



TEHNIČKA SPECIFIKACIJA USLUGE PREGLEDA KIBERNETIČKE SIGURNOSTI ZA PODIZANJE SUKLADNOSTI S NIS2 DIREKTIVOM

I EDUKACIJE DJELATNIKA PLOVPUTA D.O.O.

1. Uvod

Projekt „Cyber safety in Croatian maritime transport sector – acronim CYSCROMS“, broj projekta: 101127567

EU Program: Digital Europe (Digitalna Europa)

Digitalna Europa je program Europske unije koji je uspostavljen u okviru programskog razdoblja 2021.-2027. kako bi podupirao projekte vezane uz upotrebu umjetne inteligencije, superračunarstva, napredne digitalne vještine, osiguravanje široke upotrebe digitalnih tehnologija u cijelom gospodarstvu i društvu te vezane uz područje kibernetičke sigurnosti. Kibernetička sigurnost u središtu je Strategije Europske unije za digitalno desetljeće te zbog toga Europska unija u sklopu programa Digitalna Europa u trenutnom programskom razdoblju dodjeljuje sredstva organizacijama za jačanje njihove kibernetičke zrelosti i otpornosti.

Predmet nabave nabavlja se u sklopu Projekta kojim je ostvareno pravo na EU sufinanciranje iz programa Digitalna Europa na temelju Poziva za dodjelu bespovratnih sredstava pod nazivom „Podrška implementaciji NIS Direktive i nacionalnih strategija kibernetičke sigurnosti“ (Supporting The NIS Directive Implementation And National Cybersecurity Strategies), oznake DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE. Poziv je bio otvoren za projekte kojima se poticalo usklađivanje operatora ključnih usluga s NIS Direktivom (EU) 2016/1148, Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18) te Uredbom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18), odnosno uspostava procesa i procedura propisanih gore navedenom zakonodavnom osnovom koja je obvezujuća za sve operatore ključnih usluga.

Ministarstvo mora, prometa i infrastrukture (u nastavku: MMPI) kao nadležno sektorsko tijelo za promet u Republici Hrvatskoj prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18) formiralo je konzorcij operatora ključnih usluga u pomorskom prometu u svrhu prijave na navedeni Poziv te je projekt „Cyber safety in Croatian maritime transport sector – acronim CYSCROMS“ („Kibernetička sigurnost u hrvatskom sektoru pomorskog prometa“, u nastavku: Projekt) prepoznat kao strateški važan iskorak za pomorski promet na nacionalnoj razini.

Projekt predstavlja priliku ne samo za usklađivanje sa novom Direktivom (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (u nastavku: NIS 2 Direktiva)¹ i novim Zakonom o kibernetičkoj sigurnosti (NN 14/24, u nastavku: Zakon)², Uredbom o kibernetičkoj sigurnosti (NN 135/24, u nastavku: Uredba) i drugim

¹ NIS 2 Direktiva (EU) 2022/2555: L_2022333HR.01008001.xml (europa.eu)

² Zakon o kibernetičkoj sigurnosti (NN 14/24):
https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html



podzakonskim propisima, već i za podizanje opće razine kibernetičke zrelosti pomorskog prometa i osiguranje neometanog pružanja usluga u pomorskom prometu.

2. Opseg usluge

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 Plovput d.o.o. (nadalje: **Naručitelj** ili **Plovput**) kao VAŽNOG subjekta prema Nacionalnom centru za kibernetičku sigurnost.

Predmet nabave su usluge pregleda stanja kibernetičke sigurnosti naručitelja Plovput d.o.o. i njegovo usklađivanje s NIS2 Direktivom, Zakonom i podzakonskim propisima, provođenjem analize trenutne razine usklađenosti Plovputa s NIS 2 Direktivom što uključuje preporuke za usklađenje prema prioritetima i plan implementacije preporuka, analizu rizika s ciljem podizanja zrelosti relevantnih kritičnih procesa, infrastrukture i sustava Plovputa, izradu potrebne dokumentacije za upravljanje kibernetičkom sigurnosti te edukacijom djelatnika **Naručitelja** prema slijedećim kategorijama usluga:

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

USLUGA II. Edukacija djelatnika Plovputa s ciljem podizanja svijesti o kibernetičkoj sigurnosti.

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

Plovput je za opseg ključnih sustava proveo usklađivanje sa NIS1 Direktivom za koje ima definirane procese, Registar rizika (*Procjena i obrada rizika*) i druge dokumente, uključivo i dokumentaciju za provedeni unutarnji i vanjski penetracijski test koji je klasificiran kao tajni dokument.

Naručitelj će odabranom ponuditelju po potpisu ugovora ustupiti dostupnu dokumentaciju s naglaskom na onu koja uređuje područje informacijske i kibernetičke sigurnosti te procese nastale iz prethodnog usklađivanja s NIS1 zahtjevima.

2.1 USLUGA I.: PREGLED STANJA KIBERNETIČKE SIGURNOSTI I POVEĆANJE USKLAĐENOSTI S NIS2 DIREKTIVOM, ZAKONOM I PODZAKONSKIM PROPISIMA

U okviru ove usluge I. odabrani ponuditelj treba izvršiti:

- 1. Procjenu trenutnog okvira upravljanja informacijskom sigurnošću s analizom raskoraka:** Evaluaciju postojećih mjera usklađenosti s NIS2 Direktivom, odnosno sa Zakonom, Uredbom i drugim podzakonskim aktima koji iz njega proizlaze, te analiza raskoraka (GAP analiza) s izradom strukturiranog izvješća o nedostacima
- 2. Procjenu rizika:** Provođenje sveobuhvatne procjene rizika kako bi se identificirali nedostaci, kritični sustavi i područja za poboljšanje i ažuriranje Registra rizika kibernetičke sigurnosti Plovputa
- 3. Preporuke za poboljšanje:** Davanje jasnih i provedivih preporuka za poboljšanje usklađenosti poslovanja Plovputa s NIS 2 Direktivom, Zakonom te podzakonskim aktima i upravljanje identificiranim rizicima kibernetičke sigurnosti, s ciljem unaprjeđenja procesa identifikacije kritične imovine i smanjenja identificiranih rizika;



4. **Izradu dokumentacije Plovputa 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.
5. **Izradu Izvješća o usklađenosti s NIS 2 Direktivom, Zakonom i podzakonskim propisima:** Izrada detaljnog izvješća za Plovput, s nalazima i predloženim mjerama iz stavki 1. do 4.

2.1.1 Isporuke unutar usluge I. : (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 Plovputa sukladno NIS2 Direktivi, Zakonu 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 Plovputa,
 - 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*

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

Sva dokumentacija koju odabrani ponuditelj treba dostaviti odgovornoj osobi Naručitelja u okviru točke 2.1.1.1., mora biti isporučena u obliku dokumenta u elektroničkom obliku na hrvatskom jeziku



osobi koju ugovorom odredi Naručitelj, a završno Izvješće o usklađenosti (sa sažetkom na engleskom jeziku) mora biti potpisano i ovjereno od strane odabranog ponuditelja te dostavljeno u 3 primjerka na adresu sjedišta Naručitelja.

2.1.2 Rok i mjesto izvršenja usluge I.

Rok izvršenja usluge je najviše 6 mjeseci od dana obostrano potpisanog ugovora, a predviđeni početak potpisa Ugovora je 30. rujna 2025. g.

Mjesto izvršenja usluge I. su lokacije Naručitelja i odabranog ponuditelja

2.2 USLUGA II.: EDUKACIJE DJELATNIKA PLOVPUTA

U okviru razvoja i provedbe programa podizanja svijesti o kibernetičkoj sigurnosti zaposlenika Plovputa, podizanje svijesti zaposlenika Plovputa o kibernetičkim ugrozama mora pratiti primjenjive zahtjeve Direktive, Zakona i podzakonskih propisa te ih se treba educirati o tome.

Cilj edukacije je osigurati svim zaposlenicima:

- detaljno razumijevanje NIS2 Direktive, Zakona i drugih podzakonskih propisa i njezinih implikacija na organizaciju Plovputa,
- upoznavanje s regulatornim zahtjevima, obvezama i postupcima usklađenja,
- upoznavanje i razumijevanje tehničkih i organizacijskih mjera za jačanje kibernetičke sigurnosti u Plovputu,
- odgovornosti Plovputa i zaposlenika glede kibernetičke sigurnosti
- praktične smjernice za kibernetičku sigurnost
- primjenu najbolje prakse u zaštiti ključne infrastrukture i poslovnih procesa Plovputa.

U okviru ove usluge odabrani ponuditelj treba:

1. Razviti program edukacije za kibernetičku sigurnost djelatnika Plovputa s ciljem podizanja svjesnosti i provjeru znanja
2. Educirati Upravu, zamjenike Uprave, direktore sektora, internog revizora, voditelja sustava upravljanja kvalitetom, i druge djelatnike po zahtjevu Naručitelja, o svim zahtjevima kibernetičke sigurnosti s naglaskom na upravljanje sustavom informacijskom sigurnošću, proces prijave incidenta i sankcije te kibernetičkim rizicima (in-house).
Edukacija će se fizički održati u prostorijama u Splitu, u vrijeme i na datum sukladno dogovoru s odabranim ponuditeljem koji je dužan pripremiti nužne prezentacije, tiskane materijale i testove za in-house edukaciju.
3. Omogućiti edukaciju i certificiranje 2 zaposlenika Naručitelja iz područja NIS 2 ili ISO 27001 ili CISO, a iz skupa ponuđenih certifikacija koje se odnose na kibernetičku sigurnost u domeni organizacijskog vođenja i upravljanja.
4. Educirati sve zaposlenike o osnovama kibernetičke sigurnosti (cca. 260), a kako je primjenjivo prema radnim mjestima Naručitelja.

Odabrani ponuditelj je dužan provesti on-line edukacijski program dostupan putem digitalne platforme (dostupne i preko mobilnih uređaja) uz interaktivne module, video lekcije i dodatne tiskane materijale za učenje. Edukacijski sustav mora biti razvijen u interaktivnom obliku (slike,



video, tekst...) na način da korisniku (polazniku programa) omogući edukaciju o kibernetičkoj sigurnosti na intuitivan i lako razumljiv način.

Edukacijski sustav mora sadržavati završnu provjeru znanja u obliku pitanja kojima se želi utvrditi programom obuhvaćena edukativna građa.

Po završnoj provjeri znanja (ispunjavanju upitnika), bez obzira na točnost odgovora, sustav korisniku generira Potvrdu u kojoj je navedeno ime i prezime polaznika (zaposlenika), navod kako je polaznik toga dana uspješno pohađao Program te izjavu (u fusnoti) kako Potvrda ne predstavlja uvjerenje koje bi imalo vrijednost stručne kvalifikacije (točan sadržaj i format Potvrde Naručitelj će usuglasiti s odabranim ponuditeljem).

Edukacijski sustav bilježi korištenje od strane pojedinog korisnika (datum zadnjeg korištenja, broj točnih odgovora na upitnik, datum generiranja Potvrde).

Edukacijski sustav mora biti usklađen s odredbama NIS2 Direktive (EU), odnosno odredbama Zakona i podzakonskih propisa.

5. Odabrani ponuditelj je dužan o svim edukacijama sačuvati log (povijest pristupa i logiranja) i po završetku edukacije isporučiti osobi odgovornoj za provedbu ugovora poimeničan dokaz o edukaciji radnika i postignutoj razini znanja, a sukladno zahtjevima Zakona i podzakonskim propisima;
6. Odabrani ponuditelj je dužan dostaviti osobi odgovornoj za provedbu ugovora završno Izvješće o provedenoj edukaciji, u tiskanom obliku na hrvatskom jeziku, sa sažetkom na engleskom jeziku, koje mora biti potpisano i ovjereno od strane odabranog ponuditelja te dostavljeno u 3 primjerka na adresu sjedišta Naručitelja.
7. Odabrani ponuditelj treba osigurati tehničku podršku tijekom trajanja on-line edukacije.

2.2.1 Isporuke unutar usluge II.:

- a) Program edukacija zaposlenika i provjere znanja
- b) Edukacija Uprave i menadžmenta (in house) – Split sjedište Plovputa
- c) Edukacija za ostale zaposlenike Plovputa (on-line), brošura za edukaciju, video lekcije
- d) Provjera znanja svih zaposlenika putem online ili tiskanog testa, upitnika, i slično
- e) Dostava zapisa o educiranim radnicima i provjeri znanja i završnog izvješća
- f) Tehnička podrška

2.2.2 Rok i mjesto izvršenja Usluge II.

Rok izvršenja usluge je najviše 6 mjeseci od dana obostrano potpisanog ugovora, a predviđeni početak potpisa Ugovora je 30. rujna 2025. g.

Mjesto izvršenja usluge II. su lokacije Naručitelja i odabranog ponuditelja

- Sjedište Plovputa d.o.o., Obala Lazareta 1, 21000 Split;
- On-line edukacije