**Obrazac 5.**

**Tehnička specifikacija**

 **predmeta nabave za točku 5.9. *Sustav za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka, zahtjevima i privolama ispitanika iz Projektnog zadatka***

Postupak nabave: **Nadogradnja informacijskog sustava**

Evidencijski broj:  **E-MV-16/2018/R1**

Ponuditelj: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 *(upisati naziv ponuditelja/zajednice gospodarskih subjekata)*

*Ako nije drugačije definirano, zahtjevi definirani Tehničkim specifikacijama predstavljaju minimalne funkcionalne i tehničke uvjete koje ponuđena programska rješenja moraju zadovoljavati.*

*Ponuđena programska rješenja moraju minimalno zadovoljiti sve funkcionalne i tehničke zahtjeve iz Tablice 3.* **Minimalne zahtijevane funkcionalne i tehničke specifikacije za točku 5.9. iz Projektnog zadatka**

*Ponuditelj OBAVEZNO POPUNJAVA stupac «UVJETI ISPUNJENI (Da/Ne)» te ukoliko odgovori „DA“ na taj se način obvezuje na nuđenje programskog rješenja i licenci koja minimalno ispunjava traženi tehnički uvjet. Ukoliko se prilikom pregleda utvrdi da je neki odgovor „NE“ ili uopće* nije odgovoreno, ponuda će biti odbijena.

*U stupcu «Bilješke, napomene, reference na tehničku dokumentaciju» ponuditelj upisuje bilješke, napomene vezano za ponuđeno programsko rješenje i licencu ili broj stranice u prospektu, katalogu ili brošuri proizvođača odnosno web stranicu proizvođača na kojoj je vidljiva specifikacija nuđenog proizvoda..*

*Stupac «Ocjena DA/NE» ponuditelj* ***NE POPUNJAVA****, s obzirom na to da je stupac predviđen za ocjene naručitelja.*

*Kako bi se ponuda smatrala valjanom, ponuđeni predmet nabave mora zadovoljiti sve što je traženo u obrascu* ***Tehničkih specifikacija.***

*U slučaju postojanja sumnje u istinitost podataka navedenih u ponuđenim tehničkim specifikacijama, naručitelj zadržava pravo provjere navedenih podataka bilo kojim prikladnim sredstvom / načinom (npr. provjerom podataka na internet stranicama proizvođača, distributera ili se može obratiti proizvođaču i sl.)*

|  |
| --- |
| **Tablica 3. Sustav za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka, zahtjevima i privolama ispitanika** |
| **Puni naziv ponuđenog sustava:** |
| **Proizvođač ponuđenog sustava:** |
| **Količina i originalni naziv ponuđenih licenci sa kataloškim brojem (P/N – product number):** |
| **Trajanje uključenog proizvođačkog jamstva na ponuđene licence:** |
| **Minimalne zahtijevane funkcionalne i tehničke specifikacije za točku 5.9. iz Projektnog zadatka**  | **UVJETI ISPUNJENI (Da/Ne)** | **Bilješke, napomene, refer****ence na tehničku dokumentaciju** | **OCJENA****DA/NE** |
| **Opći zahtjevi i arhitektura sustava** |  |
| Specijalizirano industrijski prepoznato programsko rješenje (softver) za upravljanje informacijskom imovinom, rizicima, bazom znanja, evidencijama osobnih podataka i privolama ispitanika |  |  |  |
| Rješenje mora uključivati licence za 1 sustav bez ograničenja na broj analitičara, korisnika, IT servisa, rizika niti drugih ograničenja |  |  |  |
| Informatičko/aplikativno programsko rješenje u obliku dvoslojne aplikacije: * Web aplikativni dio
* Podatkovni dio / baza podataka
 |  |  |  |
| MS SQL baza podataka (osigurava Naručitelj) |  |  |  |
| Podržani različiti web preglednici (Internet Explorer, Chrome, Firefox, Opera). |  |  |  |
| API sučelje |  |  |  |
| Podrška za različite korisničke uloge u sustavu. |  |  |  |
| Mogućnost da korisnici sami mijenjaju svoje zaporke. |  |  |  |
| Mogućnost postavljanja politike zaporki. |  |  |  |
| Sučelje lokalizirano na hrvatski jezik |  |  |  |
| Način rada jedinstven kroz cijeli sustav. |  |  |  |
| Podaci na svim ekranima su pretraživi po više kriterija (jednako, sadrži, počinje s, veće od, manje od, između i sl.) |  |  |  |
| Pojedine prikaze u sustavu je moguće ispisati u više poznatih formata (PDF, Word, Excel, slike). |  |  |  |
| **Upravljanje informacijskom imovinom i procjena rizika** |  |
| Kreiranje popisa informacijske imovine i vrednovanje. |  |  |  |
| Organizacija procjene rizika po projektima. |  |  |  |
| Praćenje povijesti vrednovanja rizika. |  |  |  |
| Automatsko kreiranje rizika iz baze znanja. |  |  |  |
| Automatski izračun rizika na temelju statusa implementiranih kontrola. |  |  |  |
| Grupno izračunavanje rizika.  |  |  |  |
| Kreiranje plana implementacije kontrola. |  |  |  |
| Definiranje odgovornosti za obradu rizika. |  |  |  |
| Veza sa sustavom unutarnjih kontrola. |  |  |  |
| Odabir kontrola iz baze znanja. |  |  |  |
| Izvještavanje o rizicima po procesima. |  |  |  |
| Mogućnost brzog vrednovanja rizika u „data sheet“ modu (ažuriranje kao u Excel tablici). |  |  |  |
| Distribucija procjene rizika na više korisnika. Korisnici mogu sami procjenjivati rizike za koje su odgovorni. |  |  |  |
| Podržan uvoz informacijske imovine iz Excela, CSV-a |  |  |  |
| **Baza znanja** |  |
| Baza znanja kontrola i njihovih veza s poznatim standardima (ISO 27001:2013, ISO 27002:2013, ISO 22301:2012, CobiT, NIST, GDPR). |  |  |  |
| Popis prijetnji i grupa imovine. Gotovi katalozi prijetnji i grupa imovine. |  |  |  |
| Mogućnost kreiranja vlastitih grupa i veza između prijetnji, imovine i kontrola. |  |  |  |
| Prijavom kao administrator moguće je sve pripremljene kataloge izmijeniti po vlastitoj želji. |  |  |  |
| Izmjena kataloga vjerojatnosti, utjecaja, veličine rizika, statusa i tipova entiteta i sl. |  |  |  |
| Uvoz podataka iz vanjskih izvora za gotovo sve kataloge putem web formi. |  |  |  |
| Automatsko kreiranje SoA izvješća (Statement of Applicability). |  |  |  |
| **Katalog IS servisa i procesa te procjena usklađenosti** |  |
| Izrada kataloga IT servisa. |  |  |  |
| Izrada kataloga poslovnih procesa. |  |  |  |
| Set podataka potreban za izradu analize utjecaja na poslovanje (engl. BIA – Business Impact Analysis). |  |  |  |
| Automatsko generiranje plana oporavka IT servisa na temelju unesenih podataka  |  |  |  |
| Povijesno praćenje statusa revizija kontrola. |  |  |  |
| Upravljanje nalazima/ranjivostima. |  |  |  |
| **Izrada izvještaja** |  |
| Sve ekrane je moguće ispisati u više poznatih formata (PDF, Word, Excel, slike). |  |  |  |
| Set osnovnih izvješća poput popisa imovine i prijetnji, popisa rizika, statusa usklađenosti po raznim standardima (ISO 27001:2013, ISO 27002:2013, ISO 22301:2012, CobiT, NIST, GDPR). |  |  |  |
| Dio izvješća je moguće prikazati i u grafičkom formatu („dashboard“ stranica s više grafova). |  |  |  |
| Jednostavno sortiranje i filtriranje sadržaja izvještaja po gotovo svim parametrima. |  |  |  |
| Logo korisnika u izvješćima. |  |  |  |
| Sve ekrane je moguće ispisati u više poznatih formata (PDF, Word, Excel, slike). |  |  |  |
| Set osnovnih izvješća poput popisa imovine i prijetnji, popisa rizika, statusa usklađenosti po raznim standardima (ISO 27001:2013, ISO 27002:2013, ISO 22301:2012, CobiT, NIST, GDPR). |  |  |  |
| Dio izvješća je moguće prikazati i u grafičkom formatu („dashboard“ stranica s više grafova). |  |  |  |
| Jednostavno sortiranje i filtriranje sadržaja izvještaja po gotovo svim parametrima. |  |  |  |
| Logo korisnika u izvješćima. |  |  |  |
| **Upravljanje evidencijama osobnih podataka** |  |
| Vođenje registra evidencijama obrada osobnih podataka koji uključuje unos, promjenu, brisanje pojedinih evidencija osobnih podataka. |  |  |  |
| Mogućnost provođenja DPIA analize nad evidencijama obrada osobnih podataka |  |  |  |
| Pregledno sučelje za vizualni prikaz i obradu svih evidencija obrada osobnih podataka zajedno sa njihovim parametrima (informacijama o obradama). |  |  |  |
| Registar evidencija obrada osobnih podataka mora uključivati minimalno slijedeće informacije:* Tip evidencije i osobnih podataka
* Svrha
* Izvori prikupljanja osobnih podataka
* Osobe čiji podaci se prikupljaju
* Pravna osnova temeljem koje se podaci prikupljaju
* Kada se osobni podaci prikupljaju i ažuriraju
* Kome osobni podaci smiju biti otkriveni
* Mjesto i period čuvanja evidencije i osnova po kojoj se čuva
* Veza prema drugim aplikacijama, uvoz i izvoz osobnih podataka
* Mogućnost nadzora aktivnosti u aplikaciji putem evidencije pristupa
* Mogućnost osiguranja raspoloživosti evidencije
 |  |  |  |
| **Upravljanje zahtjevima i privolama** |  |
| Mogućnost unosa i obrade korisničkih zahtjeva i privola od strane ispitanika. |  |  |  |
| Mogućnost unosa i obrade korisničkih zahtjeva i privola od strane DPO u ime ispitanika. |  |  |  |
| Mogućnost unosa i obrade svrhe prikupljanja osobnih podataka |  |  |  |
| Mogućnost promjene svrhe prikupljanja osobnih podataka |  |  |  |
| Obrada zahtjeva i privola ispitanika. Ispitanik mora imati mogućnost povlačenja privole, uvida u osobne podatke, brisanje osobnih podataka i promjenom privole. Na osnovi tog zahtjeva DPO mora moći odrediti tko je odgovoran za njegovu obradu. Sve aktivnosti koje se obavljaju prilikom obrade ovog zahtjeva se bilježe na zahtjev te ispitanik ima uvid u tijek obrade zahtjeva. |  |  |  |
| Prijava incidenta ugroze podataka. Sustav mora omogućiti prijavu incidenta od strane ispitanika ili DPO. DPO mora imati mogućnost upisa svih aktivnosti koje se radi tijekom obrade incidenta. |  |  |  |
| Prijava zahtjeva ili incidenta od strane ispitanika ili DPO-a. Mora se moći odabrati na što se odnosi incident. |  |  |  |
| Mogućnost obrade incidenta koja omogućuje unos aktivnosti koje su poduzete prilikom obrade incidenta. |  |  |  |
| Mogućnost izrade fleksibilnih izvještaja sa različitim kombinacijama parametara o zahtjevima i privolama. |  |  |  |
| Prikaz povijesti privola ispitanika za određenu svrhu prikupljanja podataka. |  |  |  |
| Davanje privole ispitanika na pojedinačne tipove osobnih podataka. |  |  |  |
| Upravljanje povlačenjem privole na pojedine svrhe prikupljanja osobnih podataka ili za pojedine osobne podatke. |  |  |  |

Uz sve gore navedeno, Ponuda mora uključivati stručne usluge Ponuditelja kako slijedi:

**Implementacija**

**Analiza**

• izrada upitnika za implementaciju sustava

• snimka postojećih poslovnih procesa i njihovih prioriteta, pravilnika i infrastrukture neophodnih za implementaciju sustava

• organiziranje Information Governance radionica za prikupljanje informacija

**Dizajn rješenja**

• dizajn arhitekture rješenja i modela u sustavu;

• definiranje sigurnosnih politika i postavki:

• izrada dokumenta prijedloga rješenja.

**Instalacija i konfiguracija rješenja**

• Instalacija i inicijalna konfiguracija

• Integracija u postojeću infrastrukturu

• Izrada i konfiguracija sigurnosnih politika i postavki:

• Prikupljanje i analiza povratnih informacija od korisnika;

• Dorada, ispravljanje i fino podešavanje

• Priprema za produkciju

**Obuka**

Usluge obuke osoblja Naručitelja. Obuka će se sastojati od teoretskog i praktičnog dijela u trajanju od ukupno 2 dana tako da pruži neophodna znanja za administratore i operatere sustava te službeniku za zaštitu osobnih podataka. Obuku provodi Ponuditelj.

**Izrada dokumentacije**

• Izvedbena dokumentacija za implementirani sustav sa detaljno opisanim rješenjem i pojedinačnim komponentama;