenie NIKA v súvislosti s informovaním, komunikáciou a viditeľnosťou opatrení Plánu obnovy a odolnosti SR (https://www.planobnovy.sk/realizacia/dokumenty/ , časť Vizibilita);

Vzdelávacie materiály špecifikované v kapitolách 2.2 a 3.1 tohto dokumentu musia primerane zohľadňovať legislatívny rámec pre oblasť ochrany osobných údajov v Slovenskej republike, ktorý je daný najmä nasledovnými právnymi aktami:

a) Právne akty sekundárneho práva Európskej únie
   - Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov),
   - Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky
b) Všeobecne záväzné právne predpisy právneho poriadku Slovenskej republiky
   - zákon č. 18/2018 Z. z. o ochrane osobných údajov a o doplnení niektorých zákonov v znení neskorších predpisov,
   - zákon č. 452/2021 Z. z. o elektronických komunikáciách zákonov v znení neskorších predpisov.

5. Harmonogram zákazky

Zákazka bude členená do nasledovných hlavných aktivít:

- vytvorenie špecifikácie jednotlivých modulov v zmysle kap. 2.2.3.1.1 a kap. 2.2.3.1.2 (moduly č. 1 až č. 6) vzdelávacích materiálov určených na schválenie zo strany verejného obstarávateľa – po ich schválení zo strany verejného obstarávateľa úspešný uchádzač vytvorí obsah vzdelávacích materiálov v zmysle odrážky nižšie,
- vytvorenie vzdelávacích materiálov úspešným uchádzačom, na základe špecifikácií, uvedených v tomto dokumente v zmysle kapitoly 2 (Celkový opis predmetu zákazky) a kapitoly 3 (Požiadavky na vzdelávacie moduly) tohto dokumentu,
- dodanie vzdelávacích materiálov úspešným uchádzačom, v podobe a spôsobom v zmysle kapitoly 2 (Celkový opis predmetu zákazky) a kapitoly 3 (Požiadavky na vzdelávacie moduly) tohto dokumentu,
- akceptácia dodaných vzdelávacích materiálov zo strany verejného obstarávateľa, a
- pravidelná aktualizácia dodaných a odsúhlasených vzdelávacích materiálov úspešným uchádzačom počas doby trvania diela v podobe a spôsobom v zmysle kapitoly 3.3 (Periodická aktualizácia dodaných vzdelávacích materiálov) tohto dokumentu.

	Verzia	**Termín dodania**
1	Prvá fáza v súlade s kap. 2.2.3.1.1	3 mesiace odo dňa účinnosti zmluvy
2	Druhá fáza v súlade s kap. 2.2.3.1.2	6 mesiacov odo dňa účinnosti zmluvy

3	Prvá verzia vzdelávacích materiálov vrátane Ďalšieho audiovizuálneho obsahu	9 mesiacov odo dňa účinnosti zmluvy
4	Druhá verzia vzdelávacích materiálov	13 mesiacov odo dňa účinnosti zmluvy
5	Tretia verzia vzdelávacích materiálov	17 mesiacov odo dňa účinnosti zmluvy
6	Štvrtá verzia vzdelávacích materiálov	21 mesiacov odo dňa účinnosti zmluvy
7	Piata verzia vzdelávacích materiálov	25 mesiacov odo dňa účinnosti zmluvy

Každá aktualizácia musí byť dodaná úspešným uchádzačom vždy najneskôr do 1 kalendárneho mesiaca od uplynutia príslušnej vyššie špecifikovanej lehoty dodania.

6. Podmienky účasti

6.1 Požiadavky na kľúčových expertov

Uchádzač musí v ponuke predložiť doklady, ktorými preukazuje svoju technickú alebo odbornú spôsobilosť v zmysle § 34 ods. 1 písm. g) ZVO:

Verejný obstarávateľ požaduje údaje o vzdelaní a odbornej praxe alebo o odbornej kvalifikácii nasledujúcich osôb určených na plnenie zmluvy, pričom tieto osoby musia spĺňať nasledujúce minimálne požiadavky.

Minimálna požadovaná úroveň štandardov:

- Uchádzač musí disponovať dvoma kľúčovými expertmi za každú oblasť, pričom požadovaných expertov preukáže spôsobom, že na každého uvedeného experta bude prislúchať jedna osoba. Kľúčový odborník č. 1 – Tvorca vzdelávacích materiálov
- Kľúčový odborník č. 2 – Odborný garant za KB

Kľúčový odborník č. 1 – Tvorca vzdelávacích materiálov

- Minimálne ukončené vysokoškolské vzdelanie II. stupňa, preukazuje sa prostredníctvom kópie VŠ diplomu
- Minimálne 3 roky odbornej praxe zameranej na tvorbu vzdelávacích materiálov v oblasti kybernetickej **alebo** informačnej bezpečnosti **alebo** v inej oblasti IT vzdelávania. (preukazuje sa životopisom)
- V rámci požadovaného obdobia odbornej praxe musí uchádzač zároveň preukázať jednu skúsenosť v odbore tvorby vzdelávacích materiálov vo forme dištančného vzdelávania **alebo** prípravy obsahov pre online vzdelávanie v oblasti kybernetickej **alebo** informačnej bezpečnosti. (preukazuje sa životopisom)

Kľúčový odborník č. 2 – Odborný garant za KB

- Minimálne ukončené vysokoškolské vzdelanie II. stupňa, preukazuje sa prostredníctvom kópie VŠ diplomu
- Minimálne 3 roky odbornej praxe zameranej na tvorbu materiálov v oblasti kybernetickej **alebo** informačnej bezpečnosti **alebo** tvorba iných materiálov v oblasti informačno-komunikačných technológií. (preukazuje sa životopisom)

- Získaný platný certifikát audítora KB v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, podľa NBÚ certifikačnej schémy overovania odbornej spôsobilosti audítora kybernetickej bezpečnosti **alebo** získaný platný certifikát manažéra kybernetickej bezpečnosti v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, podľa NBÚ certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti (preukazuje sa certifikátom)
- minimálne2 ročná prax na pozícii certifikovaného audítora kybernetickej bezpečnosti **alebo** minimálne 2 ročná prax na pozícii certifikovaného manažéra kybernetickej bezpečnosti

Uchádzač preukáže odbornú spôsobilosť vyššie uvedených osôb predložením profesijných životopisov za každú osobu v nasledovnej štruktúre:

- meno a priezvisko;
- názov a sídlo objednávateľa, resp. zamestnávateľa;
- čas plnenia zmluvy (od - do: mesiac a rok);
- stručný popis projektov na príslušnej pozícii, resp. rozsah činností, ktoré príslušná osoba zabezpečovala;
- tel. číslo a meno zamestnanca objednávateľa alebo zamestnávateľa, u ktorého si možno overiť tieto údaje;
- vlastnoručný podpis osoby.