SPECIJALNA BOLNICA ZA MEDICINSKU
REHABILITACIJU KRAPINSKE TOPLICE
Gajeva 2, 49217 Krapinske Toplice
Tel.: 049 383 100
Faks: 049 232 140
E – mail: info@sbkt.hr
www.sbkt.hr

Prilog 4

Tehničke specifikacije

Predmet nabave: Usluga usklađenja s NIS2 Direktivom prema Zakonu o kibernetičkoj sigurnosti i podzakonskim propisima uz korištenje usluge vanjskog stručnjaka za kibernetičku sigurnost, evidencijski broj nabave: 05-42/37-2026

Predmet nabave su usluge pregleda stanja kibernetičke sigurnosti naručitelja Specijalne bolnice za medicinsku rehabilitaciju Krapinske Toplice i njeno usklađivanje s NIS2 Direktivom, Zakonom o kibernetičkoj sigurnosti i podzakonskim propisima, uzevši u obzir već prije izrađenu analizu trenutnog stanja usklađenosti Specijalne bolnice za medicinsku rehabilitaciju Krapinske Toplice s NIS 2 Direktivom, a što uključuje preporuke za usklađenje prema prioritetima i plan implementacije preporuka, analizu rizika s ciljem podizanja zrelosti relevantnih kritičnih procesa, infrastrukture i sustava Specijalne bolnice za medicinsku rehabilitaciju Krapinske Toplice, izradu potrebne dokumentacije za upravljanje kibernetičkom sigurnosti naručitelja prema slijedećoj usluzi:

➢ Pregled stanja kibernetičke sigurnosti i povećanje usklađenosti s NIS2 Direktivom, Zakonom, i podzakonskim propisima.

Povećanje usklađenosti s NIS2 Direktivom uključuje niz aktivnosti i izradu dokumenata za postizanje SREDNJE razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42., stavka 2 i Priloga II Uredbe, sve sukladno kategorizaciji naručitelja kao VAŽNOG subjekta prema Nacionalnom centru za kibernetičku sigurnost.

Analize trebaju obuhvatiti sve relevantne kritične procese, infrastrukturu i sustave naručitelja.

Usluga se mora izvršiti po fazama. Odabrani ponuditelj će nakon potpisa ugovora naručitelju dostaviti terminski plan s određenim fazama projekta i rokovima u roku od 8 dana od potpisa ugovora.

Rok isporuke usluga: **01.04.2026. godine**

U okviru ovoga predmeta nabave potrebno je izvršiti:

01 Priprema za procjenu stanja kibernetičke sigurnosti

- Inicijalni sastanak s upravom društva te prezentacija projekta,
- Evaluacija postojećih mjera usklađenosti s NIS2 Direktivom, odnosno Zakonom o kibernetičkoj sigurnosti, Uredbom i drugim podzakonskim aktima
- Prikupljanje raspoložive dokumentacije (interne procedure i pravila, organizacijski dijagrami, podatkovni i procesni dijagrama, inventarni popisi, itd.),
- Analiza i konsolidacija svih dobivenih dokumenata,
- GAP analiza s izradom strukturiranog izvješća o nedostacima,

- Izrada projektnog dokumenta (opisuje ciljeve projekta, standarde i metodologije te faze projekta i rokove).

02 Identifikacija svih IT/OT sustava

- Izrada dijagrama arhitekture sustava,
- Izrada mrežnih dijagrama,
- Izrada dokumenta arhitekture sustava.

03 Procjena rizika

- Radionice s ključnim sudionicima poslovnih procesa i kibernetičke sigurnosti u cilju utvrđivanja glavnih prijetnji, posljedica te utjecaja na poslovanje tvrtke,
- Provođenje sveobuhvatne procjene rizika kako bi se identificirali nedostavi, kritični sustavi i područja za poboljšanje i ažuriranje Registra rizika kibernetičke sigurnosti naručitelja
- Konsolidacija dobivenih podataka te izrada dokumenta procjene rizika.

04 Detekcija ranjivosti na postojećoj infrastrukturi

- Izvođenje detekcije ranjivosti (eng. vulnerability testing) na postojećoj mrežnoj i serverskoj infrastrukturi,
- Konsolidacija rezultata detekcije ranjivosti te izrada preporuka,
- Davanje jasnih i provedivih preporuka za poboljšanje usklađenosti poslovanja naručitelja s NIS2 Direktivom, Zakonom o kibernetičkoj sigurnosti i upravljanje identificiranim rizicima kibernetičke sigurnosti, s ciljem unaprjeđenja procesa identifikacije kritične imovine i smanjenja identificiranih rizika

05 Izrada plana za tretiranje rizika

- Konsolidacija rezultata dobivenih tijekom procjene rizika te detekcije ranjivosti.
- Definiranje tehničkih, operativnih i organizacijskih mjera za upravljanje rizicima.
- Izrada akcijskog plana za implementaciju tehničkih, operativnih i organizacijskih mjera u cilju mitigacije rizika.

06 Implementacija akcijskog plana za tretiranje rizika

- Implementacija tehničkih mjera sukladno akcijskom planu tretiranja rizika
- Tehničke sigurnosne mjere obuhvaćaju implementaciju tehnologija, alata i mehanizama koji štite sustave od kibernetičkih prijetnji.
    - Može obuhvaćati aktivnosti kao što su implementacija antivirusnog rješenja, implementacija vatrozida nove generacije, implementacija posebnih GPO politika, implementacija kriptiranja diskova računala, promjena konfiguracije na mrežnoj infrastrukturi, itd.
- Implementacija operativnih mjera sukladno akcijskom planu tretiranja rizika
    - Operativne sigurnosne mjere obuhvaćaju postavljanje politika, procedura i praksi koje se primjenjuju u svakodnevnom radu kako bi se osigurala sigurnost informacijskih sustava.
    - Može obuhvaćati aktivnosti kao što su izrada raznih dokumenata i procedura informacijskog sustava, kreiranje BCP politike, definiranje sigurnosne politike,

definiranje pravila za upravljanje lozinkama, pravila dodjele prava pristupa povjerljivim podacima, načine korištenja IT resursa, itd.

- Implementacija organizacijskih mjera sukladno akcijskom planu tretiranja rizika
    - Organizacijske sigurnosne mjere obuhvaćaju uspostavljanje kulture sigurnosti unutar organizacije i angažiranje zaposlenika u održavanju sigurnosti informacijskih sustava.
    - Može obuhvaćati aktivnosti kao što su osiguravanje obuke i svijesti o sigurnosti za zaposlenike, uspostavljanje odgovornosti za sigurnost informacija, kao i usklađivanje s regulatornim zahtjevima i standardima sigurnosti. Konkretna implementacija tehničkih mjera kao i nabava potrebnog hardware-a, software-a i licenci je u nadležnosti naručitelja (ako iste ne postoje mogu se preporučiti i uvesti na preporuku vanjskog stručnjaka za sigurnost).

07 Izrada dokumentacije sukladno ZKS-u

- Izrada dokumentacije naručitelja sukladno NIS2 Direktivi, Zakonu te Uredbi: Ažuriranje postojećih internih akata o kibernetičkoj sigurnosti i/ili izrada novih internih akata o kibernetičkoj sigurnosti, sve sukladno NIS 2 Direktivi, Zakonu i podzakonskim propisima.
- Izrada Izvješća o usklađenosti s NIS 2 Direktivom, Zakonom i podzakonskim propisima: Izrada detaljnog izvješća za naručitelja, s nalazima i predloženim mjerama.

08 Provedba samoprocjene kibernetičke sigurnosti s Izjavom o sukladnosti

- Izrada protokola za izvođenje samoprocjene kibernetičke sigurnosti.
- Pomoć internom osoblju prilikom izvođenja samoprocjene kibernetičke sigurnosti.
- Kreiranje izjave o sukladnosti.
- Kreiranje plana za ispravljanje pronađenih nesukladnosti te plana za ponovnu provedbu samoprocjene kibernetičke sigurnosti
- Ugovaratelj se obvezuje u roku od 6 mjeseci nakon implementacije stabilizacije mjera izvršiti periodičnu samoprocjenu.

Dodatni opis zahtjeva naručitelja vezano za isporuku predmeta nabave ((Revidirati u skladu sa zahtjevima ZSIS):

1. Revizija trenutnog okvira upravljanja (sažetak trenutnog okvira upravljanja i sigurnosnog stanja te procjenu rizika) sa analizom raskoraka (GAP ANALIZA odnosno identifikacija područja neusklađenosti i potrebnih poboljšanja)

2. Izrada i isporuka interne dokumentacije naručitelja sukladno NIS2 Direktivi, Zakonu o kibernetičkoj sigurnosti i drugim podzakonskim propisima, a ne ograničavajući se samo na sljedeće:

➢ Strateški akt sigurnosne politike,

➢ Pomoć pri uspostavi i dokumentiranju uloge i odgovornosti za kibernetičku sigurnost naručitelja

➢ Metodologija za analizu, procjenu i obradu rizika

➢ Plan obrade rizika,

➢ Izrada Procjene i obrade rizika s identificiranim kibernetičkim prijetnjama i rizicima, predloženim mjerama za otklanjanje istih (Registar identificiranih rizika) te preporuke za poboljšanje,

➢ Izvještaj o procjeni rizika,

➢ Izvještaj o primjenjivosti sigurnosnih mjera,

➢ Uspostaviti inventar kritične programske i sklopovske imovine,

➢ Razviti i dokumentirati pravila sigurnosti ljudskih potencijala,

➢ Razviti i dokumentirati pravila osnovne prakse kibernetičke sigurnosti,

➢ Razviti i dokumentirati Politiku kontrole pristupa mrežnom i informacijskom sustavu,

➢ Razviti i dokumentirati pravila sigurnosti lanaca opskrbe mrežnih i informacijskih sustava,

➢ Uspostaviti registar izravnih dobavljača i pružatelja IKT usluga,

➢ Uspostaviti i dokumentirati konfiguraciju mrežnih i informacijskih sustava uključujući sigurnosne konfiguracijske postavke za svu sklopovsku i programsku imovinu, kao i za sve korištene vanjske usluge i mreže.

➢ Propisati kontrolne procedure za upravljanje promjenama u okviru održavanja mrežnih i informacijskih sustava,

➢ Razviti i dokumentirati pravila primjene kriptografije u subjektu (kriptografske politike i procedure),

➢ Razviti i dokumentirati postupke i procedure za postupanje s incidentima,

➢ Razviti politike kontinuiteta poslovanja i upravljanja kibernetičkim krizama. Provesti analizu utjecaja incidenata na poslovanje, uspostaviti procese za upravljanje kibernetičkim krizama te razviti detaljne planove za oporavak od katastrofa i kontinuitet poslovanja,

➢ Politika fizičke sigurnosti informacijskih sustava i

➢ Izrada izvještaja za samoprocjenu.

3. Završno Izvješće o usklađenosti s NIS 2 Direktivom, Zakonom i Uredbom

Sva dokumentacija koju odabrani ponuditelj treba dostaviti odgovornoj osobi naručitelja, mora biti isporučena u obliku dokumenta u elektroničkom obliku na hrvatskom jeziku osobi koju ugovorom odredi naručitelj, a završno Izvješće o usklađenosti mora biti potpisano i ovjereno od strane odabranog ponuditelja te dostavljeno u 3 primjerka na adresu sjedišta Naručitelja.

Prilikom predaje dokumentacije ugovorne strane sastavljaju i potpisuju Zapisnik o uredno izvršenim ugovornim obvezama.