Prilog br. 1 – Tehnička specifikacija

TEHNIČKA SPECIFIKACIJA ZA PRUŽANJE USLUGE OBNAŠANJA FUNKCIJE VODITELJA INFORMACIJSKE SIGURNOSTI (CISO)

Sadržaj

1. TEHNIČKA SPECIFIKACIJA

1.1. PREDMET NABAVE

Predmet ove jednostavne nabave je pružanje usluge obnašanja funkcije Voditelja informacijske sigurnosti (CISO) za potrebe Naručitelja u razdoblju od 12 mjeseci.

Usluga obuhvaća kontinuirano savjetovanje, koordinaciju i operativnu podršku u području upravljanja informacijskom i kibernetičkom sigurnošću, uključujući inicijalno uvođenje u posao te provedbu aktivnosti definiranih operativnim godišnjim planom.

Usluga se provodi sukladno potrebama Naručitelja i u koordinaciji s odgovornim osobama Naručitelja.

1.2. TEHNIČKA SPECIFIKACIJA I OPSEG USLUGE

1.2.1. Uvodni angažman i preuzimanje funkcije

Na početku ugovornog razdoblja odabrani ponuditelj provodi aktivnosti upoznavanja s organizacijskim, poslovnim i tehnološkim okruženjem Naručitelja radi učinkovitog preuzimanja funkcije Voditelja informacijske sigurnosti.

Aktivnosti uključuju:

- održavanje uvodnih sastanaka s ključnim dionicima Naručitelja,
- pregled postojećeg sustava upravljanja informacijskom sigurnošću (ISMS), što uključuje politike, procedure, pravilnike i drugu relevantnu dokumentaciju,
- pregled informacijske i komunikacijske infrastrukture te ključnih informacijskih sustava,
- analizu postojećih tehničkih i organizacijskih informacijskih i kibernetičkih sigurnosnih mjera,
- identifikaciju specifičnih regulatornih, zakonskih i ugovornih zahtjeva relevantnih za Naručitelja,
- prikupljanje informacija o ključnim dobavljačima i trećim stranama povezanim s informacijskom sigurnošću.

Naručitelj procjenjuje navedeni angažman na 3 čovjek-dana.

1.2.2. Kontinuirano obnašanje funkcije Voditelja informacijske sigurnosti

U okviru ugovorenog razdoblja ponuditelj kontinuirano obavlja poslove Voditelja informacijske sigurnosti, što može uključivati:

- koordinaciju aktivnosti informacijske i kibernetičke sigurnosti,
- izradu, definiranje, održavanje i unapređenje internih akata i dokumentacije iz područja sigurnosti,
- redovito izvještavanje Uprave o stanju informacijske sigurnosti i informacijskog sustava Naručitelja,
- uspostavu i provedbu procesa upravljanja sigurnosnim rizicima Naručitelja sukladno uspostavljenim metodologijama,
- analizu postojećih sigurnosnih mjera unutar informacijskog sustava Naručitelja,
- predlaganje i planiranje sigurnosnih mjera i kontrola koje proizlaze iz procjene rizika,

- nadzor implementacije mjera i kontrola u skladu s najboljim praksama i sigurnosnim standardima,
- planiranje i provođenje programa za sigurnosno osvješćivanje svih zaposlenika Naručitelja,
- sudjelovanje u radu tijela odgovornih za kontinuitet poslovanja Naručitelja,
- sudjelovanje na projektima iz područja informacijske sigurnosti te sigurnosti informacijskog sustava,
- unaprjeđenje postojećih i uvođenje novih procesa vezanih uz informacijsku sigurnost,
- suradnju s vanjskim partnerima Naručitelja u cilju dodatnog podizanja razine sigurnosti informacijskog sustava Naručitelja,
- aktivnu suradnju s organizacijskom jedinicom za informacijske tehnologije, organizacijskom jedinicom za internu reviziju te ostalim organizacijskim jedinicama Naručitelja,
- suradnju s regulatorima i ostalim vanjskim revizijama Naručitelja,
- sudjelovanje u radu tijela odgovornih za upravljanje informacijskom sigurnošću Naručitelja.

Ponuditelj Naručitelju dostavlja mjesečna izvješća o provedenim aktivnostima, utrošenom vremenu i planu daljnjih aktivnosti.

Naručitelj navedeni angažman traži na bazi 3 čovjek-dana/mjesečno.

1.2.3. Operativni plan aktivnosti

1.2.3.1. GAP analiza usklađenosti s propisima o kibernetičkoj sigurnosti

Aktivnost uključuje procjenu trenutačne razine usklađenosti Naručitelja s primjenjivim propisima i najboljim praksama kibernetičke sigurnosti te obuhvaća:

- pripremne aktivnosti i prikupljanje podataka,
- procjena postojeće razine usklađenosti,
- izrada izvještaja s nalazima i preporukama.

Isporuka:

- izvještaj o procjeni trenutačne razine usklađenosti.

1.2.3.2. Uspostava dokumentacijskog okvira za upravljanje kibernetičkom sigurnošću

Izrada i uspostava temeljne dokumentacije upravljanja informacijskom i kibernetičkom sigurnošću, uključujući:

- krovnu politiku kibernetičke sigurnosti uključujući uloge i odgovornosti za kibernetičku sigurnost unutar Grupe,
- definiranje metrika za praćenje sigurnosti,
- pravilnik o upravljanju informacijskom imovinom,
- pravilnik o upravljanju korisničkim i privilegiranim pristupima informacijskom sustavu,
- pravilnik o prihvatljivom korištenju informacijskih sustava,
- pravilnik o upravljanju log zapisima i sigurnosnim događajima,
- pravilnik o upravljanju ranjivostima i sigurnosnim zakrpama,
- pravilnik o zaštiti od zlonamjernog koda,
- pravilnik o sigurnosti računalne mreže i mrežne infrastrukture,
- pravilnik o upravljanju fizičkom sigurnošću,
- postupke upravljanja dobavljačima i trećim stranama,
- pravilnik o zaštiti podataka u prijenosu i pohrani,
- pravilnik o upravljanju sigurnosnim incidentima.

Isporuka:

- cjeloviti dokumentacijski okvir koji uključuje navedene dokumente unutar ove aktivnosti.

1.2.3.3. Upravljanje kontinuitetom poslovanja

Aktivnosti uključuju:

- identifikaciju kritičnih poslovnih procesa Naručitelja,
- provedbu analize utjecaja na poslovanje (engl. Business Impact Analysis - BIA) s identificiranim zahtijevanim vremenima oporavka (RTO/RPO),
- izradu politike kontinuiteta poslovanja i upravljanja kibernetičkim krizama,
- izrada okvira plana upravljanja kontinuitetom poslovanja (engl. Business Continuity Plan - BCP).

Isporuka:

- metodologija provođenja BIA analize,
- BIA izvještaj,
- politika kontinuiteta poslovanja i upravljanja kibernetičkim krizama,
- plan kontinuiteta poslovanja.

1.2.3.4. Procjena rizika informacijske sigurnosti

Aktivnosti uključuju:

- uspostavu metodologije upravljanja rizicima i definiranje uloga i odgovornosti za upravljanje rizicima informacijskog sustava,
- identifikaciju i klasifikaciju kritične imovine obuhvaćene procjenom rizika,
- identifikacija rizika za prethodno identificiranu imovinu,
- izrada plana za tretiranje identificiranih rizika,
- predlaganje tehničkih i organizacijskih mjera za umanjivanje identificiranih rizika,
- izrada izvještaja o provedenoj procjeni rizika (registar rizika),

Isporuka:

- identifikacija i procjena prijetnji, ranjivosti i rizika za ključne informacijske resurse,
- analiza postojećih kontrola i prijedlog dodatnih mjera za smanjenje rizika,
- izvještaj o providnoj procjeni rizika s prijedlogom mjera za umanjenje.

1.2.3.5. Provjera ranjivosti informacijskog sustava

Aktivnosti uključuju:

- prikupljanje podataka i upoznavanje s informacijskim sustavom Naručitelja,
- konfiguraciju alata za provjeru ranjivosti informacijskog sustava Naručitelja,
- provedbu provjere ranjivosti informacijskog sustava Naručitelja,
- izradu završnog izvještaja.

Isporuka:

- sažetak za rukovoditelje Naručitelja,
- opis opsega i ciljeva provedene provjere ranjivosti,
- izvještaj s identificiranim ranjivostima informacijskog sustava Naručitelja.

1.2.3.6. Program podizanja svijesti zaposlenika

Uspostava i provedba kontinuiranog programa podizanja svijesti o informacijskoj sigurnosti kroz izradu mjesečnih edukativnih materijala.

Isporuka:

- jedan (1) letak (newsletter) mjesečno za period od ukupno 12 mjeseci.

1.2.4. Metodologija i standardi

Usluga se mora provoditi sukladno važećim zakonima, propisima i međunarodno priznatim standardima i najboljim praksama, uključujući:

- Zakon o kibernetičkoj sigurnosti (NN 14/24 od 15.02.2024. godine),
- Uredbu o kibernetičkoj sigurnosti (NN 135/2024 od 21.11.2024. godine).

1.2.5. Obveze Naručitelja

Naručitelj će tijekom trajanja ugovora:

- osigurati organizacijsko pozicioniranje funkcije Voditelja informacijske sigurnosti s mogućnošću izravne komunikacije s Upravom,
- imenovati kontakt osobu za koordinaciju aktivnosti,
- komunikacija s funkcijom Voditelja informacijskog sustava
- komunikacija s drugim organizacijskim jedinicama Naručitelja, a posebno s organizacijskim jedinicama odgovornim za ljudske resurse, pravne poslove i internu reviziju
- omogućiti pristup potrebnoj dokumentaciji i svim organizacijskim resursima Naručitelja u skladu s potrebom obnašanja funkcije Voditelja informacijske sigurnosti,
- prema potrebi osigurati radno mjesto za djelatnika Ponuditelja prilikom posjete i obnašanja uloge Voditelja informacijske sigurnosti na lokaciji Naručitelja.