**Obrazac 3.**

**Tehnička specifikacija**

**predmeta nabave za točku 5.7. *Sustav za pretraživanje repozitorija, praćenje tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka* 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 1.* **Minimalne zahtijevane funkcionalne i tehničke specifikacije za točku 5.7. 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 1. Sustav za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka** |
| **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 5.7. iz Projektnog zadatka** | **UVJETI ISPUNJENI (Da/Ne)** | **Bilješke, napomene, reference na tehničku dokumentaciju** | **OCJENA**  **DA/NE** |
| --- | --- | --- | --- |
|  |  |  |  |
| Rješenje mora biti u obliku visoko specijalizirane programske podrške (softvera) za pretraživanje repozitorija, praćenja tijeka osobnih podataka i sprječavanja kompromitiranja, neovlaštene upotrebe i prijenosa osobnih podataka u korporativnom okruženju (u daljnjem tekstu DLP - eng. Data Loss Prevention) |  |  |  |
| Rješenje mora uključivati licence za 330 računala i 330 korisnika |  |  |  |
| Rješenje mora biti sveobuhvatno i namijenjeno korporativnim okruženjima te detektirati i kontrolirati podatke u tri različita stanja/oblika:   * Data-in-use, DLP na računalu (DLP Endpoint) * Data-in-motion, DLP na mreži (DLP Prevent for E-mail, DLP Prevent for Web) * Data-at-rest, DLP discovery funkcionalnosti pretraživanja mrežnih repozitorija i baza podataka (DLP Discover) |  |  |  |
| Rješenje mora uključivati zaštitu podataka na radnim stanicama putem DLP Endpoint agenata i kontrolu korištenja odljeva podataka svim potencijalnim kanalima na radnim stanicama. Arhitektura mora podrazumijevati da se na štićena računala implementiraju DLP Endpoint agenti kojima se potpuno upravlja iz centraliziranog administrativnog sučelja. |  |  |  |
| Rješenje mora uključivati komponentu u obliku virtualnog mrežnog uređaja na VMware platformi za kontrolu i zaštitu e-mail poruka (DLP Prevent for E-mail) putem SMTP protokola koristeći dodavanje X header oznaka u e-mail poruke na temelju koje podržano MTA rješenje može poduzeti odgovarajuću sigurnosnu radnju.  Komponentom se mora upravljati iz centraliziranog administrativnog sučelja. |  |  |  |
| Rješenje mora uključivati komponentu u obliku virtualnog mrežnog uređaja na VMware platformi za kontrolu i zaštitu web prometa (DLP Prevent for Web) na način da se integrira sa ICAP kompatibilnim web gateway uređajem i na taj način pregledava odlazne mrežne pakete.  Komponentom se mora upravljati iz centraliziranog administrativnog sučelja. |  |  |  |
| Rješenje mora uključivati komponentu za pretraživanje mrežnih repozitorija i baza podataka (DLP Discover) sa podrškom za pretraživanje minimalno:   * Common Internet file system/ server message block (CIFS) * Network file system (NFS) * Baze podataka: Microsoft SQL, IBM DB2, MySQL Enterprise, Oracle * Microsoft Sharepoint |  |  |  |
| Rješenje mora imati mogućnosti analitike podataka otkrivenih pretraživanjem putem DLP Discover komponente koristeći Online Analytical Processing (OLAP) tehnologiju. |  |  |  |
| Agent na štićenim računalima mora biti potpuno funkcionalan i kada računala nisu spojena na mrežu (off-line mod). |  |  |  |
| Rješenje mora imati podršku za rad i zaštitu minimalno slijedećih operativnih sustava: - Windows 7 SP1 i noviji  - Windows Server 2008 R2 i noviji  - Mac OS 10.10 i noviji |  |  |  |
| Rješenje mora imati podršku sa minimalno slijedećih Internet preglednicima: - Internet Explorer - Mozilla Firefox  - Google Chrome |  |  |  |
| Agent na računalu mora imati podršku za rad sa FastUserSwitching (FUS) u Windows OS okolini sa više korisnika. |  |  |  |
| Rješenje mora podržavati integraciju sa MS Active Directory imeničkim servisom. |  |  |  |
| Rješenje mora omogućiti učinkovitu zaštitu od odjeljiva podataka putem svih od slijedećih kanala: prijenosni mediji, email, web, printing, clipboard, screen capture / print screen, kopiranje na mrežne diskove i vanjske diskove, WiFi, Bluetooth, IM - instant messaging, slanje u cloud servise. |  |  |  |
| Rješenje mora funkcionirati po principu dubinskog pregleda sadržaja digitalnih podataka (eng. Content-based ili content-aware). |  |  |  |
| Rješenje mora imati ugrađenu mogućnost klasifikacije podataka minimalno slijedećim metodama: - rječnici (eng. dictionary) - validacijski algoritmi - registracija dokumenata - ručno tagiranje (digitalno označavanje datoteka) - automatsko tagiranje - whitelisting - podrška za prepoznavanje metadata oznaka specijaliziranih rješenja drugih proizvođača (TITUS i Boldon James) |  |  |  |
| Rješenje mora imati mogućnost izrade i primjene sigurnosnih politika minimalno prema slijedećim kategorijama zaštite pri pokušaju: - slanja e-maila - slanja na web - slanjem putem mreže - slanja na print - kopiranja na prijenosni medij - kopiranja na mrežni disk - kopiranja (clipboard) - screen capture / print screen |  |  |  |
| Rješenje mora imati mogućnost minimalno slijedećih reakcija u slučaju detekcije određene radnje sa osjetljivim podatkom: - bez reakcije - blokiraj - premjesti datoteku - zatraži opravdanje - primijeni RM - rights management politiku - quarantine - tagiraj / označi - otvori DLP incident - prikaži u centralnoj konzoli - obavijesti korisnika - spremi originalnu datoteku - sačuvaj dokaz |  |  |  |
| Rješenje mora imati mogućnosti da zatraži od korisnika da unese opravdanja za iznošenje/slanje podataka (eng. justification). |  |  |  |
| Rješenje mora imati mogućnosti prilagodbe notifikacija za korisnike. |  |  |  |
| Rješenje mora imati mogućnosti privremene deaktivacije agenta. |  |  |  |
| Rješenje mora imati ugrađenu mogućnosti za digitalno označavanje datoteka (eng. content fingerprinting) automatski s obzirom na to koja je aplikacija proizvela datoteka. Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |  |  |  |
| Rješenje mora imati ugrađenu mogućnosti za digitalno označavanje datoteka (eng. content fingerprinting) automatski s obzirom na to sa koje je web aplikacije skinuta datoteka. Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |  |  |  |
| Rješenje mora imati ugrađenu mogućnosti za digitalno označavanje datoteka (eng. content fingerprinting) automatski s obzirom na to sa koje je mrežne lokacije skinuta datoteka. Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |  |  |  |
| Rješenje mora imati ugrađenu mogućnosti za nasljeđivanje digitalne oznake datoteke (eng. content fingerprinting) prilikom kopiranja ili premještanja osjetljivog sadržaja u drugu datoteku na način da se prilikom te radnje parsira sadržaj koji se replicira ili premješta te, u slučaju prepoznavanja, automatski dodjeljuje oznaka (eng. fingerprint). Na temelju oznake moraju se moći primjenjivati DLP sigurnosne politike. |  |  |  |
| Rješenje mora imati ugrađenu mogućnosti učinkovitog upravljanja sigurnosnim politikama putem pravila za zaštitu podataka. Pravila se moraju moći grupirati i dodjeljivati prema objektima u MS Active Directory imeničkom servisu. |  |  |  |
| Rješenje mora imati ugrađenu podršku za skeniranje, analizu i pronalaženje podataka (eng. Discovery scan) na korisničkim računalima koje po pronalasku mora imati minimalnu mogućnosti slijedećih radnji: - prijavi incident u središnjoj DLP konzoli - prikupi dokaz što podrazumijeva kopiranje pronađene datoteke na lokaciju za prikupljanje dokaza radi daljnjeg pregleda i obrade |  |  |  |
| Rješenje mora imati funkcionalnu mogućnost za podizanje svijesti korisnike te kroz poruke i upozorenja na računalu korisnika uključiti ga u proces medijacije. |  |  |  |
| Rješenje mora imati mogućnost standardne integracije sa postojećim rješenjem za enkripciju podataka koje Naručitelj ima na raspolaganju (McAfee Encryption) ili mora uključivati funkcionalnost i licence za enkripciju datoteka, mapa i prijenosnih medija. |  |  |  |
| Rješenje mora imati ugrađenu mogućnosti upravljanja sigurnosnim politikama za prijenosne medije (eng. Device Control ili Removable Media Control) koje raspolaže minimalno sa slijedećim mogućnostima: - filtriraj - nadgledaj (monitor) - blokiraj prijenos osjetljivih sadržaja na prijenosne medije |  |  |  |
| Upravljanje politikama za prijenosne medije mora uključivati mogućnost primjene odabirom minimalno slijedećih kriterija: - korisnik i grupa korisnika - računalo - product ID - ID proizvođača - serijski broj - klasa uređaja - naziv uređaja |  |  |  |
| Upravljanje politikama za prijenosne medije mora uključivati mogućnost primjene prema redu. |  |  |  |
| Rješenje mora imati ugrađenu mogućnost da učini određeni prijenosni mediji blokiranim ili read-only. |  |  |  |
| Rješenje mora imati mogućnost integracije sa rješenjima za enkripciju datoteka i mapa. |  |  |  |
| Rješenje mora imati mogućnost integracije sa DRM (Digital Rights Management) rješenjima i to minimalno MS AD RMS. |  |  |  |
| Rješenje mora imati mogućnost integracije sa specijaliziranim rješenjima za klasifikaciju i označavanje podataka koja rade na principu da datotekama dodaju meta podatke (eng. metadata). DLP rješenje mora biti u mogućnosti detektirati takav podatak prema prepoznatim meta podacima te automatski primijeniti određenu sigurnosnu politiku. |  |  |  |
| Rješenje mora imati mogućnost blokiranja pristupa podacima kod mapiranih uređaja na tankim klijentima i to minimalno: - lokalnim diskovima - prijenosnim medijima - printerima - CD/DVD - clipboard |  |  |  |
| Rješenjem se mora upravljati putem centralizirane upravljačke konzole u obliku web aplikacije. |  |  |  |
| Centralna upravljačka konzola mora biti prilagodljiva korisničkim zahtjevima (eng. customizable). |  |  |  |
| Centralna upravljačka konzola mora imati mogućnosti da se sučelje prilagođeno za jednog korisnika može jednostavno primijeniti i na druge korisnike. |  |  |  |
| Centralna upravljačka konzola mora imati mogućnosti izrade naprednih izvještaja i mogućnost da se izvještaji prikažu u obliku dashboarda u konzoli. Izvještaji se moraju moći izvesti (eng. export) ili automatski poslati e-mailom. |  |  |  |
| Rješenje mora imati mogućnosti podešavanja automatiziranih dnevnih aktivnosti. |  |  |  |
| Centralna upravljačka konzola mora podržavati granulirano upravljanje korisničkim pravima putem uloga (RBAC – Roled Based Access Control). |  |  |  |
| Rješenje mora imati mogućnost naknadne integracije sa rješenjem za zaštitu od naprednih prijetnji (eng. APT - Advanced Persistent Threats). |  |  |  |
| Rješenje mora imati mogućnosti iz centralne upravljačke konzole udaljeno implementirati agente na računala i kasnije njima upravljati. |  |  |  |
| Povezani incidenti moraju se moći grupirati u slučaj "case" koji se zatim može delegirati nadležnom korisniku na daljnju obradu. |  |  |  |
| Rješenje mora podržavati mogućnost da se definiraju korisnici sa posebnim pravima nad pojedinim elementima u sustavu (eng. stakeholders) koji bivaju automatski notificirani kada se dogodi određena vrsta incidenta ili koji imaju posebne privilegije u sustavu. |  |  |  |
| Rješenje mora imati dostupno API sučelje. |  |  |  |
| Rješenje mora omogućiti iz centralne upravljačke konzole izradu detaljnih izvještaja koji pokazuju auditorima, upravi i ostalim interesnim stranama informacije vezane uz interne i regulatorne sigurnosne sukladnosti. |  |  |  |

Uz sve gore navedeno, Ponuda uključuje 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 Data Governance radionica za prikupljanje informacija od korisnika koje točno poslovne informacije je potrebno štititi i na koji način - definiranje politika;

• definiranje elemenata infrastrukture na kojima će se raditi zaštita podataka:

**Dizajn rješenja**

• dizajn arhitekture rješenja;

• definiranje sigurnosnih politika i postavki:

• definiranje rasporeda skeniranja i repozitorija koji će se skenirati;

• izrada dokumenta prijedloga rješenja.

**Instalacija i konfiguracija rješenja**

• Instalacija i inicijalna konfiguracija

• Integracija u postojeću infrastrukturu

• Izrada i konfiguracija sigurnosnih politika i postavki:

• Implementacija rješenja na pilot grupi računala (do 20 računala)

• Prikupljanje i analiza povratnih informacija od korisnika;

• Dorada, ispravljanje i fino podešavanje sigurnosnih politika;

• 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;