|  |
| --- |
| **PRILOG 7. Tehničke specifikacije** |
| Naručitelj:  | Gauss d.o.o. |
| Predmet nabave:  | Razvoj prilagođenog sustava za sigurnost podataka i resursa tvrtke |

**Predmet nabave: Razvoj prilagođenog sustava za sigurnost podataka i resursa tvrtke**

Ponuditelj OBAVEZNO POPUNJAVA stupac „UVJETI ISPUNJENI DA/NE“. te ukoliko odgovori „DA“ na taj se način obvezuje na isporuku usluge koja minimalno ispunjava traženi tehnički uvjet. Ukoliko se prilikom pregleda utvrdi da je neki odgovor „NE“ ili uopće nije odgovoreno, ponuda će biti odbijena.

Ponuditelj ne smije mijenjati specifikacije navedene u stupcu „Tražene funkcionalnosti IKT rješenja/sustava“.

Za sve stavke navedene u tehničkim specifikacijama u kojima se možebitno traži ili navodi marka, norma te standardi, patent, tip ili određeno podrijetlo primjenjuje se „ili jednakovrijedno“. Eventualna prateća dokumentacija koju Ponuditelj dostavlja kao nadopunu ponudi mora jasno ukazivati na modele odnosno opcije koje se nude.

**Tehničke specifikacije IKT rješenja (sustava)** navedene u tablici u formatu kontrolne liste obavezne su kao minimalni standard koji mora zadovoljiti ukupno IKT rješenje i pojedinačni IKT moduli.

Stupac «Bilješke, napomene, reference na dokumentaciju» Ponuditelj može popuniti ukoliko smatra potrebnim.

|  |  |  |  |
| --- | --- | --- | --- |
| RB | Tražene funkcionalnosti IKT rješenja / sustava | Uvjeti ispunjeni DA / NE | Bilješke, napomene, reference na dokumentaciju |
| I | II | III | IV |
| 1. **UPRAVLJANJE EVIDENCIJOM ULAZA I PROSTORIJA**
 |
| 1 | Potrebno je analizirati postojeću situaciju u tvrtki i osmisliti jasnu i cjelovitu politiku kontrole pristupa za sve zaposlenike i vanjske posjetitelje. |  |  |
| 2 | Sustav treba sadržavati tablični pregled svih korisnika evidencije ulaza, s detaljnim informacijama, koji je dostupan samo ovlaštenim korisnicima. |  |  |
| 3 | Korisnici s nižim ovlaštenjima, privilegijama pristupa ne smiju imati pregled svih ostalih korisnika sustava, niti dinamike ulaza/izlaza. |  |  |
| 4 | Detaljne informacije o korisnicima u sustavu nisu ograničene brojem polja podataka, nego imaju opciju unosa dodatnih adresa i dodatnih kontakt ili drugih potrebnih podataka. |  |  |
| 5 | Informacije o korisnicima sustava je moguće filtrirati, sortirati i pretraživati u tabličnom prikazu i prema potrebi arhivirati i/ili vratiti iz arhive ili trajno obrisati. |  |  |
| 6 | Pregled različitih poslovnih prostora (ureda, sala, zajedničkih prostorija) unutar sustava korisnik mora imati prikazano tablično. |  |  |
| 7 | Sustav treba omogućiti kreiranje i uređivanje poslovnih prostora putem web forme. |  |  |
| 8 | Minimalni osnovni podatci za svaki poslovni prostor u sustavu moraju biti: naziv, pripadajući poslovni prostor, kratki opis, slika. |  |  |
| 9 | Izbor pripadajuće zgrade mora biti vezan za kreirane zgrade s pripadajućim podatcima. |  |  |
| 10 | Sustav treba omogućavati kreiranje i uređivanje zgrade putem web forme. |  |  |
| 11 | Sustav treba omogućiti kreiranje neograničenog broja poslovnih prostora unutar svake zgrade. |  |  |
| 12 | Sukladno ovlaštenjima, korisnik sustava mora moći uređivati ili brisati različite prostore i zgrade. |  |  |
| 13 | Sukladno ovlaštenjima, korisnik mora moći izvršiti i rezervaciju za korištenje poslovne prostorije. |  |  |
| 14 | Minimalni osnovni podatci vezani za rezervaciju prostora moraju biti: naziv, opis, napomena, datum kreiranja rezervacije, vrijeme početka rezervacije, vrijeme završetka rezervacije. |  |  |
| 15 | Korisnik koji rezervira prostor može dodijeliti druge korisnike u odabrani termin, primjerice druge zaposlenike, vanjske suradnike i klijente. |  |  |
| 16 | Svaki poslovni prostor unutar sustava ima svoju razinu zaštite, pa se mogu kategorizirati primjerice dijeljeni prostori za zaposlenike, prostori za sastanke i konferencije i posebno zaštićene poslovne cjeline. |  |  |
| 17 | Podsustav za upravljanje evidencijom ulaza, odnosno kontrole pristupa, omogućava korisnicima posebne privilegije pristupanja u prostore sukladno razinama ovlaštenja. |  |  |
| 18 | Podsustav kontrole pristupa ima posebnu zaštitu štićenih cjelina kao što su: server sobe, posebne uredske prostorije, arhivske prostorije i dr. |  |  |
| 19 | Podsustav kontrole pristupa ima arhivu pristupanja posebno zaštićenim poslovnim jedinicama. |  |  |
| 20 | Podsustav koristi rješenja za otključavanje pomoću RFID beskontaktnih kartica ili tag privjesaka i šifri. |  |  |
| 21 | Programiranje korisničkih kartica u svrhu kontrole ulaza ili privjesaka za korisnike je uključeno u izradu sustava. |  |  |
| 22 | Podsustav omogućuje da ukidanjem privilegije ulaza određenom korisniku nema promjena brava ili šifri, nego se njegova kartica i privilegija pristupa jednostavno poništi. |  |  |
| 23 | Podsustav omogućuje da svaki korisnik ima jedinstvenu karticu ili identifikacijski element što omogućava individualnu kontrolu kao i praćenje aktivnosti. |  |  |
| 24 | Podsustav omogućuje da svaki neovlašteni pokušaj ulaska u zaštićenu poslovnu cjelinu ostane evidentiran. |  |  |
| 25 | Podsustav omogućuje da svaki zabilježeni neovlašteni pokušaj ulaska u zaštićenu poslovnu cjelinu kreira automatsku notifikaciju ovlaštenoj osobi za kontrolu pristupa. |  |  |
| 26 | Tablična lista ulaza u podsustavu treba omogućiti filtriranje po mjesecu, tjednu, danu. |  |  |
| 1. **UPRAVLJANJE GDPR REGULATIVOM**
 |
| 1 | Podsustav za GDPR upravljanje sadrži evidencije incidenata vezane uz povredu osobnih podataka, evidencije zahtjeva ispitanika ua ostvarivanje prava iz GDPR uredbe, upravljanje privolama ispitanika, upravljanje GDPR |  |  |
| 2 | Voditelji obrade osobnih podataka kao i izvršitelji obrade osobnih podataka mora moći redovito ažurirati evidenciju aktivnosti obrade podataka te editirati, anonimizirati, brisati i arhivirati korisnike i dokumente. |  |  |
| 3 | Voditelj obrade osobnih podataka je ujedno administrator podsustava za upravljanje GDPR procesa te može odlučiti kojim će korisnicima dodijeliti napredna korisnička prava kako bi mogli sudjelovati u administriranju rješenja sukladno svojim ovlastima. |  |  |
| 4 | Podsustav treba omogućiti jednostavno prikupljanje i bilježenje velikog broja privola za obradu osobnih podataka vezano uz veći broj poslovnih procesa (ljudski resursi, marketinške aktivnosti) koje se temelje na zakonskoj ili ugovornoj obvezi te na legitimnom interesu. |  |  |
| 5 | Podsustav treba omogućiti kontrolu nad osobnim podacima korisnika i ostalih zainteresiranih stranaka (klijenata, poslovnih suradnika i slično). |  |  |
| 6 | Podsustav treba omogućiti ispitanicima kontrolu i transparentan pregled korištenja njihovih osobnih podataka kao i davanje ili povlačenje privole za one aktivnosti obrada koje se temelje na privolama. |  |  |
| 7 | Podsustav mora omogućiti unos svim korisnicima sustava potpisivanje i prikupljanje više vrsta privola vezanih uz Zaštitu podataka i upload i sigurno čuvanje privola drugih koji nisu korisnici sustava. |  |  |
| 8 | Minimalne informacije GDPR privole i sporazuma su: naziv, jezik, tekst svrhe, sadržaj privole, pripadnost sporazumima, jedinstveni broj, verzija, datum kreiranja, osoba koja je kreirala. |  |  |
| 9 | Proces anonimizacije unutar podsustava mora obuhvaćati šifriranje podataka prilikom pohrane kako bi eventualno pokradeni podaci bez ključa za dešifriranje bili beskorisni. |  |  |
| 10 | Nakon anonimizacije određenog korisnika, drugi neovlašteni korisnik sustava, koji je prethodno imao pristup informaciji, ne smije moći povezati anonimizirane podatke s određenom osobom, odnosno podatci moraju biti anonimizirano tako da smije biti moguće identificirati pojedinca iz anonimiziranih podataka. |  |  |
| 11 | Ovlašteni korisnik mora moći po zahtjevu anonimizirati drugog korisnika sustava. |  |  |
| 12 | Podsustav za upravljanje GDPR-om omogućuje jednostavni izvoz podataka kroz nekoliko unaprijed pripremljenih izvještaja u .xlsx formatu: evidencija aktivnosti obrade, popis korisnika i drugih osoba, popis sustava pohrane, popis ispitanika sa statusom privola po aktivnosti obrade itd. |  |  |
| 13 | Podsustav za upravljanje GDPR-om omogućava jednostavno konfiguriranje i ugrađivanje privola na postojeće web obrasce u svrhu prikupljanja privola izravno u podsustav. |  |  |
| 14 | Podsustav omogućava unos i administriranje zahtjeva ispitanika za ostvarenje svojih GDPR prava (primjerice zahtjev za anonimizaciju) s naznačenim vremenskim rokom i praćenjem promjene statusa zahtjeva. |  |  |
| 15 | GDPR zahtjeve korisnik može unijeti izravno u sustav te pratiti rješavanje.  |  |  |
| 16 | Kreiranje zahtjeva za anonimizaciju trigerira obavijest / notifikaciju korisniku zaduženom za rješavanje. |  |  |
| 1. **UPRAVLJANJE OSJETLJIVIM DOKUMENTIMA**
 |
| 1 | Postoji jedinstveni podsustav unutar kojeg je moguće upravljati različitim vrstama osjetljivih dokumenata i datoteka tvrtke (npr. dokumenti financijske prirode, intelektualno vlasništvo, osobni podaci korisnika, izvorni kod projekata kao intelektualno vlasništvo, ugovori, ponude, određeni računi, procedure za upravljanje kvalitetom). |  |  |
| 2 | Dokumente je moguće učitati i spremiti u pdf formatu, kreirati predloške, izdavati predloške, kategorizirati, sortirati, brisati, arhivirati. |  |  |
| 3 | Dokumenti se unutar podsustava mogu sortirati prema kategorijama, koje korisnik s ovlaštenjem/privilegijom može pregledavati, kreirati, uređivati i brisati. |  |  |
| 4 | Kategorije dokumenata i datoteka unutar podsustava je moguće neograničeno kreirati, primjerice prema hitnosti, vrsti dokumenta, prema radnim procesima (razvoj, uredsko poslovanje, ostalo) i drugo. |  |  |
| 5 | Dokumente i datoteke unutar podsustava je moguće dijeliti, odnosno pridružiti osobi ili klijentu. |  |  |
| 6 | Povijest svih promjena pojedinog dokumenta ili datoteke sadrži informacije o tome tko i kada je izvršio promjenu, trenutnu i sve prošle verzije istog. |  |  |
| 7 | Na dokumentima je moguće ostavljati interne bilješke korisnika vidljive samo korisniku koji ih je kreirao i korisnicima s ovlaštenjem/privilegijom za isto. |  |  |
| 8 | Unutar podsustava je moguće učitavanje, kategoriziranje i sortiranje svih skeniranih osjetljivih dokumenata. |  |  |
| 1. **UPRAVLJANJE MREŽNOM SIGURNOŠĆU I IT INFRASTRUKTUROM**
 |
| 1 | Podsustav za upravljanje mrežnom sigurnošću i IT infrastrukturom prepoznaje dvije kategorije korisnika: osnovni korisnik i freeIpa korisnik. |  |  |
| 2 | Logiranje korisnika u podsustav se odvija preko sigurnosne autentikacije; s mogućnosti dvostupanjske autorizacije. |  |  |
| 3 | Logiranje FreeIP-a korisnika se odvija uz pomoć FreeIP-a sustava. |  |  |
| 4 | Podsustav mora omogućiti dodavanje servera, web stranica, Internet stvari (engl. Internet of Things-IoT) sa pripadajućim informacijama kao tipova resursa na monitoring. |  |  |
| 5 | Podsustav omogućuje jednostavan pregled, sortiranje i filtriranje dodanih resursa, kao i uređivanje i upravljane podatcima svakog pojedinog resursa. |  |  |
| 6 | Zajednički parametri za sve resurse moraju omogućiti definiranje minimalno: intervale provjere resursa i osvježenja podataka, vrstu monitoringa (aktivni ili pasivni), očekivano vrijeme odgovora, dopušteni broj grešaka i sl. |  |  |
| 7 | Za tip resursa *serveri* podsustav mora omogućiti praćenje minimalno sljedeće parametre: broj procesa, specifikacija procesa, broj konekcija na bazu, ping (vrijeme odaziva servera) kao i ostale relevantne podatke koji omogućuju adekvatno praćenje resursa npr. slobodan prostor na disku, praćenje statusa memorije (ukupna memorija, slobodno memorije, zauzeće memorije, stanje privremenog diska) |  |  |
| 8 | Za tip resursa *IoT i ostalih uređaja*, podsustav mora omogućiti praćenje vremena odaziva sustava (PING) i ostale vrijednosti koje sustav i resurs podržavaju. |  |  |
| 9 | Za tip resursa *web stranice*, podsustav mora omogućiti praćenje minimalno sljedećih parametara: vrijeme otvaranja stranice, dostupnost baze podataka i ostalih servisa koje stranica koristi (redis, Elastic, memcached, i sl.), mogućnost definiranja posebnih adresa, mjerenja odaziva i ostalih relevantnih vrijednosti. |  |  |
| 10 | Za tip resursa *web stranica*, podsustav mora omogućiti download zasebnih modula/plugina koji će omogućiti praćenje web stranica koje koriste razne web tehnologije sa specifičnim parametrima za svaku od navedenih tehnologija. |  |  |
| 11 | Podsustav mora omogućiti praćenje valjanosti sigurnosnih certifikata. |  |  |
| 12 | Podsustav mora omogućiti preuzimanje (download) dokumentacije za ručno razvijanje modula/API poziva iz i prema sustavu (aktivni i pasivni način). |  |  |
| 13 | Podsustav mora omogućiti prepoznavanje dva tipa odnosno mode-a resursa: aktivni i pasivni resurs. |  |  |
| 14 | Aktivni resurs samostalno šalje podatke u podsustav primjerice: IoT uređaj, NodeJS ili C aplikacija. Generalno tamo gdje sustav ne može pasivnim modom dohvatiti podatke. |  |  |
| 15 | Pasivni resurs dostavlja podatke na zahtjev sustava, odnosno u okolinama gdje je to moguće. |  |  |
| 16 | Podsustav mora moći generirati korisničko ime (dalje u tekstu ID) te tajni ključ za resurse tipa server i web stranica prilikom dodavanja istog, koji će se koristiti kao identifikator i za potrebe sigurnosti.  |  |  |
| 17 | Podsustav mora omogućiti poduzimanje specifičnih akcija ovisno o vrsti resursa. |  |  |
| 18 | Podsustav mora omogućiti sljedeće akcije kod serverskih resursa: pokretanje, zaustavljanje i ponovno pokretanje servisa kao što su apache, nginx, redis, mysql, Elasticsearch, tj. ovisno o servisima instaliranima na serveru. |  |  |
| 19 | Podsustav pruža download predkompajliranog serverskog paketa (serverskog software-a) koji se instalira na server kao "daemon" (servis) te ima ugrađeni WATCHDOG. Ovaj servis prima podatke od PHP stranice (https site) koji preusmjerava na navedeni servis. Podatci sadržavaju JWT token kojim se verificira legitimnost zahtjeva. Osim toga, servis podržava komunikaciju putem porta (REST komunikaciju). Konfiguracija servisa se nalazi u konfiguracijskoj datoteci koja sadržava: Encription key, server id te ostale postavke koje se generiraju pri samom definiranju serverskog resursa te vrstu komunikacije koju server podržava (port/php site). Service mora biti pisan u C programskom jeziku. |  |  |
| 20 | Podsustav mora automatski slati notifikacije prema definicijama zapisanim u notifikacijskim postavkama. |  |  |
| 21 | Podsustav ima opciju unosa strukturiranih informacija o materijalima i opremi koje posjeduje tvrtka. |  |  |
| 22 | Podsustav mora omogućiti definiranje notifikacija za različite važne događaje. |  |  |
| 23 | Podsustav mora omogućiti slanje specifičnih notifikacija ako je dosegnuto stanje ili kombinacija stanja parametara koje se prate i to općenito za sve, za grupu resursa, za tip resursa ili za svaki pojedinačni resurs.Notifikacije se trebaju moći slati konfigurabilno: grupama korisnika, svim korisnicima, pojedinačnim korisnicima. |  |  |
| 24 | Podsustav mora za svaku notifikaciju, svakom korisniku, omogućiti izbor primanja notifikacije. Primjerice, slanje notifikacije treba biti moguće: email-om, SMS-om, push notifikacijom na mobilni uređaj. |  |  |
| 25 | Notifikacije moraju moći pripadati minimalno sljedećim razinama: normalna notifikacija, visoka razina, kritična razina. |  |  |
| 26 | Podsustav treba omogućiti slanje specifičnih izvještaja na email korisnika u određenim intervalima, primjerice; svakog dana u 7:00 sati, svakog prvog u mjesecu itd. |  |  |
| 27 | Podsustav mora omogućiti izvoz izvještaja u PDF, CSV, Excel. |  |  |
| 28 | Podsustav mora omogućiti izradu grafičkog praćenja parametara sustava u vidu konfigurabilnih grafikona. |  |  |
| 29 | Podsustav mora omogućiti definiranje upravljačke ploče tzv. dashboarda na kojoj se nalaze različiti konfigurabilni grafikoni ovisno o ovlaštenjima korisnika. |  |  |
| 30 | Podsustav mora omogućiti definiranje 3 razine alarma za istek SSL certifikata, npr: 30 dana, 7 dana i dan prije isteka istog. |  |  |
| 31 | Podsustav mora omogućiti preuzimanje (engl. download) mobilnih aplikacija. |  |  |
| 32 | Mobilna aplikacija podsustava mora imati iste mogućnosti kao i podsustav: pregled resursa, dodjelu korisnika za notifikacije, razinu kritičnosti. |  |  |
| 33 | Podsustav mora omogućiti postavljanje, pregled i uređivanje mail računa (ovisno o korisničkim ovlaštenjima): e-mail servera, korisničko ime, lozinka. Sustav mora podržavati SMTPs ili jednakovrijedan način. |  |  |
| 34 | Podsustav mora omogućiti postavljanje, pregled i uređivanje notifikacijskog računa (ovisno o korisničkim dozvolama). |  |  |
| 35 | Podsustav mora omogućiti postavljanje, pregled i uređivanje računa SMS pristupnika (ovisno o korisničkim dozvolama): ključ za sučelje za programiranje aplikacija (engl. Api key), tajni ključ za sučelje za programiranje aplikacija (engl. api secret), pošiljatelj. |  |  |
| 36 | Sustav mora omogućiti postavljanje, pregled i uređivanje FreeIPA računa (ovisno o korisničkim dozvolama): putanja do servera, potrebnih podataka za komunikaciju (url, username, password). |  |  |
| 37 | Podsustav mora omogućiti odvajanje korisničkih od sistemskih postavki. |  |  |
| 38 | Podsustav mora zapisivati i prepoznavati zadane ("default") postavke ako korisničke postavke nisu valjane ili postojane; npr. konfiguracija email servera. |  |  |
| 39 | Podsustav mora omogućiti pregled i snimanje tajnog ključa za OTP (2F autentifikaciju). |  |  |
| 40 | Podsustav mora omogućiti pregled i snimanje postavki za mobilne notifikacije. |  |  |
| 41 | Podsustav mora omogućiti pregled i snimanje Servertastic pristupnih API podataka. |  |  |
| 42 | Korisnik podsustava treba moći vidjeti (email, in-app) podsjetnike koji su definirani u raznim podsustavima. |  |  |
| 43 | Podsustav treba omogućiti mapiranje različitih vrsta fizičkih prostora i/ili spremnika za fizičke resurse kao što su oprema ili podatci. |  |  |
| 44 | Za svaki prostor/spremnik podsustav mora moći zabilježiti adresu, kat, točnu lokaciju, ovlaštenu osobu. |  |  |
| 45 | Svakom prostoru/spremniku treba biti moguće dodijeliti jednu ili više vrsta fizičkih resursa, opreme ili dokumenata. |  |  |
| 46 | Za svaki resurs, opremu ili dokument unutar spremnika potrebno je dodijeliti zaduženu osobu odgovornu za isto. |  |  |
| 47 | Svakom prostoru/spremniku treba biti moguće dodijeliti pristupnu fizičku bravu koja se otvara putem RFID ili tag kartice. |  |  |
| 48 | Svakom prostoru/spremniku treba biti moguće dodijeliti visinu sigurnosne razine u vidu pozitivnog cjelobrojnog unosa (od 0 do 100) ili razine pristupa u vidu naziva primjerice: nema ograničenja, niska razina, srednja razina, visoka razina, strogo povjerljivo. |  |  |
| 49 | Svakom korisniku treba biti moguće dodijeliti ovlaštenja za grupu prostora/spremnika, primjerice svi spremnici označeni 60 ili niže, svi spremnici visoka razina ili niže i pojedinačni pristup pojedinom prostoru/spremniku. |  |  |
| 50 | Podsustav treba omogućiti, sukladno dodijeljenim razinama ovlaštenja, otvaranje brava prostora/spremnika. |  |  |
| 51 | Podsustav mora bilježiti vrijeme otvaranja prostora/spremnika, datum i ID RFID ili tag kartice s koje je otvaranje urađeno. |  |  |
| 52 | Podsustav mora bilježiti vrijeme i datum zatvaranja svakog otvorenog prostora/spremnika. |  |  |
| 53 | Podsustav treba moći, za svaki prostor spremnik, konfigurirati vrijeme kada se isti može otvoriti (primjerice samo unutar radnog vremena) kao i maksimalno vrijeme od otvaranja do zatvaranja prostora/spremnika. |  |  |
| 54 | Pokušaj pristupa od strane neovlaštene RFID/tag kartice podsustav treba tretirati kao sigurnosni incident i aktivirati notifikaciju i/ili paljenje fizičkog alarma. |  |  |
| 55 | Pokušaj pristupa izvan dozvoljenog vremena podsustav treba tretirati kao sigurnosni incident i aktivirati notifikaciju i/ili paljenje fizičkog alarma. |  |  |
| 56 | Nezatvaranje prostora/spremnika unutar dozvoljenog konfiguriranog vremena podsustav treba tretirati kao sigurnosni incident i aktivirati notifikaciju i/ili paljenje fizičkog alarma. |  |  |
| 57 | Pristup pojedinim prostorima/spremnicima se kroz podsustav može kontrolirati na daljinu od strane ovlaštenih osoba (primjerice voditelj ureda ima nadzor nad ulaznim vratima radi primanja stranki). |  |  |
| 58 | Za svaki prostor/spremnik podsustav mora bilježiti otvaranja/zatvaranja, ID osobe koja je aktivirala radnje i pretraživanje aktivnosti za svaki pojedini prostor/spremnik. |  |  |
| 59 | Za svakog korisnika podsustav mora pružiti izvještaj povezan sa ulaskom/izlaskom i otvaranjem prostora/spremnika u kronološkom nizu. |  |  |
| 60 | Podsustav mora omogućiti grafički prikaz prostora/spremnika u vidu konfigurabilnog tlocrta na katu zgrade sa „drag&drop“ prikazom samih spremnika.  |  |  |
| 61 | Svaki otvoreni spremnik/prostor za konfigurabilnom bravom podsustav treba prikazivati na tlocrtu u 3 različite boje: zeleno za zatvoreno, crveno za otvoreno, plavo za trenutno zabranjen pristup. |  |  |
| 62 | Podsustav mora omogućiti konfiguracija za koji razinu incidenta će se generirati dokument *Zapis o incidentu.* |  |  |
| 63 | Dokument *Zapis o incidentu* treba sadržavati oznaku statusa dokumenta (primjerice: u obradi, završeno i slično). |  |  |
| 64 | Dokumentima *Zapis o incidentu* putem podsustava mogu pristupiti samo ovlaštene osobe. |  |  |
| 65 | Podsustav mora omogućiti pridruživanje certifikata (SSL) svakom odgovarajućem resursu, pratiti vrstu certifikata, vrijeme dodjele i vrijeme isteka. |  |  |
| 66 | Podsustav mora omogućiti tablični pregled svih certifikata unutar tvrtke uz mogućnost pretraživanja i filtriranja po različitim vrstama kriterija. |  |  |
| 67 | Podsustav mora posebno označavati istekle certifikate ili certifikate koje uskoro ističu. |  |  |
| 68 | Podsustav mora podržavati spajanje na sustav Servertastic u vidu automatskog ili ručnog generiranja novog certifikata. |  |  |
| 69 | Podsustav treba omogućiti praćenje web domena u vlasništvu tvrtke te dodjelu odgovarajućem resursu. |  |  |
| 70 | Podsustav će posebno označiti istekle domene ili domene koji uskoro ističu. |  |  |
| 71 | Podsustav će podržavati spajanje na sustav Servertastic u vidu automatskog ili ručnog generiranja novog certifikata. |  |  |
| 1. **UPRAVLJANJE IMOVINOM I EVIDENCIJA IT OPREME**
 |
| 1 | Postoji jedinstveni podsustav unutar kojeg je moguće upravljanje raznolikim materijalnim resursima tvrtke (npr IT opremom, radnim inventarom, i dr). |  |  |
| 2 | Podsustav ima opciju unosa strukturiranih informacija o materijalima i opremi koje posjeduje tvrtka. |  |  |
| 3 | Podsustav ima opciju unosa strukturiranih informacija o materijalima i opremi koja se nabavlja za potrebe isporuke klijentu. |  |  |
| 4 | Podsustav omogućuje korisniku upravljanje opremom na skladištu tako da može editirati podatke, brisati, izvesti u obliku csv-a. |  |  |
| 5 | Resursi i oprema koja je unesena u sustav tvrtke može imati neograničene setove atributa i kategorije koji ih pobliže opisuju. |  |  |
| 6 | Podsustav treba omogućiti korisniku pokretanje i zaključivanje procesa inventure. |  |  |
| 7 | Za vrijeme trajanja inventure sva skladišta nad kojima se provoditi inventura trebaju dobiti poseban status te će podsustav blokirati sva kretanja resursa/opreme i imovine na skladištu. |  |  |
| 8 | Podsustav treba omogućiti kreiranje inventurnih lista i dodjelu zaposlenicima. Po ispuni inventurne liste korisnik koji je zadužen za ispunu ju ujedno i zaključuje. |  |  |
| 9 | U tabličnom prikazu inventurne liste potrebno je prikazati minimalno: ID, naziv, jedinica mjere, polje za upis zatečenog stanja, bilješka, serijski broj, kod proizvođača, istek jamstva, barkod. |  |  |
| 10 | Kratkoročno zaduživanje i dugoročno zaduživanje pokreće kreiranje dokumenata za zaduživanje/ razduživanje opreme. |  |  |
| 11 | Podsustav treba omogućiti kreiranje kontrolne liste gdje će biti prikazana usporedba stanja zalihe sustava i izbrojanog stanja. |  |  |
| 12 | Podsustav treba grafički prikazati višak, manjak ili identično stanje materijala ili opreme. |  |  |
| 13 | Podsustav treba omogućiti korisniku olakšano usklađivanje zaliha, tako da prikaže viškove i manjkove za svaku stavku. |  |  |
| 14 | Podsustav treba omogućiti korisniku uslužno skladištenje resursa/opreme koja nije njegovo vlasništvo, već pripada klijentu. |  |  |
| 15 | Podsustav treba omogućiti vezanje dokumenata gdje će specificirati resurse/opremu koja se skladišti, početak skladištenja, kraj skladištenja, cijena i definirati primitak resursa, zaduženja i razduženja. |  |  |
| 1. **OPĆENITO O IKT RJEŠENJU**
 |
| 1 | Potrebno je izvršiti detaljnu analizu postojećeg stanja i kreirati dokument o budućoj informatizaciji koji optimalno rješava problematiku promatranih poslovnih područja. |  |  |
| 2 | Korisnici sustava mogu biti i zaposlenici i klijenti. Korisnik s ovlaštenjem može napraviti jednostavnu izmjenu ovlaštenja za ostale korisnike. |  |  |
| 3 | Arhitektura IKT rješenja / sustava mora koristiti relacijsku bazu podataka MySQL ili jednakovrijednu i treba se sastojati od funkcionalnih API servisa koji međusobno komuniciraju.Tehnička izvedba sustava temelji se na korištenju najnovijih tehnologija (NodeJS, C, PHP, JavaScript, ElasticSearch, Redis ili druge jednakovrijedne tehnologije) što će osigurati modularnost, skalabilnost i fleksibilnost. |  |  |
| 4 | Sustav može koristiti vanjske sustave u vidu API servisa (npr. SMS prevodilac protokola). No u slučaju korištenja vanjskih servisa isporučitelj je dužan besplatno osigurati tražene funkcionalnosti i u slučaju otkazivanja rada vanjskih servisa. |  |  |
| 5 | Sustav treba biti web aplikacija implementirana korištenjem responzivnog dizajna, tj. sva sučelja sustava trebaju imati mogućnost prilagođavanja različitim veličinama ekrana (desktop, tablet, mobilni smartphone prikaz). |  |  |
| 6 | Rješenje se isporučuje za rad na web aplikacijskom poslužitelju tako da korisnici mogu sustavu pristupiti iz svojih web preglednika. Sustavu se može pristupiti i pripadajućom mobilnom aplikacijom. |  |  |
| 7 | Sustav u cjelini i svi njegovi podsustavi trebaju težiti ka što većoj fleksibilnosti i dobrim standardima struke, posebno pri upotrebljivosti i proširivosti. |  |  |
| 8 | Stabilnost sustava treba biti na visokom nivou, uz mogućnost brze dijagnostike kroz log datoteke o nastanku kvara, te mogućnošću brzog rješavanja. |  |  |
| 9 | Nadzorna ploča osnovni je alat za pregled i kontrolu podataka u sustavu. Putem nadzorne ploče omogućeno je brzo kretanje po trenutnim odabirom podsustava: aktivnosti obrade, ispitanici, zahtjevi, incidenti, kontrola ulaza i slično. |  |  |
| 10 | Pristup sustavu i/ili dijelovima sustava bazira se na autentifikacija i autorizaciji prema ovlaštenjima korisnika. |  |  |
| 11 | Korisnik treba moći vidjeti (email, in app) podsjetnike koji su definirani u raznim podsustavima. |  |  |
| 12 | Na važnim glavnim tabličnih prikazima potrebno je implementirati mogućnost izvoza podataka. |  |  |
| 13 | Tablični prikazi unutar sustava su konfigurabilni, odnosno imaju mogućnost upravljanja kolonama: uključivanje/isključivanje kolona, izmjenu širine, te mogućnost označavanja i filtriranja prema zadanim parametrima. |  |  |
| 14 | Sustav omogućuje kreiranje izvještaja za svaki pojedini podsustav, primjerice vezano uz imovinu i inventure, upravljanje osjetljivim dokumentima i privolama, informacija vezanih uz incidente odnosno povrede sigurnosti i slično. |  |  |
| 15 | Sustav omogućuje izvoz kreiranih izvještaja u .pdf, .csv ili .xlsx datoteku. Moguća je i analiza na razini dana, tjedna, mjeseca, godine. |  |  |
| 1. **OSTALO**
 |
| 1 | Kroz faze razvoja potrebno je isporučiti dizajn korisničkog i administratorskog sučelja, sustav, provesti testiranje i kontrolu kvalitete sustava, puštanje sustava u rad u testnom okruženju, te pripremu za sljedeću aktivnost - implementaciju rješenja u poslovanje tvrtke Prijavitelja. Implementacija obuhvaća konfiguraciju i prilagodbu rješenja poslovanju Prijavitelja. |  |  |
| 2 | Obuka odnosno edukacija minimalno 10 zaposlenika vezana uz funkcionalnosti i korištenje sustava uključena u izradu sustava. Edukacijom zaposlenici trebaju dobiti znanje o naprednim metodama sigurnosti te korištenju implementiranog sustava za sigurnost kako bi naučeno prenosili ostalim zaposlenicima. |  |  |
| 3 | Sustav se isporučuje s korisničkom dokumentacijom za sve razine ovlaštenja sustava, na hrvatskom jeziku. |  |  |