

USLUGA EKSTERNALIZACIJE CISO FUNKCIJE

Opis predmeta nabave i uvjeti tehničke sposobnosti

PODACI O PREDMETU NABAVE

Opis predmeta nabave

Predmet nabave je eksteralizacija upravitelja informacijske sigurnosti uz alat koji će osigurati efikasnost provođenja CISO funkcije i kontinuitet.

Usluga vanjskog upravitelja informacijskom sigurnošću

Predmet ove nabave je usluga eksteraliziranog upravitelja informacijskom sigurnošću (eng. CISO) s ciljem uspostave, održavanja i unapređenja sustava upravljanja informacijskom sigurnošću (ISMS), upravljanja rizicima i kontinuitetom poslovanja te usklade s GDPR-om.

Trajanje usluge	1 (jedna) godina
Opseg usluge	36 radnih dana godišnje
Vrsta aktivnosti	Savjetodavne, upravljačke i nadzorne aktivnosti

Eksternalizirani upravitelj informacijskom sigurnošću treba djelovati kao strateški savjetnik upravi i ključna kontakt točka za pitanja informacijske sigurnosti.

Ključne odgovornosti i isporuke

- Definiranje, izrada i ažuriranje strategije informacijske sigurnosti usklađene s poslovnim ciljevima na godišnjoj razini
- Uspostava, izrada i održavanje politika i procedura upravljanja sigurnošću
- Upravljanje rizicima (identifikacija, procjena, tretman, praćenje) i izrada registra rizika s planom tretmana i statusima
- Savjetovanje u vezi usklađenosti s propisima (GDPR) i standardima (npr. ISO/IEC 27001)
- Sudjelovanje u planiranju i evaluaciji sigurnosnih kontrola i projekata
- Definiranje i nadzor sigurnosnih metrika (KPI/KRI) i izvještavanje upravi
- Izrada tehničko-organizacijskih mjera (TOM)
- Izrada / ažuriranje registra obrade osobnih podataka
- Izrada / ažuriranje Privacy by Design i Privacy by Default te svih ostalih ISMS dokumenata
- Podrška pri upravljanju incidentima (koordinacija, post-incident analiza)
- Izrada Business Continuity i Disaster Recovery plana
- Planiranje i izvještavanje vezano uz provođenje i koordinaciju internih procjena i priprema za audite
- Edukacija ključnih dionika (uprava, IT, poslovni korisnici) na razini svijesti i upravljanja
- Upravljanje odnosima s regulatorima i auditorima (po potrebi)
- Kvartalni izvještaji upravi (stanje sigurnosti, KPI/KRI, status inicijativa)
- Izvješća o incidentima i preporuke za poboljšanje

Alat za upravljanje rizicima i usklađenošću

Kako bi se osigurala efikasnost internih sigurnosnih/IT timova te eksternaliziranog upravitelja informacijskom sigurnošću i ujedno pojednostavnio proces usklađivanja i održavanja usklađenosti s GDPR-om (Općom uredbom o zaštiti osobnih podataka) i ostalim relevantnim standardima, u sklopu Usluge eksternaliziranog voditelja sigurnosti potrebno je isporučiti sustav za upravljanje rizicima i usklađenošću.

UVJETI TEHNIČKE I STRUČNE SPOSOBNOSTI

Stručnjaci za izvedbu usluge vanjskog upravitelja sigurnosti

Stručnjaci moraju posjedovati sljedeće certifikate ili jednakovrijedne dokumente:

Certifikat	Opis / Svrha
ISO 27001:2022 Lead Auditor (ISMS)	Auditi sustava upravljanja informacijskom sigurnošću (ISMS) u organizacijama, identifikacija rizika i nedostataka u zaštiti podataka
ISO 42001:2023 AI Management System Lead Auditor	Revizije sustava upravljanja umjetnom inteligencijom, ocjena usklađenosti s međunarodnim standardima i identifikacija rizika u implementaciji AI sustava
ISACA – CRISC (Certified in Risk and Information Systems Control)	Identifikacija, procjena i upravljanje IT rizicima te uspostava kontrole informacijskih sustava
CISA – Certified Information Systems Auditor	Revizija, nadzor i procjena informacijskih sustava, sigurnosnih kontrola i poslovnih procesa

S obzirom na kompleksnost usluge te važnost pravovremene i neometane komunikacije, svi navedeni stručnjaci moraju biti u mogućnosti pružati usluge u opsegu ove nabave na hrvatskom jeziku.

Ponuditelj treba priložiti popis stručnjaka i njihove životopise uz navođenje potrebnih važećih certifikata koje stručnjaci posjeduju. Također, ponuditelj treba priložiti i preslike navedenih certifikata.

Obrazloženje

Naručitelj traži navedene dokaze stručnosti kojima se dokazuje poznavanje metodologije rada koji se koriste pri pružanju usluge kod Naručitelja. Navedeni dokazi i broj traženih stručnjaka uz poznavanje navedenih metodologija rada i alata prema procjeni Naručitelja potvrđuju potrebnu razinu stručnosti stručnjaka zaduženih za izvršenje predmeta nabave, odnosno isti osigurava određenu razinu znanja, iskustva i vještine koje su potrebne za uredno izvršenje ugovora o javnoj nabavi.

Naručitelj traži raspolaganje s više od jednog stručnjaka u svrhu brze, kontinuirane i adekvatne podrške.

Norme osiguranja kvalitete ili norme upravljanja okolišem

Gospodarski subjekt mora potvrditi sukladnost sa sljedećim normama osiguranja kvalitete:

- **HRN ISO/IEC 27001** ili jednakovrijednoj normi – za sustav upravljanja informacijskom sigurnošću