OPIS PRZEDMIOTU ZAMÓWIENIA

Wzrost wykorzystania e-usług w obszarze zdrowia w Szpitalu Psychiatrycznym w Toszku

Zleceniodawca:

Samodzielny Publiczny
Zakład Opieki Zdrowotnej
Szpital Psychiatryczny
Ulica: Gliwicka 5
44-180 Toszek
NIP: 969-09-46-632
REGON: 000293114
E-mail: info@szpitaltoszek.pl
Telefon:32 233 41 12
Faks:32 233 52 44
www.szpitaltoszek.pl

Spis treści

Założenia do realizacji projektu 5
Opis stanu obecnego 5
Lokalizacja i oddziały szpitala 5
Komórki organizacyjne szpitala 5
Pozostałe komórki organizacyjne szpitala 5
Oprogramowanie cześć Biała 6
Oprogramowanie cześć Szara 7
Uruchomione e-usługi 7
Inwentaryzacja środków trwałych 8
Komputery 8
Serwery 9
Pamięci masowe 9
Przełączniki 10
Urządzenia bezpieczeństwa UTM 10
Ogólne założenia dla rozbudowy oprogramowania 10
Założenia dla publicznie dostępnego Medycznego Portalu Informacyjnego 11
Bezpieczeństwo Systemów 13
Wymagany minimalny poziom dojrzałości e-usług 14
Wytyczne do analizy przedwdrożeniowej 14
Wymagania dotyczące wdrożenia (Uruchomienie e-usług) 14
Informacje dodatkowe 15
Dokumentacja powykonawcza 16
Zakres dostawy 16
Część nr 1 16
Medyczny Portal Informacyjny 17
Aplikacja mobilna e-Obchód 19
e-Zarządzenie Dokumentacją Medyczną 20
e-Ankieta 23
e-Recepta 24
e-Powiadomienia 24
e-Potwierdzenia 24
e-Zwolnienia 24
e-Skierowania 25
Telekonsultacje Lekarz-Pacjent 26
Telekonsultacje Lekarz-Lekarz 30

e-ZLA Pracowników 34
e-Kontrola Kontrahentów 34
Podpis elektroniczny 34
Moduł obsługi podpisu cyfrowego w systemie HIS 35
Zakres i wymagania dla serwisu technicznego 35
Zakres i wymagania dla nadzoru autorskiego 37
Część nr 2 38
Serwer wirutalizacyjny (4 szt.) 38
Macierz dyskowa (1 szt.) 41
Przełącznik 25Gb (1 stack switchowy złożony z min. 2 elementów o poniższych parametrach) 42
Punkty dostępowe Access Point (5szt.) 44
System ochrony i akceleracji aplikacji sieciowych (rozwiązanie programowe) 45
Systemy ochrony w punkcie styku typu UTM (2szt. HA) 49
Część nr 3 53
Tablet (10 szt.) 53
Część nr 4 54
Czytnik do dowodu osobistego (e-Dowodu) – 2 sztuki 54
Część nr 5 54
Laptop (5szt.) 54
Część nr 6 59
Urządzenie wielofunkcyjne (2szt.) 59
Część nr 7 60
Stacja robocza z monitorem (10szt.) 60

Założenia do realizacji projektu

Bezpośrednim celem realizacji projektu jest rozwój e-usług dostępnych dla pacjentów a także dostarczenie szybkich i zautomatyzowanych procesów pozwalających jednostce efektywniej wypełniać cele związane z ochroną i promocją zdrowia.

Projekt zakłada zakup licencji oprogramowania dla modułów e-usług, dostawy sprzętu i oprogramowania towarzyszącego, adaptacje oraz prace wdrożeniowe, które mają na celu uzyskanie w pełni funkcjonalnego rozwiązania pozwalającego na osiągnięcie zakładanych wskaźników.

Opis stanu obecnego

Lokalizacja i oddziały szpitala

Planowana inwestycja będzie realizowana w następującej lokalizacji:

- województwo śląskie,
- powiat gliwicki,
- miasto Toszek,
- ul. Gliwicka 5

Komórki organizacyjne szpitala

Lp.	Nazwa komórki organizacyjnej	Liczba łóżek (miejsc)	Umiejscowienie komórki organizacyjnej
1	Oddział internistyczny VIII	28	Budynek „D”
2	Oddział psychiatryczny ogólny III	225	Budynek „Ł”
3	Oddział psychiatryczny sądowy VI	30	Budynek „S”
4	Oddział psychiatryczny sądowy odwykowy VII	30	Budynek „S”
5	Oddział psychiatryczny sądowy V	30	Budynek „S”
6	Oddział psychiatryczny przewlekły XI	80	Budynek „D”
7	Oddział rehabilitacji psychiatrycznej XVI w Dąbrówce	40	Rezerwat Przyrody Hubertus 44-187 Dąbrówka
8	Oddział detoksykacji alkoholowej XII	25	Budynek „D”
9	Oddział odwykowy alkoholowy XIII	26	Budynek „D”
10	Oddział psychiatryczny sądowy dla nieletnich o wzmocnionym zabezpieczeniu XVII	25	Budynek „ON”
	Razem łóżek:	**539**	

Pozostałe komórki organizacyjne szpitala

Lp.	Nazwa komórki organizacyjnej	Umiejscowienie komórki organizacyjnej
1	Medyczne Laboratorium Diagnostyczne	Budynek „D”
2	Pracownia diagnostyki obrazowej	Budynek „D”

3	Pracownia diagnostyki ultradźwiękowej i USG zabiegowego	Budynek „D”
4	Pracownia diagnostyki kardiologicznej	Budynek „D”
5	Pracownia endoskopii	Budynek „D”
6	Ośrodek rehabilitacyjno-terapeutyczny	Budynek „D”
7	Pracownia psychologiczna	Budynek „O”
8	Apteka Szpitalna	Budynek „D”
9	Izba przyjęć	Budynek „Ł”
10	Zespół Pracowników Socjalnych	Budynek „D”
11	Poradnia zdrowia psychicznego	Budynek „P”
12	Poradnia chorób wewnętrznych – gastroenterologiczna	Budynek „P”
13	Poradnia Medycyny Pracy	Budynek „P”
14	Gabinet diagnostyczno-zabiegowy	Budynek „P”
15	Sekretariat	Budynek „E”
16	Dział Kadr	Budynek „E”
17	Dział Organizacyjny	Budynek „E”
18	Dział Księgowości	Budynek „E”
19	Dział Zamówień Publicznych	Budynek „E”
20	Sekcja Rejestracji i Dokumentacji Chorych	Budynek „M”
21	Pielęgniarka Epidemiologiczna	Budynek „E”
22	Dział Administracyjno-Gospodarczy	Budynek „E”

Oprogramowanie cześć Biała

Jednostka posiada licencje na oprogramowanie AMMS firmy Asseco Poland S.A.

EDM	bez limitu	użytkownik/stanowisko
Izba przyjęć	bez limitu	użytkownik/stanowisko
Oddział	bez limitu	użytkownik/stanowisko
Statystyka medyczna	bez limitu	użytkownik/stanowisko
Kolejki oczekujących	bez limitu	użytkownik/stanowisko
Gruper JGP	bez limitu	użytkownik/stanowisko
Rozliczenia z NFZ	bez limitu	użytkownik/stanowisko

Apteczka oddziałowa	bez limitu	użytkownik/stanowisko
Zlecenia	bez limitu	użytkownik/stanowisko
Apteka	bez limitu	użytkownik/stanowisko
Punkt pobrań	bez limitu	użytkownik/stanowisko
Laboratorium	bez limitu	użytkownik/stanowisko
Laboratorium – aparatura diagnostyczna	8	interfejs
Rejestracja przychodni	bez limitu	użytkownik/stanowisko
Poradnia ambulatoryjna	bez limitu	użytkownik/stanowisko
Pracownia	bez limitu	użytkownik/stanowisko
Zakażenia szpitalne	bez limitu	użytkownik/stanowisko
Żywienie	bez limitu	użytkownik/stanowisko

Oprogramowanie cześć Szara

Kadry	bez limitu	użytkownik/stanowisko
Płace	bez limitu	użytkownik/stanowisko
Grafiki	bez limitu	użytkownik/stanowisko
Finansowo/księgowy	bez limitu	użytkownik/stanowisko
Rejestr sprzedaży	bez limitu	użytkownik/stanowisko
Kasa	bez limitu	użytkownik/stanowisko
Rachunek kosztów	bez limitu	użytkownik/stanowisko
Wycena kosztów normatywnych, wycena procedur medycznych	bez limitu	użytkownik/stanowisko
Środki trwałe i wyposażenie	bez limitu	użytkownik/stanowisko
Gospodarka magazynowa	bez limitu	użytkownik/stanowisko
Informacja zarządcza	bez limitu	użytkownik/stanowisko

Uruchomione e-usługi

e-Rejestracja	bez limitu	użytkownik
e-Kolejka	bez limitu	użytkownik
e-Komunikacja	bez limitu	użytkownik
e-Kontrahent	bez limitu	użytkownik

e-Dokumentacja	bez limitu	użytkownik

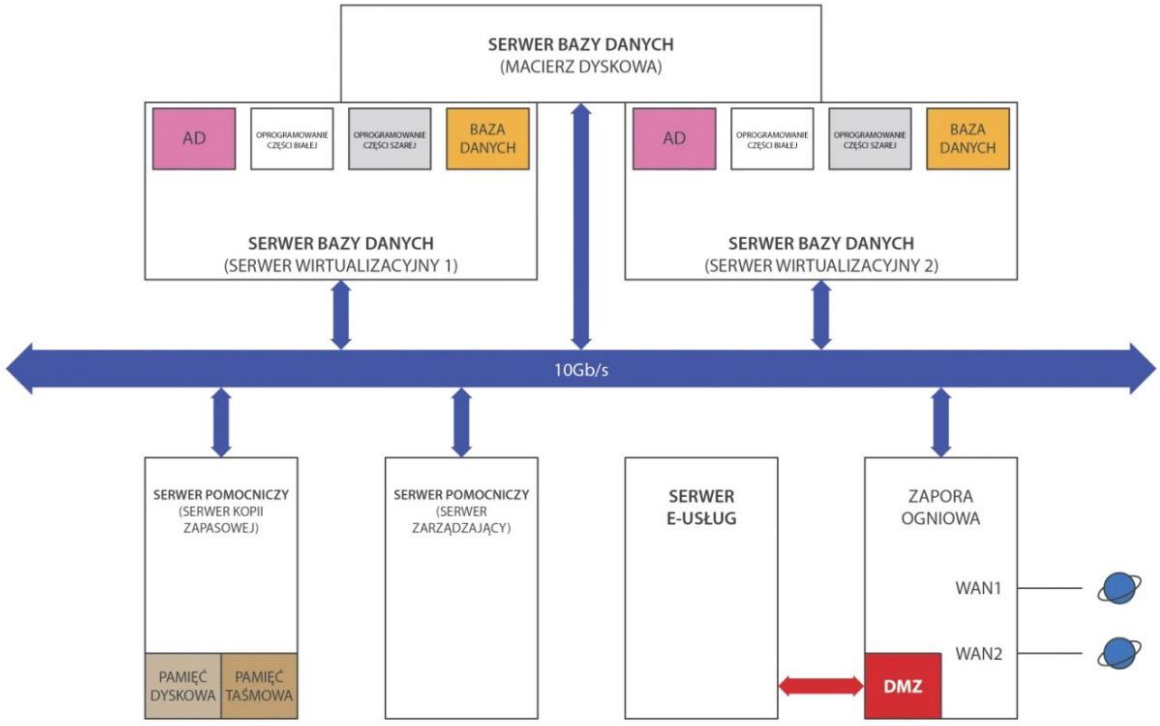
Inwentaryzacja środków trwałych

Obecnie użytkowana serwerownia w SPZOZ Szpitalu Psychiatrycznym w Toszku została uruchomiona w 2015 roku. Powstała w zaadaptowanym byłym budynku archiwum. Prace adaptacyjne objęły remont i adaptację budynku na potrzeby serwerowni. W ramach adaptacji wydzielono pomieszczenie serwerów, pomieszczenie techniczno-kablowe, archiwum oraz pomieszczenia dla obsługi z zapleczem sanitarnym.

Ze względów finansowych ograniczono wykonanie prac instalacyjnych do niezbędnego minimum. Wykonano podłogę techniczną w pomieszczeniu serwerów, uruchomiono system klimatyzacji precyzyjnej oraz system podtrzymania napięcia.

W serwerowni zabudowano zestaw specjalizowanych serwerów niezbędnych do uruchomienia kompleksowego zintegrowanego pakietu systemu informatycznego, którego zadaniem jest obsługa części medycznej (białej) oraz administracyjnej (szarej) szpitala. Do przechowywania danych uruchomiono macierz dyskową pojemności 24 TB. W serwerowni umieszczono również przełączniki główne światłowodowej sieci strukturalnej szpitala.

Jednostka posiada dobrze przygotowane pomieszczenie serwerowni oraz pozwalające na podstawowe funkcjonowanie rozwiązania serwerowe, przestrzeni dyskowej oraz podstawowy poziom cyberbezpieczeństwa zapewniony przez urządzenie UTM na brzegu sieci.



Zmodernizowana w ostatnich latach sieć jest przygotowana do ciągłej i wydajnej pracy personelu medycznego oraz administracji w tym działu informatycznego.

Komputery

Model	**Ilość**
(Gigabyte M61SME-S2)	1
(MSI MS-7808)	1

ACER Veriton L670G	14
DELL Inspiron 3157	1
DELL Latitude E7440	1
DELL Optiflex 7010	1
Dell Optiplex	1
DELL OptiPlex 7010	4
DELL OptiPlex 745	5
Dell Optiplex 755	1
DELL OptiPlex 780	1
Dell Optiplex 980	1
FUJITSU ESPRIMO C5730	1
FUJITSU LIFEBOOK A530	1
HP Compaq 8200 Elite	5
HP Compaq 8200 Elite SFF	2
HP Compaq dc7800p	2
HP ProDesk 400 G2.5 SFF	105
HP Z800	1
Laptop Toshiba	1
Lenovo G780	1
LENOVO ThinkStation E20	2
MAXDATA	1
TRILINE PROFI 31	1
Suma:	**155**

Serwery

Nazwa serwera	Typ	System	RAM	CPU
ESX1	HP ProLiant DL380 Gen9	vmWare Sphere Essential v6.5	256 GB	2x Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
ESX2	HP ProLiant DL380 Gen9	vmWare Sphere Essential v6.5	256 GB	2x Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
BACKUP	HP ProLiant DL380 Gen9	Windows Server 2012 R2	32 GB	Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz
AD	HP ProLiant DL360 Gen9	Windows Server 2012 R2	32 GB	Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz

Pamięci masowe

Nazwa urządzenia	Typ	Pojemność
Napęd taśmowy	HP 1/8 G2 3000 SAS	LTO-5
Macierz	MSA 2040	24TB

Przełączniki

Model	Ilość
M5300-28G Management Switch	9
M5300-52G Management Switch	4
M4300-24X24F Managament Switch	1
M7300-24XF Management Switch	1
Suma:	**15**

Urządzenia bezpieczeństwa UTM

- Fortigate FG-200D
- Fortigate FG-60D

Ogólne założenia dla rozbudowy oprogramowania

Celem projektu jest rozbudowa i unowocześnienie posiadanych systemów informatycznych HIS produkcji firmy Asseco Poland S.A., z pełnym wdrożeniem opisanych modułów e-usług i zapewnienie interoperacyjności z innymi systemami, nie dublując ich funkcjonalności poprzez:

- odbiór danych przez interfejsy udostępnione w platformach P1 w zakresie e-recepty, e-skierowania, zdarzenia medycznego i innych dokumentów oraz powiązanych z nimi słownikami i rejestrami niezbędnymi do ich prawidłowego przekazania do systemu centralnego,
- zapewnić zgodność z interfejsem ZUS PUE w celu automatycznego przekazywania danych z systemu medycznego do ZUS.
- tworzenie elektronicznej dokumentacji medycznej (EDM) zgodnej z narodowym standardem HL7 CDA (opracowanym i opublikowanym przez CSIOZ) umożliwiającym przesyłania różnych elektronicznych komunikatów w bezpieczny sposób pomiędzy programami komputerowymi wykorzystywanymi przez wszystkich dostawców usług zdrowotnych, zgodnie z profilami IHE,
- gwarantowanie bezpieczeństwa systemów i usług poprzez zastosowanie systemów bezpieczeństwa do ochrony w punkcie styku z internetem (NGFW – Next Generation Firewall) oraz dzięki, niezależnemu od aplikacji sieciowej (Medyczny Portal Informacyjny, na którym osadzone zostaną e-usługi), systemowi ochrony aplikacji.
- poprawne funkcjonowanie działających na chwile obecną systemów PACS/RIS, LIS oraz programów kadrowo-płacowych i finansowo-kosztowych (tzw. cześć szara).

W związku z posiadanymi zasobami serwerowymi oraz zasobami informatycznymi zapewniającymi bezpieczne przechowywanie i archiwizację danych jednostka nie przewiduje korzystania z rozwiązań zewnętrznych w chmurze prywatnej. Jeżeli jednak niedostępność zasobów lub czynniki ekonomiczne i finansowe będą wskazywały na potrzebę uruchomienia tego typu usług, archiwa oraz kopie zapasowe będą przetwarzane w chmurze prywatnej z zapewnieniem nie gorszego niż w ramach obecnego systemu poziomu bezpieczeństwa i integralności danych.

Poszerzenie dostępności usług w obszarze elektronicznym zapewni zmniejszenie obciążenia zasobów osobowych jednostki o zakres ujęty w ramach e-usług. Cyfryzacja procesu wpłynie pozytywnie na czas realizacji procesów dzięki otrzymywaniu elektronicznie potwierdzonych danych, rejestrowanych i weryfikowanych w ramach posiadanego systemu informatycznego. Interesariusze (pacjenci) uzyskają dostęp do informacji wcześniej nie udostępnianych elektronicznie z własnych domostw lub dowolnego miejsca na świecie w szybszym, niż do tej pory, czasie. Tak zaprojektowane usługi będą sukcesywnie zwiększać efektywność funkcjonowania jednostki zmniejszając jednocześnie próg błędu wynikający z czynnika ludzkiego – większość danych będzie przekazywana, walidowana i dostarczana w formie

cyfrowej, rejestrowanej i niezmienionej w ramach systemu informatycznego. Pozwala to również na większą niż do tej pory rozliczalność wykonanych prac i zapewnia adekwatną w tym zakresie integralność danych.

Zwiększenie dostępności usług elektronicznych będzie miało pozytywny wpływ na rozwój cyfrowych kompetencji w regionie dostarczanych przez jednostkę usług ochrony zdrowia, co wskazuje, iż projekt wpisuje się w założenia Strategii Rozwoju Społeczeństwa Informacyjnego Województwa Śląskiego.

Założenia dla publicznie dostępnego Medycznego Portalu Informacyjnego

Zaplanowano następujące rozwiązania zgodnie z dokumentem pn. „Standardy dostępności dla polityki spójności 2014-2020":

- Treści nietekstowe, takie jak zdjęcia, rysunki, schematy, wykresy, animacje, nagrania dźwiękowe, kontrolki formularzy i elementy interfejsu graficznego, posiadać będą tam gdzie to możliwe tekst alternatywny;
- Elementy strukturalne, takie jak akapity, nagłówki, listy, tabele, łącza, grupy kontrolek, oraz elementy semantyczne, takie jak wyróżnienia, cytaty, indeksy górne lub dolne, zostaną oznaczone odpowiednimi, przeznaczonymi do tego celu znacznikami HTML;
- Wszędzie tam, gdzie kolejność przedstawianych informacji ma wpływ na ich zrozumienie, zaprogramowana kolejność elementów będzie taka sama jak kolejność ich wyświetlania;
- Instrukcje przekazywane użytkownikowi nie będą opierać się wyłącznie na bodźcach wzrokowych lub słuchowych, takich jak kształt, rozmiar, wzrokowa lokalizacja, orientacja w przestrzeni lub dźwięk;
- Informacje przekazywane za pomocą koloru będą dodatkowo udostępnione także w inny sposób, na przykład w treści tekstowej, w tekście alternatywnym lub programistycznie;
- Współczynnik kontrastu między tekstem a tłem wynosić będzie przynajmniej 4,5:1, a dla dużego tekstu (czcionka co najmniej 18 punktów) - przynajmniej 3:1. Wymaganie to nie dotyczy tekstów dekoracyjnych, będących nieistotną częścią obrazu albo częścią logo lub nazwy własnej produktu (marki);
- Rozmiar tekstu będzie mógł zostać powiększony do 200% bez użycia technologii wspomagających oraz bez utraty treści lub funkcjonalności. Wymaganie nie dotyczy napisów rozszerzonych oraz tekstu w postaci grafiki;
- Do przekazywania informacji wykorzystywany będzie tekst, a nie z graficzna prezentacja tekstu lub z obrazu tekstu. Wymaganie nie dotyczy sytuacji, w których prezentacja tekstu w postaci graficznej jest istotna dla zrozumienia przekazywanej informacji (na przykład gdy tekst jest częścią wykresu lub diagramu). Wymaganie nie dotyczy również tekstu, który jest częścią logo lub nazwy własnej produktu;
- Cały serwis i wszystkie jego funkcje będą obsługiwane za pomocą klawiatury lub interfejsu klawiatury. Można więc użyć alternatywnej klawiatury. Jeśli jakąś funkcję można wykonać przy pomocy myszy lub jakiegoś innego urządzenia wskazującego, to należy zapewnić, by można ją było wykonać również za pomocą klawiatury;
- Jeżeli jakakolwiek funkcja musi być wykonana w określonym czasie (limit czasowy), to należy zapewnić jedną z poniższych opcji:
    - użytkownik wyłączy limit czasowy zanim czas upłynie,
    - użytkownik swobodnie dostosuje limit czasowy (co najmniej o wartość 10 razy większą od wartości domyślnej) zanim czas upłynie,
    - użytkownik jest ostrzegany przed upłynięciem limitu czasowego i ma co najmniej 20 sekund na wydłużenie limitu za pomocą prostej czynności (na przykład wciśnięcia klawisza spacji) oraz może wydłużyć limit co najmniej dziesięciokrotnie;

- Jeśli jakakolwiek informacja będzie automatycznie wprawiana w ruch, będzie przewijana lub zaczynie migotać, trwa dłużej niż 5 sekund i jest prezentowana równolegle z inną treścią, zapewniony zostanie mechanizm dostępny dla użytkownika, który pozwala ją przerwać, zatrzymać lub ukryć, chyba że ruch, przewijanie lub migotanie jest częścią aktywności, w której jest to niezbędne.
- Jeśli jakakolwiek automatycznie aktualizowana informacja jest prezentowana równolegle z inną treścią, należy zapewnić mechanizm dostępny dla użytkownika, który pozwala ją przerwać, zatrzymać lub ukryć albo kontrolować częstotliwość aktualizacji, chyba że automatyczna aktualizacja jest częścią aktywności, w której jest to niezbędne;
- Jeśli informacje w aplikacji internetowej lub na stronie internetowej będą wyświetlane w określonej kolejności istotnej dla zrozumienia tych informacji, to zapewniony zostanie mechanizm, który pozwoli nawigować fokusem zgodnie z tą kolejnością wyświetlania;
- Każde łącze prowadzi do jakiegoś miejsca. Jeśli to możliwe, należy zapewnić łącze tekstowe, które jednoznacznie informuje, dokąd to łącze prowadzi, bez konieczności odgadywania jego celu z kontekstu:
    - opis łącza będzie jednoznacznie wskazywać gdzie nastąpi przekierowanie,
    - ostrzeżenie użytkownika o otwarciu strony w nowym oknie lub zakładce będzie obowiązkowe;
- Zapewniona zostanie widoczność fokusa klawiatury, by użytkownik posługujący się klawiaturą wiedział, jaki element aplikacji internetowej lub strony internetowej jest aktywny;
- Przeniesienie fokusa na dowolny element interfejsu użytkownika nie będzie zmieniało treści w innych częściach strony internetowej lub aplikacji internetowej;
- Zmiany wprowadzane przez użytkownika w elementach interfejsu użytkownika nie będą powodować zmian w innych częściach strony internetowej lub aplikacji internetowej. Zmiany takie mogą być niezrozumiałe przez użytkownika, chyba że zostanie on o nich wcześniej powiadomiony;
- Jeśli w danym serwisie internetowym występować będzie wiele stron lub w danej aplikacji internetowej występować będzie wiele ekranów, to należy zapewnić, by nawigacja po tych stronach i ekranach była konsekwentnie powtarzalna. Zmiany w sposobach nawigacji na różnych stronach tego samego serwisu będą powodować duże utrudnienia;
- Komponenty, które pełnią te same funkcje w danym serwisie internetowym i występują na wielu jego podstronach lub występują w aplikacjach internetowych, będą konsekwentnie i powtarzalnie nazywane i przedstawiane we wszystkich miejscach, w których występują;
- W przypadku formularza wypełnianego przez użytkownika każdy błąd wprowadzania danych, który zostanie wykryty automatycznie, będzie sygnalizowany. Wskazany zostanie błędny element (na przykład poprzez zaznaczenie go innym kolorem) i przedstawiony opis tego błędu w postaci tekstu;
- Elementy interfejsu użytkownika posiadać będą poprawne etykiety (na przykład pole tekstowe, przycisk, lista rozwijana) powiązane z odpowiadającymi im komponentami, w taki sposób aby technologie wspomagające mogły je jednoznacznie rozpoznać;
- Tam gdzie to możliwe wprowadzona zostanie walidacja formularzy; Użytkownik będzie miał możliwość sprawdzenia i korekty wprowadzonych danych;
- Komponenty interfejsu użytkownika (na przykład elementy formularzy, linki, komponenty wygenerowane przez skrypty) będą stworzone tak, by ich nazwa, rola, stan, właściwości oraz wartości były dostępne dla technologii wspomagających.
- Zostanie zapewniona dostępność wszystkich komponentów z jakich zbudowana jest aplikacja lub usługa.

Bezpieczeństwo Systemów

Zgodnie z §20 Rozporządzenia Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz normami dotyczącymi służby zdrowia, projektowany system informatyczny uwzględnia zasadę bezpieczeństwa i będzie on zgodny z normami dotyczącymi służby zdrowia:

System powstały w wyniku niniejszego projektu musi funkcjonować zgodnie z obowiązującymi przepisami prawa w tym również wymogów RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Aby spełnić standardy bezpieczeństwa zostały określone poniższe wymagania:

1. dotyczące uwierzytelniania:
   a) system informatyczny musi posiadać zaimplementowane mechanizmy kontroli dostępu do danych
   b) jeżeli dostęp do danych w systemie posiadają co najmniej dwie osoby, należy zapewnić, aby:
      - w systemie rejestrowany był dla każdego użytkownika odrębny identyfikator,
      - dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
   c) nie należy ponownie przydzielać identyfikatora użytkownika, który utracił uprawnienia do przetwarzania danych,
   d) w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, system musi wymuszać jego zmianę nie rzadziej niż co 30 dni; hasło musi składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
2. dotyczące zabezpieczeń:
   a) system musi posiadać ochronę przed zagrożeniami pochodzącymi z sieci publicznej opartą na fizycznych lub logicznych zabezpieczeniach chroniących przed nieuprawnionym dostępem,
   b) stosuje się środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej,
   c) system musi być zabezpieczony przed:
      - działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
      - utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
3. System zostanie wdrożony zgodnie z najlepszymi praktykami bezpieczeństwa, w zakresie technologii, jaka zostanie zastosowana do jego budowy. Dostarczone przez dostawcę oprogramowania ma zapewnić:
   - wykorzystanie gotowych frameworków bezpieczeństwa np. JAAS w Javie,
   - zastosowanie odpowiednich mechanizmów uwierzytelniania i autoryzacji podczas logowania się do systemu,
   - w kontekście danych medycznych wykorzystanie silnych metod np. bezpieczny podpis elektroniczny,
   - zastosowanie odpowiednich mechanizmów bezpiecznego przechowywania danych – dostęp do danych powinny mieć tylko uprawnione osoby, dane powinny być szyfrowane,

- w przypadku korzystania z aplikacji klient – serwer, szczególnie w modelu innym niż model klasyczny, zabezpieczenie komunikacji np.: poprzez wykorzystanie protokołu SSL (HTTPS),
- na żądanie i automatyczne wylogowywanie się z systemu po określonym czasie nieaktywności użytkownika.

4. Po dokonaniu wdrożenia Wykonawca przekaże wytyczne w formie pisemnej dla administratorów Zamawiającego w zakresie monitorowania pracy serwerów aplikacji.

Wymagany minimalny poziom dojrzałości e-usług

- Aplikacja mobilna e-Obchód (A2A)
- e-Zarządzenie Dokumentacją Medyczną (A2A)
- e-Recepta (A2C) - Poziom dojrzałości: 3
- e-Ankieta (A2C) - Poziom dojrzałości: 4
- e-Powiadomienia (A2C) - Poziom dojrzałości: 5
- e-Potwierdzenia (A2C) - Poziom dojrzałości: 4
- e-Zwolnienia (A2A)
- e-Skierowania (A2A)
- Telekonsultacje lekarz-pacjent (A2C) - Poziom dojrzałości: 5
- Telekonsultacje lekarz-lekarz (A2A)
- e-JEDZ (A2B) - Poziom dojrzałości: 4
- e-Rekrutacja (A2B) - Poziom dojrzałości: 3
- e-ZLA Pracowników (A2A)
- e-Kontrola Kontrahentów (A2A)

Wytyczne do analizy przedwdrożeniowej

Wykonawca jest zobowiązany do przygotowania i dostarczenia w wyznaczonym przez Zamawiającego terminie analizy przedwdrożeniowej.

Analiza przedwdrożeniowa ma na celu opisać sposób wdrożenia wymaganych przez OPZ funkcjonalności tak, aby spełniały one swoje funkcje (ujęte z punktu widzenia personelu Zamawiającego). Funkcjonalności mogą realizować te funkcje bezpośrednio lub pośrednio (wówczas należy wskazać sposób ich realizacji tzn., poprzez lub w ramach jakich funkcjonalności są one realizowane). Analiza przedwdrożeniowa musi obejmować również analizę integracji poszczególnych systemów Zamawiającego oraz sposób i terminy migracji danych z uwzględnieniem przewidywanych przerw w pracy poszczególnych systemów tak, aby Zamawiający mógł przygotować się do tych przerw i odpowiednio zaplanować pracę Szpitala w trakcie tych przerw. Wykonawca winien wskazać nie tylko konieczność zaplanowania przerwy, ale także określić szacowany termin i czas trwania przerwy.

Wymagania dotyczące wdrożenia (Uruchomienie e-usług)

W ramach usług wdrożeniowych Wykonawca zobowiązany będzie wykonać następujące prace związane z wdrożeniem infrastruktury sprzętowej i oprogramowania e-Platformy:

1. Dokonać uruchomienia i konfiguracji urządzeń wymaganych do uruchomienia i realizacji nowych e-usług.
2. Dokonać uruchomienia środowiska produkcyjnego i – jeżeli to konieczne – środowiska testowo-szkoleniowego.
3. Przeprowadzić testy dostarczonych urządzeń i oprogramowania potwierdzające skuteczną realizacje zakładanych funkcjonalności.

4. Wykonanie rozbudowy systemu o funkcjonalności e-usług i funkcjonalności integracji systemu z platformą P1. Wdrożenie dostarczanego oprogramowania musi uwzględniać ciągłość pracy jednostki. Wszelkie przerwy w działaniu systemu wynikające z prowadzonych prac wdrożeniowych muszą zostać uzgodnione i obustronnie zatwierdzone.
5. Przeprowadzić instruktarze dla wskazanego przez jednostkę personelu odpowiedzialnego za realizację określonych e-usług (nie więcej niż 30 osób). Dodatkowo przekazana zostanie instrukcja dla personelu udostępniona w formie elektronicznej dla każdej e-usługi.
6. Przeprowadzić instruktaże dla Administratorów w siedzibie Zamawiającego ze wskazanego zakresu zarządzania e-usługami oraz dostarczonym sprzętem.
7. Opracować i dostarczyć dokumentację powykonawczą.

Informacje dodatkowe

Każdy z Dostawców i Wykonawców ma obowiązek zapoznać się ze wszystkimi częściami Zamówienia (dotyczy wzajemnych relacji pomiędzy dostawą sprzętu, infrastruktury i oprogramowania).

Dostawa oprogramowania w ramach zamówienia, obejmuje dostarczenie kodów licencyjnych lub nośników z programami ze wszelkimi kodami/instrukcjami, które umożliwią jego legalne i poprawne zainstalowanie oraz funkcjonowanie dla wszystkich zakupionych licencji.

Oprogramowanie dostarczone i uruchomione w ramach zamówienia nie będzie wiązało się z koniecznością wprowadzenia zasadniczych zmian obecnej architektury logicznej oraz fizycznej dotychczasowych rozwiązań. **Prace inwestycyjne koncentrują się na rozbudowie systemów o nowe moduły funkcjonalne.**

Wykonawca zobowiązany jest zainstalować, skonfigurować i uruchomić dostarczone przez siebie rozwiązania w środowisku teleinformatycznym udostępnionym przez Zamawiającego.

W przypadku, gdy Wykonawca uzna, że z jakichkolwiek względów (funkcjonalnych, wydajnościowych, bezpieczeństwa, itd.) nie jest w stanie zapewnić poprawności działania dostarczanych przez siebie rozwiązań na w/w infrastrukturze teleinformatycznej, może w takim przypadku dostarczyć dedykowaną infrastrukturę techniczną (np. dedykowany serwer fizyczny). W takim przypadku Wykonawca przedłoży Zamawiającemu szczegółową specyfikację sprzętu wraz z uzasadnieniem konieczności jego wdrożenia. Wykonawca może wdrożyć dodatkową infrastrukturę techniczną tylko za zgodą Zamawiającego. Wykonawca dostarcza infrastrukturę techniczną bez dodatkowego wynagrodzenia ze strony Zamawiającego. Dostarczony przez Wykonawcę sprzęt objęty jest warunkami gwarancji analogicznymi jak całość przedmiotu umowy.

W przypadku gdy Wykonawca uzna, że dla potrzeb instalacji dostarczonych przez siebie rozwiązań informatycznych, wymagana będzie instalacja środowisk informatycznych lub/i licencji oprogramowania wykraczających poza udostępniane przez Zamawiającego, Wykonawca musi dostarczyć we własnym zakresie bez dodatkowego wynagrodzenia wymagane dla dostarczonych rozwiązań niezbędne środowiska informatyczne, dodatkowe oprogramowanie niezbędne do poprawnego funkcjonowania rozwiązań objętych niniejszym postępowaniem, licencje oprogramowania upoważniające do bezterminowego korzystania z dostarczonego oprogramowania oraz wszelkie niezbędne komponenty.

Ilekroć mowa o integracji z posiadanym przez Zamawiającego systemem HIS, wszędzie gdzie to wymagane, Wykonawca zobowiązany będzie dostarczyć właściwe licencje integracyjne upoważniające do bezterminowego korzystania z dostarczonego oprogramowania dla nielimitowanej liczby użytkowników.

W trakcie realizacji przedmiotu zamówienia ma być zachowana ciągłość pracy umożliwiająca bieżące prowadzenie elektronicznej dokumentacji pacjentów, wystawianie w formie elektronicznej niezbędnych dokumentów (m.in. e-skierowanie, e-recepta, e-ZLA), rozliczanie świadczeń z NFZ, gromadzona informacja na temat ubezpieczenia pacjenta (eWUŚ) oraz Kolejek Oczekujących (AP-KOLCE).

Zakres obowiązków Wykonawcy obejmuje również:

- Wypakowanie i utylizacja opakowań.
- Montaż w miejscu przeznaczenia używania (odpowiednie szafy RACK).
- Podłączenie do istniejącej infrastruktury sieci LAN i zasilania.
- Rekonfiguracja istniejącej infrastruktury.
- Prezentacja zasobów macierzowych do nowych hostów (środowisko wirtualne + systemy bazodanowe).

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

Dokumentacja powykonawcza

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierającą opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu. Hasła muszą zostać dostarczone w zamkniętej kopercie i przekazane muszą być protokolarnie wyznaczonemu przedstawicielowi Zamawiającego.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania – w wersji elektronicznej.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Dokumentacja musi być sporządzona w języku polskim. Dokumentacja dotycząca sprzętu oraz przeznaczona dla administratorów systemu może być dostarczona w języku angielskim.

Zakres dostawy

Część nr 1

e-Usługi oraz oprogramowanie towarzyszące

Uwzględnione w projekcie E-usługi prezentowane będą w ramach medycznego portalu informacyjnego, w sekcji pacjenta. Wszystkie E-usługi oraz platforma e-usług musi zostać zaktualizowana do spełniania poniższych wymagań:

- Pełna mobilność – dostępność usługi musi być możliwa z poziomu stacji roboczych i urządzeń mobilnych, w tym tabletów, za pośrednictwem połączeń kablowych szerokopasmowych, bezprzewodowych komórkowych czy WIFI.
  Dodatkowo zostanie dostarczona aplikacja mobilna na urządzenia mobilne zapewniająca dostęp do dokumentacji opisującej leczenie w szpitalu lub przychodni.

- Przyjazny interfejs – możliwość dostosowania interfejsu do wymagań użytkownika tj. wersja kontrastowa, zwiększanie czcionki – ułatwienia dla osób niedowidzących oraz definiowania własnych stylów CSS co pozwoli na modyfikacje interfejsu zorientowanego na użytkownika (UX).
- Wielojęzyczność – możliwość przełączenia z języka polskiego na język angielski z możliwością dalszej rozbudowy w razie potrzeby o kolejne wersje językowe.
- Ciągłość działania – przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, dostępność do realizowanych e-usług.
- Wieloplatformowość – moduł aplikacyjny przystosowany do pracy na platformie wirtualizacyjnej lub w chmurze.
- Wymiana informacji – dzięki EDM, integralności z platformami krajowymi, gotowości do wymiany informacji z platformami regionalnymi dzięki otwartym standardom wymiany danych (HL7).
- Współpraca podmiotów Ochrony Zdrowia – dzięki EDM, posiadanej platformie obsługi kontrahentów oraz telekonsultacjom.

Medyczny Portal Informacyjny

1. System zapewnia przesyłanie danych z wykorzystaniem bezpiecznego kanału komunikacji - powinien umożliwiać szyfrowanie transmisji danych co najmniej pomiędzy komputerem pacjenta (klienta), a pierwszym komponentem systemu, na którym są one przetwarzane.
2. System powinien posiadać dedykowany moduł obsługi uprawnień, pozwalający na tworzenie i przydzielanie uprawnień użytkownikom osobowym, jak i innym systemom informatycznym (np. zintegrowanym z nim aplikacjom).
3. Wymagana jest zgodność interfejsu użytkownika z WCAG 2.1 (ang. Web Content Accessibility Guidelines).
4. System udostępnia graficzny interfejs użytkownika dostosowujący się do wielkości ekranu urządzenia, na którym jest użytkowany. Wymagana jest możliwość użytkowania systemu w przeglądarkach smartfonów, tabletów i komputerów osobistych.
5. Wymagana jest możliwość użytkowania systemu na najnowszych wersjach popularnych przeglądarek internetowych: Google Chrome, Firefox, Microsoft Edge bez konieczności instalacji dodatkowych elementów środowiska uruchomieniowego.
6. Wymagana jest możliwość dostosowywania wyglądu aplikacji w zakresie definiowania własnych stylów CSS co pozwala na projektowanie i modyfikacje interfejsu zorientowanego na użytkownika (UX).
7. System powinien posiadać modułową budowę - preferowana architektura oparta o mikrousługi.
8. Należy zapewnić możliwość skalowania horyzontalnego wybranych modułów systemu (w zależności od obciążenia).
9. System powinien udostępniać interfejs programowy (API) umożliwiający jego ewentualną integrację z innym oprogramowaniem działającym obecnie lub w zaprojektowanym w przyszłości.
10. Architektura systemu powinna pozwalać na wdrożenie go w wariancie wysokiej dostępności (ang. high availability) poprzez równoczesne działanie jego "zapasowej" instancji.
11. Wymagana jest zapewnienie możliwości instalacji systemu zarówno w infrastrukturze jednostki, jak również w zewnętrznym Centrum Przetwarzania Danych (CPD) i/lub chmurze obliczeniowej (w modelu PaaS lub IaaS).
12. Zakłada się dostarczenie gotowych do uruchomienia komponentów systemu wraz z wszystkimi zależnościami i domyślną konfiguracją – preferowane wykorzystanie technologii konteneryzacji.
13. System musi udostępniać interfejs użytkownika w języku polskim i angielskim wraz z możliwością prezentacji nazw słownikowych w obydwu językach.

14. System musi umożliwiać samodzielne utworzenie konta w Medycznym Portalu Informacyjnym.
15. Rejestracja do portalu udostępniana jest pacjentom w postaci odnośnika na stronie internetowej Jednostki Ochrony Zdrowia. Po samodzielnym utworzeniu konta użytkownik posiada dostęp do portalu z określonym poziomem uprawnień.
16. Rejestracja konta użytkownika, który jest lub potencjalnie będzie pacjentem jednostki:
    - system musi umożliwiać rejestracje podstawowych danych pacjenta tj.:
        - imię, nazwisko,
        - dane identyfikacyjne pacjenta: nr PESEL albo numer ewidencyjny lub numer dokumentu tożsamości nadane we wskazanym kraju (w przypadku rejestracji obcokrajowców),
    - system musi umożliwiać rejestrację adresu e-mail użytkownika portalu
    - system musi umożliwiać rejestrację nr telefonu komórkowego użytkownika portalu
    - system podczas rejestracji użytkownika musi wymuszać akceptację regulaminu portalu, oraz zgody na przetwarzanie danych osobowych zgodnie z Ustawą z dnia 10 maja 2018 roku o Ochronie Danych Osobowych.
    - system umożliwia utworzenie konta dla którego:
        - w zależności od ustawień systemu możliwe jest: logowanie przy pomocy podanego adresu e-mail lub wygenerowanej przez system łatwej do zapamiętania unikalnej nazwy użytkownika (np. pierwsza litera imienia + nazwisko + opcjonalnie nr kolejny użytkownika) lub wprowadzonej przez rejestrującego własnej nazwy użytkownika z kontrolą jej unikalności,
        - system umożliwia podanie i powtórzenie hasła do konta oraz weryfikuje poprawność podanego hasła z zadaną polityką.
17. Rejestracja konta użytkownika reprezentującego swojego podopiecznego:
    - system umożliwia rejestrację konta użytkownika poprzez podanie jego imienia, nazwiska, danych kontaktowych (w zależności od przyjętego kanału komunikacji e-mail lub SMS), nazwy użytkownika i hasła,
    - system umożliwia rejestrację danych podopiecznego użytkownika analogicznie do danych pacjenta.
18. System umożliwia weryfikację podanego w czasie rejestracji konta kanału komunikacyjnego:
    - e-mail, poprzez przesłanie na podany adres wiadomości zawierającej odnośnik z wygenerowanym kodem potwierdzenia autentyczności adresu e-mail,
    - SMS, poprzez przesłanie na podany nr telefonu wiadomości zawierającej kod potwierdzenia autentyczności podanego numeru; system udostępnia funkcję umożliwiającą wprowadzenie nr telefonu oraz przesłanego kodu.
19. Blokowanie możliwości zalogowania się użytkownika, który nie potwierdził żadnego kanału komunikacyjnego.
20. System przypisuje zarejestrowanemu użytkownikowi predefiniowane uprawnienia do dostępnych funkcji, po potwierdzeniu kanału komunikacyjnego.
21. Możliwość ustawienia nowego hasła dla konta, dla którego wykonano poprawną weryfikację adresu e-mail lub numeru telefonu polegającą na wprowadzeniu przesłanego kodu potwierdzenia.
22. Potwierdzenie tożsamości pacjenta z wykorzystaniem profilu zaufanego ePUAP.
23. Możliwość samodzielnej autoryzacji (określenie danych dostępowych – login/hasło) użytkownika – pacjenta po poprawnym potwierdzeniu rejestracji.
24. System udostępnia funkcję logowania do portalu, w ramach której, w zależności od przyjętej polityki bezpieczeństwa, mogą być weryfikowane następujące parametry:
    - wymuszenie zmiany hasła po upłynięciu określonego czasu od jego ostatniej zmiany,
    - wymuszenie zmiany hasła użytkowników, którzy pierwszy raz logują się do systemu,

- czasowe zablokowanie konta użytkownika po przekroczeniu określonej liczby nieudanych logowań.

25. System podczas zmiany hasła musi weryfikować jego poprawność względem przyjętej polityki, w ramach której możliwe jest określenie: minimalnej długości hasła, minimalnej liczby wielkich liter, cyfr, znaków specjalnych, liczby niepowtarzających się kolejnych haseł użytkownika.
26. Aktualizacja profilu pacjenta/użytkownika Portalu; możliwość aktualizacji danych kontaktowych: adresu e-mail, nr-telefonu, adresu zamieszkania.
27. Obsługa zdarzeń medycznych
    System integruje się z Platformą P1 w zakresie wymiany Zdarzeń Medycznych, które są przetwarzane w Systemie Informacji Medycznej zgodnie z Ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.
28. System musi umożliwiać z poziomu zintegrowanego systemu medycznego (HIS):
    - założenie konta użytkownika Medycznego Portalu Informacyjnego,
    - rejestrację pacjentów związanych z kontem Medycznego Portalu Informacyjnego (właściciel konta lub jego podopieczni),
    - autoryzację konta użytkownika (potwierdzenie faktu sprawdzenia tożsamości użytkownika Medycznego Portalu Informacyjnego) oraz jego uprawnień do reprezentowania podopiecznych.

Aplikacja mobilna e-Obchód

1. Aplikacja mobilna musi umożliwić pracę użytkownikowi w zakresie uprawnień określonych dla pełnej wersji systemu HIS (dotyczy to dostępu do danych jak i realizacji funkcji)
2. Aplikacja musi umożliwiać pracę w kontekście zalogowanego pracownika
3. Aplikacja musi umożliwić wylogowanie się zalogowanego użytkownika.
4. Musi istnieć możliwość wylogowania użytkownika lub blokowania aplikacji po upływie ustalonego czasu bezczynności aplikacji
5. Aplikacja musi umożliwić podgląd podstawowych danych pacjenta: Nazwisko, Imię, Numer PESEL, status EWUŚ, data urodzenia, wiek, informacje o alergiach
6. Aplikacja musi umożliwiać podglądu podstawowych danych pobytu pacjenta: tryb przyjęcia, data przyjęcia, numer KG, numer sali, rozpoznanie główne, wstępne lub ze skierowania, listę ostatnio zleconych leków, listę zleconych badań, listę ostatnio mierzonych parametrów życiowych
7. Aplikacja musi umożliwić przypisanie pacjenta do określonej sali i łóżka
8. Aplikacja musi umożliwiać przegląd listy pacjentów przebywających na oddziale, w szczególności w podziale na sale oraz pacjentów nie przypisanych do sali.
9. Aplikacja musi umożliwiać przegląd listy pacjentów przebywających na oddziale, przypisanych do zalogowanego lekarza w roli lekarza prowadzącego.
10. Aplikacja mobilna udostępnia funkcjonalność przeglądania statystyk oddziału prezentujących liczbę pacjentów ogółem oraz w podziale na przebywających na oddziale, skierowanych do wypisu oraz czekających na przyjęcie na oddział
11. Historia choroby i dokumentacja medyczna
12. Aplikacja musi umożliwiać przegląd historii choroby, co najmniej w zakresie:
    - rozpoznań ze skierowania, wstępnych oraz końcowych
    - obserwacji lekarskich
    - zestawienie pozostałych elementów historii choroby, w szczególności, danych wywiadu, badania fizykalnego, informacji o stosowanym leczeniu, uzasadnienia przyjęcia
13. Aplikacja musi umożliwiać dodanie wpisów obserwacji lekarskich w historii choroby pacjenta
14. Aplikacja mobilna umożliwia rejestrację, w dokumentacji medycznej pacjenta dowolnej notatki oraz dołączenia notatki głosowej, zdjęcia i krótkiego nagrania video

15. Aplikacja umożliwia podgląd dokumentów dokumentacji medycznej pacjenta typów udostępnionych do przeglądu na aplikacji mobilnej, . W szczególności: Historia Choroby, Karta Informacyjna, Karta Statystyczna
16. Zlecenia
17. Aplikacja musi umożliwić przegląd listy zleconych leków w formie karty zleceń leków
18. Aplikacja musi umożliwić zlecanie podań leków w tym:
    - zlecenie leku z podaną datą końca obowiązywania zlecenia
    - zlecenie leku bez podania daty końca obowiązywania zlecenia
    - zlecenie leku podania jednorazowe (ad hoc)
19. Aplikacja musi umożliwić odnotowanie podania pacjentowi wieloskładnikowej mieszanki leków.
20. Aplikacja musi umożliwić modyfikację zlecenia podania leku, co najmniej w zakresie:
    - wstrzymania (zamknięcia) zlecenia
    - zmiany terminu obowiązywania zlecenia
21. Aplikacja musi umożliwić podgląd listy zleceń diagnostycznych i laboratoryjnych.
22. Aplikacja musi umożliwić podgląd wyników zleceń diagnostycznych i laboratoryjnych.
23. Aplikacja musi umożliwić zlecanie badan diagnostycznych i laboratoryjnych z wykorzystaniem predefiniowanych zestawów badań (panele badań) diagnostycznych i laboratoryjnych.
24. Aplikacja musi uwzględniać uprawnienia zalogowanego użytkownika do zlecania badań diagnostycznych, laboratoryjnych oraz zleceń podań leków.
25. Aplikacja musi umożliwiać zlecanie badań diagnostycznych, laboratoryjnych oraz zleceń podań leków w imieniu innej niż zalogowana osoby
26. Aplikacja musi umożliwiać przeglądanie, rejestrację i modyfikację diet przypisanych pacjentowi minimum z dokładnością do dnia
27. Wyniki i pomiary
28. Aplikacja musi umożliwiać grupową rejestrację wyników pomiarów parametrów życiowych - wprowadzanie kolejno wyników pomiarów dla pacjentów z listy.
29. Aplikacja musi umożliwiać przegląd parametrów życiowych w formie wykresów (dla wartości pomiarów ewidencjonowany jako wartości numeryczne)
30. Aplikacja musi umożliwiać wyszukiwanie pacjenta za pomocą odczytu danych identyfikacyjnych zapisanych w formie kodu kreskowego
31. Aplikacja musi pozwalać na określenie w konfiguracji, minimum wymienionych funkcjonalności (grupy danych) jaka powinna się uruchamiać po odczytaniu danych identyfikacyjnych zapisanych w formie kodu kreskowego:
    - rekord medyczny dotyczący danego pacjenta
    - karta zleceń leków
    - karta wprowadzania pomiarów
32. Czynności pielęgniarskie
33. W zakresie czynności pielęgniarskich aplikacja musi umożliwiać:
    - przegląd, rejestrację i modyfikację diagnoz pielęgniarskich
    - odnotowanie realizacji zaplanowanych procedur pielęgniarskich
    - przegląd przebiegów pielęgniarskich

e-Zarządzenie Dokumentacją Medyczną

1. Śledzenie obiegu dokumentacji medycznej od momentu przyjęcia pacjenta do placówki, jego wypisu oraz w okresie archiwizacji (udostępnienia / wypożyczenia).
2. Kontrola procesu zdawalności dokumentacji medycznej pacjenta z oddziałów do archiwum lub sekcji weryfikacji np. w zakresie monitorowania liczby teczek wypożyczonych i zwróconych.
3. Realizacja zadań zleconych bezpośrednio komórce archiwizującej tj. wypożyczanie dokumentacji, brakowanie.

4. Tworzenie protokołów, zestawień, kart wypożyczeń oraz określenie aktualnej lokalizacji dokumentacji medycznej.
5. Wsparcie pracowników sekcji weryfikacji / archiwum:
    a. automatyczne tworzenie protokołów przeniesienia dokumentacji,
    b. wykaz teczek pacjentów zwróconych z sekcji weryfikacji lub nie przekazanych,
    c. tworzenie wniosków o udostępnienie dokumentacji,
    d. informowanie o stanie teczki pod kątem wypożyczania,
    e. informowanie o aktualnym miejscu przechowywania teczki (nawet po wypisie pacjenta ze szpitala).
6. Automatyczna segregacja i dzielenie teczek wg różnych kategorii informacji.
7. Monitorowanie terminów zwrotów / wykaz przekroczeń terminów.
8. Automatyczne tworzenie spisów zdawczo-odbiorczych.
9. Przyjmowanie dokumentów przychodzących elektronicznych oraz digitalizacja dokumentów papierowych
10. Znakowanie dokumentów za pomocą kodów kreskowych lub QR
11. Cyfryzacja zeskanowanych dokumentów (OCR) z możliwością ręcznej korekty błędów cyfryzacji
12. Opis dokumentu i odpowiednia jego dekretacja
13. Akceptacja dokumentu i wprowadzenie do systemu
14. Automatyczne kierowanie dokumentów do wybranych użytkowników i archiwum, w ściśle określonym czasie i kolejności
15. Śledzenie procesów decyzyjnych związanych z wybranym dokumentem oraz pełna kontrola nad przepływem dokumentu
16. Prowadzenie pełnej ewidencji wyświetleń dokumentu, odczytu informacji oraz zmian wprowadzonych przez pracowników
17. Podgląd stanu dokumentu przez uprawnione osoby
18. Prowadzenie i wydruk książki pocztowej
19. Archiwizacja dokumentów w postaci cyfrowej
20. Automatyczne usuwanie dokumentu po upływie ustawowego czasu przechowywania
21. Repozytorium formularzy i druków do druku i interaktywnych
22. Rejestr dokumentów wychodzących
23. Integracja systemu obiegu dokumentów z istniejącym systemem ERP i HIS

Szczegółowy opis dokumentacji formularzowej

System posiada moduł umożliwiający użytkownikowi samodzielne definiowanie wzorców formularzy przeznaczonych do gromadzenia danych

1. System musi umożliwiać definiowanie formularza, na którym można zaewidencjonować co najmniej dane typu:
    - Liczba
    - Tekst
    - Data
    - Wartość logiczna
    - Wartość słownikowa
    - Obraz
2. Składniki formularza można umieszczać na zakładkach i w sekcjach
3. Składniki formularza można dodawać przy pomocy mechanizmu "Przeciągnij i upuść"
4. System musi zapewniać, by poszczególnym składnikom formularza można przypisać domyślną wartość

5. System musi zapewniać, by w definiowalnych formularzach można było zdefiniować wymagalności wypełnienia wskazanych składników
6. Wydruk formularza
7. Moduł na podstawie wzorca formularza umożliwia zdefiniowanie jego szablonu wydruku.
8. Na szablon wydruku można dodawać dodatkowe elementy (nie będące składnikami wzorca formularza) co najmniej takie jak:
   - etykieta
   - obraz
9. System powinien umożliwiać wykonanie operacji importu/ eksportu szablonów formularzy w standardzie XML

Elektroniczna Dokumentacja Medyczna

1. Możliwość archiwizacji dokumentacji medycznej w postaci elektronicznej.
2. Możliwość archiwacji dokumentów złożonych, wieloczęściowych i przyrostowych np. księgi
3. Możliwość obsługi załączników do dokumentacji
4. Możliwość rejestracji dokumentów elektronicznych generowanych przez system medyczny w repozytorium dokumentacji elektronicznej
5. Możliwość rejestracji dokumentów elektronicznych utworzonych poza systemem HIS, manualna rejestracja dokumentów zewnętrznych
6. Cyfryzacja dokumentu papierowego i dołączanie go do dokumentacji elektronicznej
7. Dostęp do całości dokumentacji przechowywanej w EDM:
   - z poziomu wbudowanych w systemy medyczne mechanizmów
   - z poziomu dedykowanego interfejsu
8. Możliwość eksportu/importu dokumentu elektronicznego do/z pliku w formacie XML. Możliwość eksportu/importu jednocześnie wielu dokumentów.
9. Możliwość złożenia podpisu elektronicznego na dokumencie
10. Możliwość złożenia podpisu elektronicznego na zbiorze dokumentów
11. Możliwość weryfikacji podpisu
12. Możliwość weryfikacji integralności dokumentu
13. Możliwość weryfikacji i czytelnej prezentacji informacji o zgodności podpisu elektronicznego z treścią podpisanego dokumentu.
14. Możliwość wydruku dokumentu
15. Możliwość wyszukiwania dokumentów za pomocą zaawansowanych kryteriów oraz meta danych.
16. Możliwość wersjonowania przechowywanych dokumentów z dostępem do pełnej historii poprzednich wersji.
17. Repozytorium EDM musi umożliwiać:
    - rejestrację dokumentu
    - pobieranie dokumentów w formacie XML (dla dokumentów przechowywanych w formacie HL7 CDA)
    - pobieranie postaci binarnej dla dokumentów w formacie HL7 CDA z osadzoną binarną postacią dokumentu
    - pobieranie dokumentów w formacie PDF (dla dokumentów przechowywanych w formacie PDF)
    - wyszukiwanie materializacji dokumentów
18. System uprawnień pozwalający na precyzyjne definiowanie obszarów dostępnych dla danego użytkownika.
19. Możliwość zarządzania uprawnieniami dostępu do określonych operacji w repozytorium. Przykłady uprawnień systemowych: uruchomienie systemu, zarządzanie uprawnieniami użytkowników, zarządzanie parametrami konfiguracyjnymi, zarządzanie typami dokumentów.

20. Możliwość zarządzania uprawnieniami do wykonywania operacji na poszczególnych typach dokumentów. Przykłady uprawnień do dokumentów: dodawanie dokumentów do repozytorium, odczyt dokumentu, podpisywanie dokumentu, eksport dokumentu, anulowanie dokumentu, wydruk dokumentu itd.
21. Możliwość definiowania nowych typów dokumentów obsługiwanych przez repozytorium dokumentów elektronicznych.
22. Indeksowane powinny być wszystkie wersje dokumentu
23. Indeks powinien uwzględniać rozdzielenie danych osobowych od danych medycznych
24. Możliwość indeksowania dokumentów w celu łatwego jej wyszukiwania wg zadanych kryteriów
25. Indeks dokumentacji powinien być zorientowany na informacje o dokumencie: autor, data powstania, rozmiar, typ itp.
26. System musi umożliwić udostępnianie dokumentacji:
    - w celu realizacji procesów diagnostyczno-terapeutycznych w ZOZ
    - pacjentom i ich opiekunom
    - podmiotom upoważnionym np. prokurator
27. System powinien umożliwiać współpracę z platformą P1 w zakresie:
    - obsługi e-Recept
    - obsługi e-Skierowań
28. System powinien umożliwiać Wymianę Dokumentacji Medycznej w ramach platformy P1 w zakresie:
    - indeksowania dokumentacji w postaci elektronicznej
    - dostępu do dokumentacji zaindeksowanej na platformie
    - udostępniania dokumentacji innym świadczeniodawcom
    - możliwości dołączania pobranej dokumentacji do dokumentacji prowadzonej lokalnie"
    - obsługi Zamówień na dokumentację Medyczną zaindeksowaną na platformie (możliwość zamawiania zbiorów dokumentów zawierających również dokumenty niedostępne w momencie zamówienia ale pobierane w sposób asynchroniczny po zmianie stanu dostępności)
29. Dostarczone rozwiązanie musi być zintegrowane z działającym w szpitalu systemem dziedzinowym HIS w oparciu o API producenta systemu HIS:
30. Rejestracja dokumentów w repozytorium z poziomu systemu HIS
31. Wersjonowanie dokumentów (przekazywanie nowej wersji istniejącego dokumentu)
32. Generowanie dokumentów w formacie PIK HL7 CDA w oparciu o dane źródłowe przekazane z systemu dziedzinowego HIS
33. Wyszukiwanie dokumentów w oparciu o dane indeksowe takie jak: Pacjent, JOS, Autor, Typ dokumentu, Data utworzenia, ID dokumentu
34. Pobieranie dokumentów (w formacie XML lub PDF)
35. Zmiana statusu dokumentów (np. anulowanie dokumentu)
36. Współpracę z innymi systemami dziedzinowymi np. działającym w placówce systemem LIS
37. Rozwiązanie powinno dostarczać aplikację do podpisu elektronicznego komunikującą się z systemem dziedzinowym HIS za pomocą usług sieciowych zgodnie z API producenta systemu HIS

e-Ankieta

1. System musi umożliwiać przeprowadzenie badań satysfakcji pacjentów poprzez udostępnienie ankiet związanych z udzielonymi świadczeniami medycznymi.
2. System musi umożliwiać pacjentom wypełnienie zdefiniowanej ankiety dotyczącej udzielonego świadczenia medycznego.
3. System musi umożliwiać udostępnienie różnych ankiet dla określonych usług medycznych.
4. System musi przesyłać pacjentom wiadomości z prośbą o wypełnienie ankiety z wykorzystaniem wybranego kanału komunikacyjnego (SMS, e-mail, wiadomość portalowa).

System umożliwia uruchomienie ankiety do wypełnienia poprzez kliknięcie odnośnika przesłanego w wiadomości e-mail.

5. System umożliwia interpretację wyników wprowadzonych przez pacjentów ankiet przez personel medyczny szpitala.
6. System musi wspierać prowadzenie profilaktycznych programów zdrowotnych poprzez:
   - możliwość zdefiniowania kwestionariusza zawierającego informacje służące do kwalifikacji pacjenta do programu,
   - udostępnianie kwestionariusza kwalifikacyjnego wskazanej docelowej grupie pacjentów,
   - informowanie pacjentów o możliwości wypełnienia wskazanej ankiety powiązanej z programem profilaktycznym,
   - umożliwienie pacjentowi wypełnienia i przesłania ankiety do personelu kwalifikującego do programu profilaktycznego,
   - automatyczną integrację z systemem HIS w zakresie wysyłania informacji udzielonych przez pacjentów w wypełnionych ankietach z możliwością ich dalszej analizy,
   - umożliwienie przeglądu i kwalifikacji ankiet programów profilaktycznych zaewidencjonowanych przez pacjentów w systemie MPI przez personel szpitala,
   - powiadamianie pacjentów za pomocą wiadomości email/sms/portalowej o pozytywnym lub negatywnym wyniku wykonanej kwalifikacji do programu profilaktycznego.

e-Recepta

1. Usługa umożliwia wysłanie recepty przygotowanej w systemie HIS do rejestru centralnego działającego w ramach projektu P1.
2. Usługa umożliwia pobranie identyfikatorów recepty nadanych przez system centralny: klucz pakietu recept, klucz recepty, kod recepty.
3. Usługa umożliwia sprawdzenie recept wystawionych pacjentowi.
4. Usługa umożliwia wysłanie dokumentu anulowania wystawionej recepty.

e-Powiadomienia

1. System automatycznie wysyła powiadomienia o zdarzeniach medycznych związanych z pacjentem.
2. System umożliwia zapisanie zgody oraz kanałów komunikacji (sms, email) dla opiekuna.
3. System umożliwia wysyłanie powiadomienia bezpośrednio po wystąpieniu zdarzenia.
4. System umożliwia wysyłanie automatycznych powiadomień opiekunom o zdarzeniach (takich jak: przyjęcie, wypis, zaplanowanie terminu, przeniesienie międzyoddziałowe, zlecenie badania, wynik badania) związanych z pacjentem, za pośrednictwem sms, email.
5. Konfiguracja umożliwiająca wskazanie, które zdarzenia (z dostępnych rodzajów) dotyczące zdarzeń medycznych pacjenta są wysyłane do opiekunów.
6. System umożliwia zapisanie w systemie informacji o zgodzie pacjenta na wysyłanie powiadomień do opiekuna w ramach opieki/hospitalizacji.

e-Potwierdzenia

1. Umożliwia pacjentowi łatwe potwierdzenie lub anulowanie wizyty e-mailem lub SMS-em.
2. Pacjent otrzymuje informację o zaplanowanej wizycie wraz z możliwości odesłania zwrotnego SMS z treścią TAK lub NIE potwierdzający aktualność planowanej wizyty.
3. Pacjent otrzymuje informację o wizycie z linkiem aktywnym umożliwiającym potwierdzenie lub odwołanie wizyty.

e-Zwolnienia

1. System musi zapewnić zgodność z interfejsem ZUS PUE, bazującym na usługach sieciowych, umożliwiającym wystawianie oraz korektę zwolnień lekarskich bezpośrednio z poziomu systemów dziedzinowych zewnętrznych względem ZUS dostawców oprogramowania.

2. System musi umożliwiać logowanie do systemu PUE - ZUS bezpośrednio z aplikacji gabinetowej. Logowanie możliwe jest poprzez podpisanie oświadczenia wygenerowanego przez ZUS za pomocą: elektronicznego podpisu kwalifikowanego, certyfikatu wystawionego przez ZUS, podpisu kwalifikowanego w chmurze lub profilu zaufanego ePUAP.
3. System musi umożliwić wylogowanie z systemu PUE - ZUS, w chwili zamknięcia sesji pracy z systemem.
4. System musi umożliwiać wystawienie zaświadczenia lekarskiego w trybie bieżącym. Aplikacja gabinetowa w czasie wystawiania zwolnienia powinna umożliwiać posługiwanie się zarówno danymi lokalnymi jak i danymi pobieranymi z systemu PUE - ZUS.
5. System musi umożliwiać podpisywanie dokumentu zaświadczenia lekarskiego podpisem kwalifikowanym na nośniku fizycznym lub w chmurze, za pomocą ePUAP lub certyfikatem ZUS PUE.
6. System musi umożliwić przekazywanie utworzonych dokumentów zaświadczeń lekarskich do systemu PUE-ZUS.
7. System musi umożliwiać wydruk dokumentu zaświadczenia lekarskiego zgodnie z opublikowanym przez ZUS wzorem.
8. System musi umożliwiać anulowanie zaświadczenia przekazanego do PUE-ZUS (dla zaświadczeń, dla których ZUS dopuszcza taką możliwość).
9. System musi umożliwiać pobranie i rezerwację puli serii i nr ZLA dla zalogowanego lekarza (użytkownika) na potrzeby późniejszego wykorzystania w trybie alternatywnym (np. w sytuacji braku możliwości połączenia się z systemem PUE-ZUS).
10. System musi umożliwić w aplikacji gabinetowej w przypadku braku połączenia z systemem PUE-ZUS, wystawienie zwolnienia w trybie alternatywnym (off-line) w oparciu o zarezerwowaną wcześniej dla bieżącego lekarza (użytkownika) pulę serii i nr ZLA.
11. System musi umożliwić wydruk dokumentu zaświadczenia lekarskiego wystawionego w trybie alternatywnym zgodnie z opublikowanym przez ZUS wzorem zarówno przed jego elektronizacją jak i po elektronizacji.
12. System musi umożliwiać unieważnienie zaświadczenia lekarskiego wystawionego w trybie alternatywnym, jeśli nie dokonano jeszcze jego elektronizacji (nie przesłano go wcześniej do ZUS).
13. System musi umożliwić elektronizację zaświadczenia lekarskiego polegającą na przesłaniu do ZUS zaświadczenia wystawionego wcześniej w trybie alternatywnym.
14. System musi umożliwić zbiorczą elektronizację zaświadczeń lekarskich polegająca na przesłaniu do ZUS zaświadczeń wystawionych wcześniej w trybie alternatywnym.
15. System musi umożliwić anulowanie zaświadczenia przekazanego do PUE-ZUS (da zaświadczeń, dla których ZUS dopuszcza taką możliwość).
16. System musi umożliwiać wystawianie oraz anulowanie zwolnień elektronicznych bezpośrednio w systemie HIS.
17. System musi umożliwiać przegląd danych źródłowych oraz dokumentów zaświadczeń lekarskich wystawionych w lokalnej aplikacji gabinetowej.
18. System powinien umożliwiać wystawianie zwolnień elektronicznych przez asystentów medycznych oraz umożliwiać przekazywanie takich dokumentów do systemu ZUS PUE.
19. System musi umożliwiać podgląd listy poprzednich zwolnień pacjenta zarejestrowanych w ZUS, w tym zwolnień zarejestrowanych w innych placówkach medycznych, z możliwością filtrowania wyników względem daty wystawienia zwolnienia oraz okresu niezdolności do pracy.

e-Skierowania

1. Możliwość wystawienia, przez uprawnionego pracownika medycznego, e-skierowania w systemie lokalnym Usługodawcy, wraz z podpisaniem dokumentu elektronicznym podpisem, zgodnie z wytycznymi CSIOZ.

2. Dokument ten jest podpisywany podpisem elektronicznym, na przykład:
    - certyfikatem ZUS,
    - Profilem Zaufanym,
    - podpisem kwalifikowanym.
3. Pacjent, podczas konsultacji lekarskiej może otrzymać:
    - wydruk informacyjny z danymi niezbędnymi do rejestracji na wizytę.
    - SMSa, w którym podany będzie czterocyfrowy kod dostępowy. W celu realizacji e-skierowania w wybranym podmiocie leczniczym, pacjent podaje kod dostępowy wraz ze swoim numerem PESEL.
    - e-maila, w którym będzie dostępny wydruk informacyjny w postaci pliku .pdf. W celu realizacji e-skierowania w wybranym podmiocie leczniczym, pacjent podczas rejestracji na wizytę udostępnia personelowi placówki telefon / tablet, na którym wyświetlony jest wydruk informacyjny, w celu sczytania kodu kreskowego lub podaje czterocyfrowy kod dostępowy, który znajduje się na wydruku oraz swój numer PESEL.
4. Usługa lokalna umożliwia ewidencjonowanie dodatkowych informacji dotyczących wysłanych danych dostępowych e-skierowania, w szczególności kanału wysyłki i poprawności dostarczenia danych.
5. Usługa lokalna Usługodawcy umożliwia przegląd wystawionych, we wskazanym okresie, e-skierowań w kontekście pacjenta i zapoznanie się z ich bieżącym statusem w P1.
6. Możliwość anulowania e-skierowania u Usługodawcy, u którego wystawiono dokument a dokument pozostaje w statusie 'Wystawione'.
7. Usługa lokalna umożliwia podgląd wersji prezentacyjnej e-skierowania.
8. Usługa lokalna umożliwia wydrukowanie:
    - wersji prezentacyjnej e-skierowania,
    - wersji informacyjnej e-skierowania,
    - informacji o skierowaniu zawierającej identyfikator skierowania oraz kod dostępowy, tj. dokumentów umożliwiających realizację wystawionego e-skierowania.
9. Usługa lokalna Usługodawcy umożliwia obsługę e-skierowań pacjenta, w tym dokonywania zmiany statusu e-skierowania w Systemie P1 przez:
    - przyjęcie do realizacji, w tym wpisanie na listę oczekujących,
    - rezygnację z realizacji e-skierowania,
    - zakończenie realizacji e-skierowania.
10. Usługa lokalna umożliwia wyszukanie wszystkich e-skierowań wystawionych pacjentowi w podmiocie leczniczym niezależnie od jednostki organizacyjnej podmiotu i lekarza wystawiającego.
11. Usługa jest zintegrowana z Platformą P1 w zakresie zapisywania i pobierania przez system lokalny poprawnego dokumentu e-skierowania w Systemie P1.

Telekonsultacje Lekarz-Pacjent

1. System musi udostępniać interfejs programowy (API) umożliwiający integrację z innym oprogramowaniem działającym obecnie lub w przyszłości w Szpitalu.
2. Architektura systemu musi pozwalać na wdrożenie w wariancie wysokiej dostępności (ang. high availability), poprzez równoczesne działanie jego 'zapasowej' instancji.
3. System powinien zostać zaprojektowany w taki sposób, aby z części jego funkcjonalności mogły korzystać inne systemy np. z poziomu Medycznego Portalu Informacyjnego.
4. Interfejs użytkownika musi być zgodny z WCAG 2.1 (ang. Web Content Accessibility Guidelines).
5. System udostępnia graficzny interfejs użytkownika dostosowujący się do wielkości ekranu urządzenia, na którym jest użytkowany. System może być używany w przeglądarkach smartfonów, tabletów i komputerów osobistych.

6. System udostępnia interfejs użytkownika w języku polskim i angielskim wraz z możliwością prezentacji nazw słownikowych w obydwu językach.
7. System musi zapewniać przesyłanie danych w sieci rozległej (pomiędzy uczestnikami telekonsultacji) z wykorzystaniem bezpiecznego kanału komunikacji.
8. System musi zapewniać niezaprzeczalność informacji przesyłanych pomiędzy uczestnikami telekonsultacji.
9. System musi posiadać moduł obsługi uprawnień, pozwalający na tworzenie i przydzielanie uprawnień użytkownikom osobowym, jak i innym systemom informatycznym (np. zintegrowanym z nim aplikacjom).
10. System musi umożliwić rejestrację instytucji – podmiotu leczniczego, będącego stroną w procesach telekonsultacji, w zakresie:
    a. wskazanie personelu (lekarzy) – uczestników procesów telekonsultacji posiadających odpowiednie uprawnienia,
    b. rejestracja danych dostępowych do użytkowanych w danej instytucji systemów informatycznych zintegrowanych z platformą telekonsultacji.
11. System musi umożliwić rejestrację danych personelu – uczestników procesów telekonsultacji, w zakresie:
    a. rejestracja danych osobowych i kontaktowych personelu,
    b. utworzenie użytkowników dla zarejestrowanego personelu oraz określenie uprawnień dla utworzonych użytkowników.
12. System musi umożliwić konfigurację jednostek organizacyjnych podmiotu leczniczego i lekarzy obsługujących telekonsultacje.
13. System zapewnia logowanie pacjentów z uwzględnieniem logowania SSO z Medycznego Portalu Informacyjnego.
14. System umożliwia autoryzację i uwierzytelnienie użytkowników.
15. System umożliwia przeprowadzenie zdalnej konsultacji pomiędzy lekarzem a pacjentem z wykorzystaniem jednego z wybranych kanałów komunikacyjnych:
    a. Audio,
    b. Video,
    c. Czat.
16. System umożliwia planowanie telekonsultacji, w zakresie:
    a. wskazanie jednostki i lekarza,
    b. możliwość wybrania terminu w terminarzu udostępnianym przez e-usługę e-Rejestracja (już funkcjonującego w jednostce).
17. Podczas rezerwowania terminu wizyty system umożliwia pacjentowi wprowadzenie opisu przypadku medycznego.
18. Dla zaplanowanej telekonsultacji pacjent ma możliwość:
    a. dodania załączników,
    b. podglądu załączników.
19. Istnieje możliwość zmiany terminu wizyty przez pacjenta lub lekarza.
20. Pacjent ma możliwość rezygnacji z zaplanowanej konsultacji.
21. Lekarz może odwołać wizytę z podaniem powodu odwołania.
22. Możliwość odrzucenia przez lekarza połączenia zainicjowanego przez pacjenta, z podaniem powodu odrzucenia.
23. Istnieje możliwość zaplanowania przez lekarza kolejnej telekonsultacji dla pacjenta.
24. Pacjent ma możliwość śledzenia na bieżąco statusu konsultacji.
25. Przed rozpoczęciem telekonsultacji pacjent ma możliwość wybrania typu konsultacji (audio, wideo, czat).
26. System udostępnia lekarzowi następujące funkcjonalności:
    a. przeglądanie listy zaplanowanych konsultacji z pacjentami,
    b. możliwość rozpoczęcia telekonsultacji z oczekującym pacjentem.

27. W trakcie telekonsultacji system daje lekarzowi możliwość:
    a. wprowadzenia przez lekarza notatek podczas konsultacji,
    b. podglądu przypadku medycznego i załączników podczas konsultacji,
    c. zamknięcia procesu konsultacji przez lekarza.
28. Lekarz ma możliwość dodania do przypadku medycznego dokumentu z wynikiem konsultacji i zaleceniami dla pacjenta.
29. Lekarz posiada dostęp do wcześniejszych konsultacji i przypadków medycznych pacjenta (ograniczony uprawnieniami).
30. Lekarz ma możliwość śledzenia na bieżąco statusu przypadku medycznego i statusu konsultacji.
31. System umożliwia wysyłanie do pacjenta powiadomień SMS/e-mail o zbliżającej się telekonsultacji.
32. System informuje lekarza o gotowości pacjenta do rozpoczęcia telekonsultacji.
33. System umożliwia prowadzenie konsultacji ad-hoc pomiędzy lekarzem i pacjentem, inicjowanych przez pacjenta.
34. System udostępnia pacjentowi następujące funkcjonalności konsultacji ad-hoc:
    a. pacjent ma możliwość wyboru metody połączenia ad-hoc (video/audio/czat),
    b. pacjent może nawiązywać połączenia audio/wideo/czat z dostępnym lekarzem w dowolnym momencie,
    c. system umożliwia wprowadzenie opisu przypadku medycznego przez pacjenta przez nawiązaniem połączenia.
35. System udostępnia lekarzowi następujące funkcjonalności konsultacji ad-hoc:
    a. lekarz może nawiązać połączenie audio/wideo/czat z dostępnym pacjentem w dowolnym momencie,
    b. istnieje możliwość odrzucenia połączenia przez lekarza z podaniem przyczyny,
    c. system prezentuje listę pacjentów oczekujących na telekonsultacje.
36. Dla wybranych usług medycznych system umożliwia obsługę konsultacji ad-hoc w następujący sposób:
    a. lekarz ma możliwość ustalenia listy pacjentów podlegających telekonsultacji oraz określenia dla nich możliwości śledzenia statusu lekarza,
    b. jeżeli lekarz określił listę telekonsultowanych pacjentów, to pacjent może inicjować konsultacje ad-hoc, jeśli został przez lekarza dodany do tej listy,
    c. jeżeli lekarz umożliwił pacjentowi śledzenie swojego statusu, to system prezentuje pacjentowi status lekarza,
    d. lekarz może rozpoczynać konsultacje ad-hoc z pacjentem, którego dodał do listy telekonsultowanych pacjentów, o ile bieżący status pacjenta w systemie to umożliwia.
37. System integruje się z systemem dziedzinowym HIS w następującym zakresie:
    a. wymagana jest integracja rejestru lekarzy konsultujących zdalnie pacjenta z rejestrem lekarzy w aktualnie posiadanym systemie dziedzinowym HIS, rozumiana jako możliwość rejestracji lekarzy na podstawie danych w aktualnie posiadanym systemie dziedzinowym HIS oraz powiązanie odpowiednich pozycji w tych rejestrach,
    b. wsparcie rejestracji konsultowanych przypadków medycznych na podstawie pobytów/wizyt w systemie dziedzinowym HIS,
    c. automatyczne rejestrowanie wyników badań z systemu dziedzinowego HIS, jako załączników do konsultowanych przypadków medycznych,
    d. każda telekonsultacja posiada odwzorowanie w systemie dziedzinowym HIS (wizyta, pobyt) z możliwością dalszej obsługi (np. wystawianie recept, skierowań, planowanie wizyt stacjonarnych, rozliczenia),
    e. wyniki telekonsultacji są zapisywane w systemie dziedzinowym HIS.
38. System integruje się z repozytorium EDM systemu HIS w zakresie rejestracji dokumentów medycznych jako załączników do konsultowanych przypadków medycznych.

39. System integruje się z Portalem Pacjenta - w szczególności z Kontem Pacjenta umożliwiającym dostęp zarejestrowanym użytkownikom do usługi Telekonsultacji Lekarz-Pacjent.
40. System udostępnia interfejs w postaci niezależnych technologicznie usług (preferowane REST lub WebServices)
41. System musi umożliwiać rejestrację historii zmian danych osobowych pacjentów i personelu medycznego ze wskazaniem użytkownika dokonującego modyfikacji danych.
42. System musi umożliwiać rejestrację historii zmian danych medycznych (informacje opisujące konsultowany przypadek medyczny) ze wskazaniem użytkownika dokonującego modyfikacji danych.

Obsługa pacjenta w gabinecie

1. System musi umożliwiać dostęp do listy pacjentów zarejestrowanych do gabinetu zabiegowego
2. System umożliwia rejestrację faktu rozpoczęcia obsługi wizyty pacjenta w gabinecie (przyjęcie)
3. System musi umożliwić przegląd danych pacjenta, co najmniej, w następujących kategoriach:
   - dane osobowe,
   - podstawowe dane medyczne (grupa krwi, uczulenia, stale przyjmowane leki, choroby przewlekłe, szczepienia),
   - uprawnienia z tytułu umów komercyjnych,
   - historia leczenia (dane ze wszystkich wizyt i pobytów szpitalnych pacjenta),
   - wyniki badań,
   - przegląd rezerwacji pacjenta.
4. Obsługa wizyty obejmuje przegląd, modyfikację i rejestrację danych w następujących kategoriach:
   - informacje ze skierowania,
   - zlecanie badań diagnostycznych i laboratoryjnych, konsultacji, zabiegów,
   - usługi, świadczenia w ramach wizyty,
   - wystawione skierowania,
   - wykonane podczas wizyty procedury dodatkowe
   - wystawianie zaświadczeń i druków na formularzach zdefiniowanych dla wizyty
   - wynik badania
   - możliwość przechwytywania pojedynczych klatek obrazu z kamery lub innego źródła np. aparatu USG i dołączanie go do wyniku badania
5. System umożliwia stosowanie słownika tekstów standardowych do opisu danych wizyt
6. System umożliwia stosowanie „pozycji preferowanych" dla użytkowników, jednostek organizacyjnych w ramach używanych słowników
7. System umożliwia ewidencję wykonania usług rozliczanych komercyjnie.
8. Obsługa zakończenia badania/wizyty:
   - autoryzacja medyczna badania,
   - automatyczne tworzenie karty wizyty/wyniku badania
9. Wgląd w rozliczenia NFZ z tytułu zrealizowanych w trakcie wizyty usług
10. Automatyczna generacja i przegląd Wykazu Zabiegów
11. Obsługa wyników badań:
    - wprowadzanie opisów wyników badań diagnostycznych
    - wprowadzanie opisów wyników badań na definiowalnych formularzach wyników dostosowanych do rodzaju wykonywanego badania
    - autoryzacja wyników badań diagnostycznych
    - wydruk wyniku wg wzoru, jakim posługuje się pracownia
    - wielokrotny wydruk tego samego dokumentu
12. Dla zleceń laboratoryjnych, możliwość odnotowania informacji o pobranym materiale dla pojedynczego badania lub zestawu badań
13. System musi umożliwiać obsługę i wydruk dokumentacji zbiorczej tj.:

- Wykaz Zabiegów
- Wykaz Badań
- Harmonogram przyjęć
- Księga Zdarzeń Niepożądanych
- Księga Ratownictwa

14. System musi umożliwiać tworzenie raportów i wykazów Pracowni
15. Konfiguracja pracy gabinetu
16. System musi umożliwiać rejestrację przypadku medycznego w postaci wersji roboczej, widocznej tylko dla autora tych informacji.
17. System pozwala na dostosowanie modułu do specyfiki pracy gabinetu zabiegowego co najmniej w zakresie:
    -możliwości zdefiniowania elementów menu (zakładek) w zależności od potrzeb użytkownika
    -możliwości zdefiniowania wzorów dokumentów dedykowanych dla gabinetu
    -możliwości wykorzystania zdefiniowanych wcześniej wzorów dokumentów.

Telekonsultacje Lekarz-Lekarz

1. System musi udostępniać interfejs programowy (API) umożliwiający integrację z innym oprogramowaniem działającym obecnie lub w przyszłości w Szpitalu.
2. Architektura systemu musi pozwalać na wdrożenie w wariancie wysokiej dostępności (ang. high availability), poprzez równoczesne działanie jego 'zapasowej' instancji.
3. Wymagana jest niezależność systemowa stacji roboczych, na których uruchamiane są aplikacje klienckie.
4. Interfejs użytkownika musi być zgodny z WCAG 2.1 (ang. Web Content Accessibility Guidelines) przynajmniej w zakresie dostępnym dla zewnętrznych partnerów projektu – lekarzy realizujących telekonsultacje.
5. System udostępnia graficzny interfejs użytkownika dostosowujący się do wielkości ekranu urządzenia, na którym jest użytkowany. System może być używany w przeglądarkach smartfonów, tabletów i komputerów osobistych.
6. System udostępnia interfejs użytkownika w języku polskim i angielskim wraz z możliwością prezentacji nazw słownikowych w obydwu językach.
7. System musi zapewniać przesyłanie danych w sieci rozległej (pomiędzy partnerami telekonsultacji) z wykorzystaniem bezpiecznego kanału komunikacji.
8. System musi zapewniać niezaprzeczalność informacji przesyłanych pomiędzy partnerami telekonsultacji.
9. System musi posiadać moduł obsługi uprawnień, pozwalający na tworzenie i przydzielanie uprawnień użytkownikom osobowym, jak i innym systemom informatycznym (np. zintegrowanym z nim aplikacjom).
10. System musi umożliwić rejestrację instytucji – jednostki ochrony zdrowia, będącej stroną w procesach telekonsultacji, w zakresie:
    - określenie roli instytucji względem innych organizacji: konsultant dla wskazanych organizacji, instytucja konsultowana przez wskazane organizacje,
    - wskazanie personelu (lekarzy) – uczestników procesów telekonsultacji, reprezentujących daną instytucję z określeniem uprawnień (ról: prezenter, ekspert, kwalifikator) rejestrowanej osoby do realizacji określonych operacji w systemie w kontekście danej instytucji
    - rejestracja danych dostępowych do użytkowanych w danej instytucji systemów informatycznych zintegrowanych z platformą telekonsultacji.
11. System musi umożliwić rejestrację danych personelu – uczestników procesów telekonsultacji, w zakresie:
    - rejestracja danych osobowych i kontaktowych personelu,

- utworzenie użytkownika w Systemie Kontroli Dostępu dla rejestrowanej osoby lub przypisanie osoby do istniejącego użytkownika,
- określenie uprawnień (ról) użytkownika powiązanego z rejestrowaną osobą w kontekście wskazanej instytucji reprezentowanej przez tę osobę,
- wskazanie personelu (lekarzy), który może być reprezentowany przez rejestrowaną osobę (np. lekarze, w których imieniu system jest obsługiwany przez sekretarkę medyczną).

12. Integracja z systemem HIS w zakresie:
    - wsparcie rejestracji konsultowanych przypadków medycznych na podstawie pobytów/wizyt w systemie HIS,
    - możliwości rejestrowanie wyników badań z systemu HIS jako załączników do konsultowanych przypadków medycznych,
    - integracja z repozytorium EDM systemu HIS w zakresie rejestracji dokumentów medycznych jako załączników do konsultowanych przypadków medycznych.
13. System musi umożliwiać rejestrację historii zmian danych osobowych pacjentów i personelu medycznego ze wskazaniem użytkownika dokonującego modyfikacji danych.
14. System musi umożliwiać rejestrację historii zmian danych medycznych (informacje opisujące konsultowany przypadek medyczny) ze wskazaniem użytkownika dokonującego modyfikacji danych.
15. System musi umożliwiać rejestrację informacji opisujących przypadek medyczny w postaci wersji roboczych, widocznych tylko dla autora tych informacji.
16. System musi umożliwiać rejestrację danych przypadku medycznego w celu zdalnej konsultacji z ekspertem, w zakresie:
    - rejestracja danych osobowych pacjenta, którego dotyczy przypadek medyczny,
    - rejestracja krótkiego opisu przypadku medycznego,
    - możliwość wskazania rozpoznań opisujących przypadek medyczny,
    - wskazanie instytucji konsultującej przypadek medyczny (w przypadku, gdy jednostka konsultowana powiązana jest z wieloma jednostkami konsultującymi),
    - uzupełnianie danych rejestrowanego przypadku medycznego (dane pacjenta, rozpoznania) na podstawie informacji o pobytach pacjenta zarejestrowanych w zintegrowanym systemie HIS,
    - możliwość rejestracji załączników do przypadku medycznego, możliwość rejestracji załączników dotyczących lub powiązanych z wcześniej zarejestrowanymi (np. nowa wersja załącznika, notatka dotycząca innego załącznika itp.). Załączniki mogą mieć postać:
        - notatek tekstowych,
        - zbiorów danych (np. obrazów, dokumentów) ze wskazanych nośnikach danych; dla zbiorów w standardowych formatach obsługiwanych przez przeglądarki (dokumenty html, obrazy, filmy) należy zapewnić podgląd ich postaci,
        - obrazów radiologicznych w formacie DICOM; należy zapewnić możliwość automatycznego wyszukiwania i dołączania plików DICOM znajdujących się na wskazanym nośniku danych; możliwość podglądu zawartości dołączonych plików DICOM (do podglądu nie jest wymagana jakość diagnostyczna, ale jest wymagana instalacja przeglądarki plików DICOM),
        - dokumentów medycznych w formacie HL7 CDA; należy zapewnić możliwość integracji z użytkowanym Repozytorium EDM systemu HIS w celu wyszukiwania i pobierania załączanych dokumentów medycznych.
    - automatyczne uzupełnianie danych przypadku medycznego na podstawie meta danych znajdujących się we wskazanym pliku DICOM,
    - automatyczne uzupełnianie danych przypadku medycznego na podstawie danych odczytanych z nagłówka dokumentów medycznych w postaci HL7 CDA.
17. W zakresie planowanie telekonsultacji przypadku medycznego, system zapewnia:

- możliwość zaakceptowania wskazanego przypadku medycznego do telekonsultacji przez instytucję konsultującą; automatyczna akceptacja przypadku medycznego w przypadku rozpoczęcia realizacji procesu telekonsultacji,
- możliwość zaplanowania telekonsultacji w formie audio lub wideokonferencji – wskazanie planowanej daty i godziny oraz uczestników telekonsultacji,
- możliwość anulowania wcześniej zaplanowanej telekonsultacji
- możliwość przypisania przypadku medycznego wskazanym osobom reprezentującym instytucję konsultującą (ekspertom),
- możliwość odrzucenia wskazanego przypadku medycznego z procesu telekonsultacji ze wskazaniem przyczyny odrzucenia,
- możliwość anulowania wskazanego przypadku medycznego przez prezentera (przedstawiciela instytucji rejestrującej przypadek medycznych) z podaniem przyczyny anulowania telekonsultacji.

18. W zakresie realizacji telekonsultacji przypadku medycznego, system zapewnia:
    - możliwość przeglądu kompletnych informacji dotyczących przypadku medycznego; możliwość pobrania załączników i ich przeglądu z wykorzystaniem zewnętrznych narzędzi dostępnych na stacji roboczej (np. przegląd obrazów DICOM z wykorzystaniem systemów radiologicznych zapewniających wymaganą dla diagnostyki jakość prezentacji),
    - możliwość rejestracji załączników do przypadku medycznego przez ekspertów konsultujących przypadek medyczny (w formie analogicznej do rejestracji załączników dołączanych przez prezenterów przypadku medycznego),
    - prowadzenie telekonsultacji zarejestrowanego przypadku medycznego w formie audio lub wideo konferencji,
    - automatyczna rejestracja przypadku medycznego w przypadku rozpoczęcia audio lub wideokonferencji (telekonsultacje w trybie pilnym),
    - zakończenie telekonsultacji przez eksperta z wprowadzeniem podsumowania konsultacji przypadku medycznego.
19. System musi informować zainteresowanych uczestników procesu telekonsultacji o zdarzeniach w systemie w formie komunikatów w systemie oraz zasubskrybowanych wiadomości e-mail lub SMS. System musi informować o następujących zdarzeniach:
    - zainteresowanych ekspertów o zarejestrowaniu, modyfikacji danych i anulowaniu przypadków medycznych do telekonsultacji,
    - zainteresowanych prezenterów o zaakceptowaniu, odrzuceniu i zakończeniu konsultacji przypadków medycznych w procesie telekonsultacji,
    - zainteresowanych ekspertów o przypisaniu do konsultowania danych przypadków medycznych,
    - uczestników telekonsultacji w formie audio i wideo konferencji o zaplanowaniu i zbliżających się terminach zaplanowanych telekonsultacji.

Integracja z RIS/PACS

1. Integracja z wykorzystaniem standardu HL7
2. Segmenty wspólne dla komunikatów wysyłanych przez HIS i RIS
3. Segment MSH - nagłówek komunikatu obejmujący:
    - kod systemu nadawcy
    - kod systemu adresata
    - data i czas utworzenia komunikatu
    - typ komunikatu
    - unikatowy identyfikator komunikatu
    - tryb interpretacji komunikatu
    - wersja standardu HL7

- potwierdzenia: transportowe i aplikacyjne
- stosowany system kodowania znaków
- język komunikacji

4. Dane przesyłane z systemu HIS
5. Segment PID - dane demograficzne pacjenta obejmujące:
   - PESEL
   - Imiona i nazwisko pacjenta, nazwisko rodowe
   - identyfikator pacjenta
   - data urodzenia
   - płeć
   - adres
6. Segment PV1 - informacje o wizycie lub pobycie pacjenta, obejmujący:
   - rodzaj pobytu: pobyt na IP, wizyta ambulatoryjna, hospitalizacja
   - jednostka organizacyjna
   - rodzaj świadczenia
   - identyfikator pobytu, np. nr księgi
7. Segment IN1 - informacje o ubezpieczeniu pacjenta obejmujące:
   - identyfikator płatnika
   - rodzaj skierowania
8. Segment ORM^O01 - dane zlecenia obejmujące:
   - nr zlecenia
   - planowana data wykonania, pilność
   - datę i czas zlecenia
   - dane osoby zlecającej
   - identyfikator zlecanego badania
   - rozpoznanie ze zlecenia
   - komentarz do zlecenia
   - dane badania (kod i nazwa badania)
9. Anulowanie zlecenia
10. Modyfikacja zlecenia
11. Dane przesyłane z systemu RIS
12. Segment ORU^R01 - wynik obejmujący:
    - status wyniku
    - dane zlecenia
    - kod wykonanego badania
    - datę wykonania
    - dane personelu wykonującego: lekarz wykonujący, lekarz opisujący, lekarz konsultujący, technik, osoba autoryzująca
    - wartość wyniku
13. Odnośniki (załączniki)do wyników badań
14. Miniatury obrazów
15. Wyniki badań dozleconych (dodatkowych)
    - dane personalne pacjentów (nazwisko, imię, PESEL, miejsce zamieszkania)
    - dane zlecenia (numer zlecenia, techniczny identyfikator zlecenia, jednostka zlecająca, lekarz zlecający)
    - dane badania (kod i nazwa badania)
16. Przekazywanie zleceń drogą elektroniczną wraz z danymi skierowania oraz danymi osobowymi pacjenta
17. Przesyłanie do systemu HIS informacji o terminie umówienia badania.
18. Automatyczne odsyłanie do systemu HIS opisu badania zleconego elektronicznie.
19. Możliwość anulowania/odrzucenie zlecenia wysłanego z systemu HIS po stronie RIS.

20. Śledzenie statusu realizacji zlecenie po stronie HIS.
21. Możliwość przesyłania linków do wyników badań w systemie RIS (dostęp on-line do wyników wykonanych w systemie RIS)
22. Automatyczne uzupełnianie danych rozliczeniowych NFZ w systemie HIS po odesłaniu wyników badania z systemu RIS.
23. Automatyczne rozsyłanie komunikatów o zmianie danych osobowych pacjenta w systemie HIS
24. Dostęp z systemu RIS do badań gromadzonych w systemie HIS
25. Dostęp z systemu RIS do historii leczenia pacjenta
26. Dostęp z systemu RIS do rejestru pacjentów w systemie HIS z celu umówienie na badanie.
27. Możliwość dopisanie pacjenta po stronie HIS podczas rejestracji pacjenta w systemie RIS
28. Wgląd z systemu RIS do słowników systemów HIS instytucji kierujących, lekarzy kierujących systemu możliwością wprowadzenie, modyfikacji pozycji słownika.
29. Możliwość zapisu informacji w systemie HIS o umówionym/wykonanym badaniu w systemie RIS
30. Z poziomu RIS dopisanie pacjenta do kolejki oczekujących obsługiwanej w systemie HIS

e-ZLA Pracowników

Importowanie danych z Platformy Usług Elektronicznych ZUS do modułu Kadry-Płace. Usługa umożliwia automatyczne pobranie raportu z PUE ZUS dla wystawionych zaświadczeń e-ZLA pracowników szpitala i zaimplementowanie danych do modułu Kadry i Płace. W związku z tym uzyskuje się poprawę komfortu obsługi kadrowej poprzez skrócenie czasu generacji danych do systemu księgowo-płacowego oraz automatyzację procesu pobierania danych o zwolnieniach pracowników-odejście od pojedynczych plików CSV.

e-Kontrola Kontrahentów

Biała Lista Podatników

Usługa oferująca kompleksowe rozwiązanie w obszarze weryfikacji obecnych i przyszłych Kontrahentów.

Z uwagi na wprowadzane nowe wymogi prawne dotyczące konieczności wielokrotnego sprawdzania aktywnych płatników VAT i powiązanych z nimi numerów kont bankowych jest to rozwiązanie oparte na automatycznym pobieraniu danych z bazy CEIDG/REGON oraz z tzw. Białej Listy Podatników VAT. Umożliwi to Użytkownikowi:

- pobranie danych Kontrahenta przy zakładaniu kartoteki w momencie jego rejestrowania,
- weryfikację Kontrahenta jako aktywnego płatnika VAT wraz z zapisem daty jego weryfikacji
- sprawdzenie czy dla danego numeru NIP Kontrahenta przypisany dla niego rachunek bankowy jest obowiązujący w dniu weryfikacji w bazie białej listy podatników,
- weryfikację poprawności rachunku podczas generowania przelewu w dniu jego generacji.

Podpis elektroniczny

Wykonawca zobowiązany jest do dostarczenia puli minimum 50 licencji na podpis cyfrowy:

- ważność puli 60 miesięcy
- Zamawiający ma prawo, w uzgodnieniu z Wykonawcą, do przypisania i usunięcia z puli podpisów określonych użytkowników (zmiana ta jest dopuszczalna co 12 miesięcy)
- podpis musi umożliwiać autoryzację dokumentacji zgodnie z obowiązującym prawem
- dostarczony podpis elektroniczny, umożliwia jego wykorzystanie do podpisywania dokumentów, bez użycia fizycznej karty i nośnika z certyfikatem

Wykonawca zobowiązany jest do dostarczenia czterech systemów do autoryzacji dokumentów za pomocą podpisu odręcznego:

1. Urządzenie ma wyświetlać formularz elektroniczny w takiej formie jak wersja wydrukowana.
2. Urządzenie ma posiadać rozdzielczość Full HD (1920x1080) i przekątną co najmniej 10 cali.
3. Ekran powinien mieć funkcję powiększania, zmniejszania i przesuwania wyświetlanego formularza gdyby ten był na tyle duży że w całości nie był by czytelny.
4. Ekran dotykowy musi posiadać czułość co najmniej 1000 poziomów nacisku.
5. Ekran jest na stałe połączony z komputerem co pozwala na digitalizację dokumentu w czasie rzeczywistym.
6. Odręczny podpis z tego ekranu powinien być w systemie przechowywany jako grafika oraz informacje zawierające behawioralne cechy grafologiczne.
7. Urządzenie ma mieć możliwość wyświetlania różnych treści, a nie tylko podpisywane dokumenty.
8. Dedykowany rysik do tego urządzenia powinien mieć możliwość przymocowania go na stałe oraz w razie awarii samego rysika jego wymiany.
9. Do urządzenia powinna być dostarczona licencja umożliwiająca pełną integrację z użytkowanym system HIS

Moduł obsługi podpisu cyfrowego w systemie HIS

1. Rozwiązanie powinno dostarczać aplikację do podpisu elektronicznego komunikującą się z systemem dziedzinowym HIS za pomocą usług sieciowych zgodnie z API producenta systemu HIS
2. Podpis cyfrowy umożliwia podpisywanie dokumentów elektronicznych:
   - dając pewność autorstwa dokumentu (autentyczność pochodzenia),
   - utrudniając wyparcie się autorstwa lub znajomości treści dokumentu (niezaprzeczalność),
   - pozwalając wykryć nieautoryzowane modyfikacje dokumentu po jego podpisaniu
3. System musi umożliwiać złożenie podpisu cyfrowego na przekazanych dokumentach oraz zapewnia:
   - możliwość podpisywania pojedynczych dokumentów,
   - możliwość podpisywania grupy dokumentów z jednokrotnym zapytaniem o PIN,
4. System musi umożliwiać przegląd podpisywanych dokumentów:
   - przegląd listy podpisywanych dokumentów (dla podpisywania grupowego),
   - podgląd podpisywanych dokumentów XML.
5. System musi umożliwiać podpisywanie elektronicznej dokumentacji medycznej przetwarzanej w Repozytorium EDM, w szczególności:
   - rejestrację w Repozytorium EDM informacji o złożeniu podpisu,
   - składanie podpisu cyfrowego oraz rejestrację sygnatury dokumentu w Repozytorium EDM
6. System umożliwia złożenie podpisu elektronicznego z wykorzystaniem następujących metod:
   - podpis z wykorzystaniem dowodu osobistego z warstwą elektroniczną (tzw. podpis osobisty)
   - kwalifikowany podpis elektroniczny z wykorzystaniem fizycznych kart kryptograficznych
   - kwalifikowany podpis elektroniczny z wykorzystaniem kart wirtualnych (tzw. podpis w chmurze)
   - podpis elektroniczny złożony za pośrednictwem certyfikatu ZUS
   - podpis elektroniczny złożony za pośrednictwem platformy ePUAP
7. System powinien umożliwić prowadzenie centralnego rejestru certyfikatów podpisu elektronicznego, pozwalającego na składanie podpisu elektronicznego na dowolnej stacji roboczej podłączonej do systemu bez konieczności przechowywania kopii certyfikatów lokalnie na stacjach roboczych.

Zakres i wymagania dla serwisu technicznego

1. W ramach opieki serwisowej oprogramowania aplikacyjnego Wykonawca zapewnia:

a) Instalowanie i serwisowanie aktualnych wersji oprogramowania aplikacyjnego będącego przedmiotem zamówienia

b) Usuwanie awarii oprogramowania aplikacyjnego będącego przedmiotem zamówienia,

c) Bieżące optymalizowanie konfiguracji oprogramowania aplikacyjnego, uwzględniając potrzeby Zamawiającego,

d) Pomoc w awaryjnym odtwarzaniu, na wniosek Zamawiającego, stanu oprogramowania aplikacyjnego i zgromadzonych danych archiwalnych, poprawnie zabezpieczonych na odpowiednich nośnikach,

e) Doradztwo w zakresie rozbudowy środków informatycznych,

f) Dokonywanie ponownych instalacji oprogramowania w przypadkach rozbudowy infrastruktury informatycznej Zamawiającego

g) Korzystanie z konsultacji telefonicznych (Hot-Line)

h) Prowadzenie rejestru kontaktów z Zamawiającym, obejmującego wizyty serwisowe i wykonane czynności, w tym zmiany konfiguracji oprogramowania

2. Opieka serwisowa może być świadczona zdalnie za pomocą łączy lub w siedzibie Zamawiającego.

3. Świadczenie opieki serwisowej odbywać się będzie w godzinach od 8:00 do 16:00 od poniedziałku do piątku. Czas reakcji serwisu na zgłoszoną awarię wynosi 24 h. Wizyty serwisowe wymagające interwencji w siedzibie Zamawiającego odbywać się będą w ciągu 48 godzin od momentu zgłoszenia awarii przez Zamawiającego.

   W przypadku, gdy zgłoszenie błędu zostanie przyjęty przez Wykonawcę:
   a. w godzinach pomiędzy 08:00 a 16.00 – traktowane jest jak przyjęte danego dnia;
   b. w godzinach pomiędzy 16.00 a 24.00 – traktowany jest jak przyjęty o godz. 8.00 następnego dnia;
   c. w godzinach pomiędzy 0.00 a 8.00 - traktowany jest jak przyjęty o godz. 8.00 danego dnia;
   d. w sobotę, niedzielę i święta - traktowany jest jak przyjęty o godz. 8.00 następnego dnia roboczego dnia;

4. W przypadku tzw. błędu krytycznego, tj. takiego, który uniemożliwia użytkowanie Oprogramowania Aplikacyjnego (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego:

   a. czas dokonania naprawy wyniesie do 3 dni roboczych od chwili rozpoczęcia czynności serwisowych;
   b. w przypadku wystąpienia „błędu krytycznego” Wykonawca może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem błędu krytycznego; w takim przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły.

   W pozostałych przypadkach, określanych jako „błędy zwykłe”:

   a. czas naprawy wyniesie do 30 dni roboczych od chwili rozpoczęcia czynności serwisowych;

5. Zgłoszenie błędu przez Zamawiającego odbywać się będzie poprzez witrynę internetową Centralnego Help-Desku Wykonawcy www. ……; w razie trudności z

rejestracją zgłoszenia na w/w witrynie internetowej, Zamawiający może dokonać zgłoszenia telefonicznie (z zastrzeżeniem niezwłocznego potwierdzenia zgłoszenia poprzez witrynę internetową Centralnego Help-Desk'u, e-mail lub faks) pod numerem telefonu: **.....** lub za pomocą poczty elektronicznej na adres ……..@....., opcjonalnie faksem na numer ……..; wypełnienie jednego formularza może dotyczyć tylko jednego rodzaju błędu występującego w konkretnym module.

Zakres i wymagania dla nadzoru autorskiego

W ramach nadzoru autorskiego Wykonawca zapewnia nadzór autorski producenta:

1) udostępnienie poprawek do Oprogramowania Aplikacyjnego, w przypadku stwierdzenia przez Zamawiającego błędu Oprogramowania Aplikacyjnego (tzn. nie spowodowanego przez Zamawiającego powtarzalnego działania Oprogramowania Aplikacyjnego niezgodnie z jego dokumentacją):

   a. w przypadku tzw. błędu krytycznego, tj. takiego, który uniemożliwia użytkowanie Oprogramowania Aplikacyjnego (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego:

      (1) czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego „błędu krytycznego") wynosi 1 dzień roboczy;

      (2) czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 3 dni roboczych od chwili rozpoczęcia czynności serwisowych;

      (3) w przypadku wystąpienia „błędu krytycznego" Wykonawca może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem błędu krytycznego; w takim przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły;

   b. w pozostałych przypadkach, określanych jako „błędy zwykłe" - błędy Oprogramowania Aplikacyjnego inne niż błędy krytyczne:

      (1) czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego błędu zwykłego) wynosi do 15 dni roboczych;

      (2) czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 60 dni roboczych od chwili rozpoczęcia czynności serwisowych;

   c. zgłoszenie błędu przez Zamawiającego odbywać się będzie poprzez witrynę internetową Centralnego Help-Desku Wykonawcy www. ……; w razie trudności z rejestracją zgłoszenia na w/w witrynie internetowej, Zamawiający może dokonać zgłoszenia telefonicznie (z zastrzeżeniem niezwłocznego potwierdzenia zgłoszenia poprzez witrynę internetową Centralnego Help-Desk'u, e-mail lub faks) pod numerem telefonu: **.....** lub za pomocą poczty elektronicznej na adres ……..@....., opcjonalnie faksem na numer ……..; wypełnienie jednego formularza może dotyczyć tylko jednego rodzaju błędu występującego w konkretnym module;

(1) w przypadku, gdy zgłoszenie błędu zostanie przyjęty przez Wykonawcę:
   (a) w godzinach pomiędzy 08:00 a 16.00 – traktowane jest jak przyjęte danego dnia;
   (b) w godzinach pomiędzy 16.00 a 24.00 – traktowany jest jak przyjęty o godz. 8.00 następnego dnia;
   (c) w godzinach pomiędzy 0.00 a 8.00 - traktowany jest jak przyjęty o godz. 8.00 danego dnia;
   (d) w sobotę, niedzielę i święta - traktowany jest jak przyjęty o godz. 8.00 następnego dnia roboczego dnia;

2) wprowadzanie zmian w Oprogramowaniu Aplikacyjnym, w zakresie dotyczącym istniejącej funkcjonalności Oprogramowania Aplikacyjnego objętego niniejszą Umową, w zakresie wymaganym zmianami powszechnie obowiązujących przepisów prawa lub przepisów prawa wewnętrznie obowiązujących Zamawiającego, wydanych na podstawie delegacji ustawowej, z zastrzeżeniem, że Wykonawca zobowiązany jest do:

   i) przekazania Zamawiającemu informacji o nowych wersjach Oprogramowania Aplikacyjnego, co odbywać się będzie poprzez opublikowanie odpowiedniego komunikatu na witrynie Centralnego Help-Desku;

   ii) udostępniania uaktualnień Oprogramowania Aplikacyjnego (nowych wersji Oprogramowania Aplikacyjnego),

3) udostępnienie Internetowego Portalu Szkoleniowego, zawierającego pakiet szkoleń z obsługi Oprogramowania Aplikacyjnego.

Zamawiający wymaga minimum 600 h opieki serwisowej w czasie 60 miesięcy (łączna ilość godzin serwisowych, konsultacji itp.). Ostateczną liczbę godzin opieki serwisowej określa wykonawca jako jedno z kryterium oceny ofert.

Część nr 2

Serwer wirutalizacyjny (4 szt.)

1. Obudowa max 1U do instalacji w standardowej szafie RACK 19”, dostarczona wraz z szynami i prowadnicą kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3. Chipset: dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
4. Procesor: procesor min. szesnastordzeniowy klasy x86 przeznaczony do pracy z zaoferowanym serwerem. Procesor umożliwiający osiągnięcie wyniku min. 259 punktów w teście SPECrate2017_int_base dostępnym na stronie ww.spec.org dla dwóch procesorów
5. Pamięć RAM: min 512GB DDR4 RDIMM 3200MT/s. Na płycie głównej powinno znajdować się min. 16 slotów przeznaczonych do instalacji pamięci, umożliwiających obsługiwać do 1TB pamięci RAM. Zabezpieczenie pamięci: Memory Health Check, Memory Page Retire
6. Interfejsy sieciowe: min 2 porty Gigabit Ethernet w standardzie BaseT
7. Interfejsy dodatkowe: cztery interfejsy sieciowe 25Gb Ethernet w standardzie SFP28
8. Kabel direct attach SFP28-SFP28 25Gb o długości min. 3m - 4 szt.
9. Zainstalowane dwa dyski hot-swap M.2 SATA o pojemności min. 240GBz możliwością konfiguracji RAID1
10. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
11. Grafika: zintegrowana karta graficzna pracująca z rozdzielczością min 1600x900
12. Wbudowane porty: min. port USB 2.0 oraz port USB 3.0, port VGA
13. Zasilanie: redundantne zasilacze HotPlug o mocy min 800W.

14. Moduł TPM 2.0 V3. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. Możliwość wymazywania danych ze znajdujących się dysków wewnątrz serwera – niezależnie od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
15. Karta zarządzania: zdalny dostęp do graficznego interfejsu Web karty zarządzającej, szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, możliwość podmontowania zdalnych wirtualnych napędów, wirtualną konsolę z dostępem do myszy, klawiatury, wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH, możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz, możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, integracja z Active Directory, wsparcie dla automatycznej rejestracji DNS, wsparcie dla LLDP, wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, możliwość podłączenia lokalnego poprzez złącze RS-232, możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy, monitorowanie zużycia dysków SSD, automatyczne zgłaszanie alertów do centrum serwisowego producenta, automatyczne update firmware dla wszystkich komponentów serwera, możliwość przywrócenia poprzednich wersji firmware, możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych, automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram, możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera, serwer musi posiadać funkcjonalność umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI
16. Praca w konfiguracji klastra niezawodnościowego HA
17. 60 miesięcy gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.
    Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
    Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.
    Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
18. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
    Serwer musi posiadać deklarację CE.
    Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.
    Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022 x64 .

Serwery wirtualizacyjne – oprogramowanie

W celu rozbudowy obecnego środowiska programowego niezbędne jest dostarczenie (adekwatnych do zaoferowanych serwerów wirtualizacyjnych):

1. Cztery licencje VMware vSphere w najnowszej wersji
2. Jednej licencji Vmware vCenter w najnowszej wersji

oraz

3. Cztery licencje Windows Server 2022 Datacenter + 240 CAL (SSO)

Równoważność

Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i nielimitowanej ilości wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.
SSO musi posiadać następujące, wbudowane cechy:

1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,
4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
8. wbudowane wsparcie instalacji i pracy na wolumenach, które:
   I. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),
9. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
10. wbudowane szyfrowanie dysków
11. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
12. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
13. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
14. graficzny interfejs użytkownika,
15. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
17. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
18. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
19. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
    3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
III. zdalna dystrybucja oprogramowania na stacje robocze,
IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    1) dystrybucję certyfikatów poprzez http,
    2) konsolidację CA dla wielu lasów domeny,
    3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
VI. szyfrowanie plików i folderów,
VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
VIII. VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
IX. serwis udostępniania stron WWW,
X. wsparcie dla protokołu IP w wersji 6 (IPv6),
XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
    1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,
    3) obsługi 4-KB sektorów dysków,
    4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
    5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
    6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),

20. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,
21. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
22. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
23. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
24. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Macierz dyskowa (1 szt.)

1. Macierz przystosowana do montażu w szafie rack 19” o wysokości maks. 2U pozwalająca na instalację 24 dysków 2,5”, dostarczona wraz z wszystkimi elementami montażowymi
2. Dwa kontrolery RAID pracujące w trybie active – active posiadające łącznie minimum osiem

portów iSCSI SFP+. Możliwość konfiguracji RAID 0,1,5,6,10,50, ADAPT.

3. Pamięć cache min. 8GB na kontroler, pamięć cache zapisu mirorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h lub w razie awarii.
4. Zainstalowane 17 dysków Hot-Plug o pojemności 3,84TB SAS SSD. Możliwość rozbudowy przez dokładania/wymianę kolejnych dysków/półek dyskowych do łącznie min. 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
5. Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej fazy zasilania. Redundantne: kontrolery macierzowe, wentylatory i zasilacze.
6. Macierz lub oprogramowanie umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN oraz 1024 kopii migawkowych na całą macierz. Licencja zaoferowanej macierzy powinna umożliwiać podłączenie minimum 8 hostów. Konieczne jest posiadanie automatycznego rozkładania danych między dyskami poszczególnych typów (tzw. Auto tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków.
7. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.
8. Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5
9. minimum podwójny 4-portowy kontroler 25Gb iSCSI
10. W wyposażeniu: kabel SFP+-SFP+ o dł. Min. 0,5m - 8 szt.
11. Wsparcie dla systemów Microsoft Windows Server 2012R2, Microsoft Windows Server 2016 Microsoft Windows Server 2019 , VMware ESXi, Red Hat Linux, SLES,
12. 60 miesięcy gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.
    Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
    Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.
    Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.
13. Macierz musi w pełni współpracować z oferowanymi serwerami. Wszystkie niezbędne elementy instalacji powinny znaleźć się w wycenie oferenta.
14. Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2015

Przełącznik 25Gb (1 stack switchowy złożony z min. 2 elementów o poniższych parametrach)

1. Przełącznik 25Gb/s do montażu w szafach Rack 19”
2. 48 portów 25Gb/s SFP28, 4 porty 100GB/s QSFP28
3. 1 port konsolowy RJ45, 1 port zarządzający typu out-of-band management
4. Dwa redundantne zasilacze AC
5. Chłodzenie urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne). Musi być wyposażony w redundantne i wymienne w trakcie pracy (hot-swap) wentylatory.
6. Minimalne wymagania wydajnościowe:
   - matryca przełączająca o wydajności min. 4Tbps (full duplex), min. 1.58 pps
   - ramki Jumbo o długości min. 9kB
   - ilość WLAN – co najmniej 4000
   - pamięć dla co najmniej 150 000 adresów MAC
7. Wymagania dotyczące obsługiwanych standardów oraz funkcji:
   - musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+, MSTP

- musi wspierać funkcjonalność wirtualnej agregacji portów
- urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG
- musi obsługiwać protokoły dynamicznego routingu dla IPv4 i dla IPv6: OSPF, BGP
- musi obsługiwać protokół BFD, przynajmniej dla protokołu OSPF i OSFP v3 i tras statycznych
- musi przechowywać sprzętowo minimum 32000 wpisów routingu IPv4 i 16000 wpisów routingu IPv6
- musi wspierać mechanizm L3 ECMP Load Balancing
- musi wspierać protokół redundancji VRRP
- wsparcie dla DHCP server i DHCP Relay oraz DHCPv6 Relay
- obsługa Policy Based Routing
- obsługa Muticastów, IGMP Snooping oraz Multicast Snooping, protokołu PIM oraz filtrów dla PIM
- musi obsługiwać funkcjonalność VxLAN, Static VxLan
- musi obsługiwać funkcjonalność VXLAN BGP EVPN (Ethernet VPN) z MP-BGP
- obsługa routingu między VxLAN-ami (VxLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway
- obsługa Multi-AS dla EVPN oraz trybów Asymmetric IRB (Integrated routing and bridging) oraz Symmetric IRB
- obsługa mechanizmu BGP unnumbered dla EVPN
- możliwość wyboru ścieżki routingu na podstawie długości AS-PATH dla EVPN route type 5
- obsługa mechanizmu ARP Suppression dla EVPN
- wsparcie dla obsługi klastra Microsoft NLB (dystrybucja pakietów do różnych serwerów o tym samym adresie IP/MAC)
- klasyfikacja ruchu dla klas różnej jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, vlan, wartość DSCP
- implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi.
- możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- implementacja mechanizmu Weighted Random Early Detection (WRED)
- obsługa IP Precedence i DSCP
- obsługa Control-Plane-Policing (ochrona systemu operacyjnego przed atakami DoS)
- musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow Control oraz Priority Flow Control oraz Enhanced Transmission Selection i iSCSI TLV
- autoryzacja użytkowników/portów w oparciu o 802.1x
- obsługa list dostępu ACL dla adresów MAC i adresów IPv4 i IPv6

8. Zarządzanie – funkcje:
   - możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2
   - obsługa monitorowania ruchu na porcie (Port Monitoring), ACL-Based Monitoring oraz RSPAN
   - urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony typu ethernet 100/1000BaseT
   - plik konfiguracyjny urządzenia musi być możliwy do edycji ‘off-line’. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian.

- wsparcie dla mechanizmu Beacon LED control – włączenie diody danego interfejsu celem identyfikacji
- urządzenie musi posiadać funkcjonalność automatycznej instalacji oprogramowania poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware), w trakcie pierwszego podłączenia do sieci Ethernet
- urządzenie musi mieć możliwość utworzenia skryptów systemu linux oraz uruchomienia skryptów utworzonych w języku Python oraz umożliwiać jego konfigurację przez narzędzia Ansible, Chef i Puppet
- możliwość użycia Restconf API , autoryzacja w oparciu o tokeny dla REST API oraz wsparcie dla mechanizmu tłumaczenia dowolnej komendy CLI na wywołanie Restconf
- możliwość konfiguracji restartu urządzenia w określonym czasie

9. Komponenty dodatkowe: kabel 100GbE direct attach QSFP28-QSFP28 o dł. min. 1 m
10. 60 miesięcy gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.
    Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
    Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.

Punkty dostępowe Access Point (5szt.)

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -10–45°C,
    b. Wilgotność 10–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac,
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Liczba interfejsów:
    a. Ethernet – 1 w standardzie 10/100/1000 Base-TX,
6. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
8. Wsparcie dla QoS: 802.11e, WME/WMM Multimedia Extensions, konfigurowalne polityki QoS per użytkownik/aplikacja.
9. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 3x3,
    b. Transmit Beam Forming (TxBF),
11. Minimalna przepustowość dla poszczególnych modułów radiowych:

    a. 400 Mbps;
    b. 1300 Mbps;
12. Moc nadawania:
    a. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
    b. min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
13. Wsparcie dla 802.11n 20/40Mhz HT,
14. Wsparcie dla kanału 80 MHz dla 802.11ac,
15. Anteny – 6 wewnętrznych dla nadajników standardu 802.11 o zysku min. 3dBi dla pasma 2.4GHz, 4dBi dla pasma 5GHz.
16. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
17. Funkcje interfejsu radiowego:
    a. Skaner częstotliwości 2.4 oraz 5 GHz,
    b. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
    c. Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,
18. Funkcje dodatkowe:
    a. Low-Density Parity Check (LDPC) Encoding,
    b. Maximum Likelihood Demodulation (MLD),
    c. Maximum Ratio Combining (MRC),
    d. A-MPDU and A-MSDU Packet Aggregation,
    e. MIMO Power Save,
    f. Short Guard Interval,
19. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.

System ochrony i akceleracji aplikacji sieciowych (rozwiązanie programowe)

Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne

1. Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
2. Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
3. Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
4. Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
5. Odwzorowanie struktury organizacji w oparciu o Active Directory
6. Jednostronna synchronizacja komputerów oraz drukarek z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
7. Automatyczne skanowanie całości lub wybranych grup Active Directory oraz sieci
8. Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
9. Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
10. Łączenie elementów wyposażenia w zestawy
11. Możliwość podpięcia dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
12. Przypisywanie sprzętu do konkretnych osób
13. Automatyczne wyznaczanie 'Głównego użytkownika' komputera
14. Przypisywanie sprzętu do dowolnej lokalizacji
15. Definiowanie własnych, dowolnych atrybutów sprzętu
16. Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia

Informacje o sprzęcie

1. Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu

2. Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
3. Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
4. Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
5. Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)
6. Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
7. Odczyt informacji o module TPM
8. Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
9. Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu
10. Automatyczne wykrywanie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)
11. Automatyczne tworzenie zestawów: Komputer + Monitor
12. Automatyczne utworzenie zestawów: Komputer + drukarka lokalna
13. Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
14. Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
15. Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)
16. Automatyczna aktualizacja adresów IP komputerów

Raporty zasobów

1. Automatyczne tworzenie historii zmian sprzętu
2. Ewidencja zdarzeń serwisowych
3. Dodanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
4. Informacja na temat pojemności dysków twardych oraz wolnego miejsca
5. Wydruk lub zapisanie do pliku raportów ze szczegółami sprzętu
6. Porównywarka wyników skanowania sprzętu
7. Dzienniki zdarzeń systemu Windows
8. Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu
9.

Zasoby -funkcje dodatkowe

1. Zdalne wykonywanie skryptów (batch) - Obsługa zadań jednorazowych i cyklicznych
2. Wykonywanie zadań dla wszystkich komputerów
3. Edytor skryptów (batch)
4. Wykorzystywanie predefiniowanych skryptów (batch)
5. Import informacji o wyposażeniu z pliku CSV
6. Obsługa kodów QR
7. Archiwum zasobów
8. Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu

Zarządzanie oprogramowaniem - licencje

1. Inwentaryzacja licencji
2. Automatyczne tworzenie licencji na podstawie kluczy produktów
3. Automatyczne generowanie historii zmian w licencji
4. Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności)
5. Przypisywanie licencji do komputera
6. Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska
7. Definiowanie kluczy seryjnych i przypisywanie do licencji

Zarządzanie oprogramowaniem - skanowanie oprogramowania

1. Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera

2. Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
3. Śledzenie zmian w stanie zainstalowanego oprogramowania
4. Zdalny skan komputerów (bieżący lub okresowy)
5. Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
6. Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
7. Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
8. Wykrywanie plików multimedialnych
9. Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
10. Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
11. Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych

Zarządzanie oprogramowaniem - funkcje

1. Wykrywanie kluczy/identyfikatorów programów
2. Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)
3. Zdalna dezinstalacja oprogramowania
4. Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej
5. Raport zainstalowanych aktualizacji systemu Windows

Kontrola wykorzystania sprzętu i oprogramowania

1. Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
2. Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
3. Zarządzanie stanowiskami użytkowników
4. Odczytywanie informacji o użytkownikach z Active Directory
5. Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
6. Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
7. Przypisywanie do użytkownika załączników (pliki)
8. Przypisywanie notatek do użytkownika
9. Ewidencja zdarzeń przypisanych do użytkowników
10. Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory

Kontrola wykorzystania sprzętu i oprogramowania -raporty

1. Analiza aktywności użytkowników
2. Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
3. Analiza przerw w pracy
4. Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
5. Analiza wykorzystania poszczególnych aplikacji w czasie
6. Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie
7. Statystyki najczęściej wykorzystywanych aplikacji
8. Statystyki wykorzystania komputerów przez poszczególnych użytkowników
9. Statystyki aktywności użytkownika i grup użytkowników
10. Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
11. Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
12. Monitoring wydruków na drukarkach sieciowych
13. Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)

Kontrola wykorzystania sprzętu i oprogramowania - funkcje

1. Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.

2. Autoryzacja nośników zewnętrznych
3. Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
4. Baza informacji o napędach zewnętrznych
5. Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
6. Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM

Kontrola wykorzystania Internetu

1. Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
2. Blokada stron internetowych dla protokołu http \ https (IE, Chrome, Firefox, Opera, Edge, Chromium, Vivaldi)
3. Kategoryzacja stron internetowych
4. Blokada dostępu do witryn zgodnie z harmonogramem

Kontrola wykorzystania Internetu - raporty

1. Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach
2. Dokładna analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)
3. Monitoring stron internetowych dla protokołu http \ https (IE, Edge, Chrome, Firefox, Opera, Vivaldi)
4. Analiza liczby wejść na poszczególne strony lub domeny
5. Analiza odwiedzanych domen i stron
6. Raport informujący o plikach pobranych przez przeglądarki WWW
7. Monitoring wysyłanych oraz pobieranych plików przez przeglądarki internetowe

Helpdesk

1. Rejestracja i obsługa zgłoszeń
2. Tworzenie notatek dla zgłoszeń
3. Archiwizacja zgłoszeń
4. Monitoring czasu pracy nad incydentem (time tracking)
5. Raport ewidencji czasu pracy nad zgłoszeniem
6. Informacja o czasie reakcji do podjęcia zgłoszenia
7. Wydruk historii zgłoszenia

Moduł połączeń zdalnych

1. Operacje na plikach i katalogach
2. Zarządzanie procesami i rejestrem
3. Monitoring pracy wykonywanej na komputerze
4. Zdalny podgląd pulpitów wielu stacji jednocześnie
5. Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
6. Wysyłanie wiadomości do użytkowników
7. Uruchamianie na stacjach programów z wiersza poleceń Command Line
8. Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
9. Przejęcie kontroli nad stacją roboczą
10. Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
11. Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
12. Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
13. Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
14. Obsługa wielu monitorów dla podglądu pulpitu
15. Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu
16. Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
17. Zarządzanie usługami systemu Windows

Serwisy i licencje

1. Powinny zostać dostarczone licencje, na co najmniej 60 miesięcy, upoważniające do korzystania z aktualnych baz funkcji programu dla co najmniej 200 użytkowników i 4 administratorów

Systemy ochrony w punkcie styku typu UTM (2szt. HA)

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Parametry fizyczne:

- 12 portów Gigabit Ethernet RJ-45.
- 8 gniazd SFP 1 Gbps.
- 2 gniazda SFP+ 10 Gbps.
- wbudowany port konsoli szeregowej
- gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
2. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
3. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
4. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
5. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Do urządzenia powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware vCenter (ESXi).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal – gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. Routingu statyczny.
2. Policy Based Routing.
3. Dynamiczny routing w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Rozwiązanie systemowe musi posiadać certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

Powinny zostać dostarczone licencje (na okres 60 miesięcy) upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmujące: kontrolę aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Wymagane dostarczenie minimum 25 licencji na uwierzytelnienie dwuskładnikowe z wykorzystaniem smartfonu.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Zamawiający wymaga minimum 600 h opieki serwisowej w czasie 60 miesięcy (łączna ilość godzin serwisowych, konsultacji itp.). Ostateczną liczbę godzin opieki serwisowej określa wykonawca jako jedno z kryterium oceny ofert.

Część nr 3

Tablet (10 szt.)

Według poniższej specyfikacji (wymagania minimalne):

1. Procesor-Intel® Atom™ x7-Z8750 lub równoważny osiągający wynik nie gorszy niż procesor referencyjny w testach PassMark CPU Mark https://www.cpubenchmark.net/.
2. Pamięć RAM-4 GB
3. System operacyjny-spełniający wymagania aplikacji e-Obchód
4. Pamięć ROM- minimum 64 GB
5. Wyświetlacz-10.1” FHD LCD, pojemnościowy P-CAP, sterowanie dotykowe (do 10 punktów), Corning® Gorilla® Glass 3
6. Rozdzielczość: full HD
7. Dźwięk-wbudowane głośniki
8. Audio Jack (mikrofon+słuchawki)
9. Kamera-Przód min 2.0-megapixel auto-focus
10. Tył min 5.0-megapixel auto-focus z fleszem LED
11. Sensory-Ambient Light Sensor

12. Czytnik kodów-wbudowany 1D/2D barcode scanner
13. Porty (min.):
    I/O-1 x micro HDMI,
    1 x USB 3.0,
    1 x combo audio jack,
    1 x SIM card reader,
    1 x micro SD card
14. Komunikacja -WLAN/Bluetooth IEEE 802.11a/b/g/n/ac, Bluetooth® v4.1
15. NFC 13.56 MHz, kompatybilny z ISO15693, ISO14443A, ISO 14443B, FeliCa
16. Bateria-wymienna podczas pracy urządzenia ze wskaźnikiem pojemności
17. Czas pracy na baterii min.: 3 godziny,
18. Czas ładowania: <3 godzin
19. Stacja dokująca z replikacja portów
20. Pasek do noszenia na ramię
21. Waga-poniżej 1kg
22. Klasa szczelności-IP65
23. Odporność na upadek-z wysokości do 120 cm
24. Zamawiający wymaga Gwarancji min 36 miesięcy. Ostateczną długość gwarancji określa wykonawca jako jedno z kryterium oceny ofert.

Część nr 4

Czytnik do dowodu osobistego (e-Dowodu) – 2 sztuki

1. Specyfikacja czytnika zgodna ze specyfikacją wymagań technicznych dla czytnika kart do zastosowania w środowisku zaufanym.
2. Czytnik musi umożliwiać integrację z systemem HIS i ERP.
3. Zamawiający wymaga Gwarancji min 36 miesięcy. Ostateczną długość gwarancji określa wykonawca jako jedno z kryterium oceny ofert.

Część nr 5

Laptop (5szt.)

1. Procesor Intel Core i5 lub wyższy, lub AMD ryzen 5 lub wyższy,
2. Pamięć RAM 8 GB lub więcej,
3. Karta graficzna zintegrowana,
4. Dysk twardy półprzewodnikowy SSD, minimum 512 GB,
5. Przekątna ekranu min. 15,6 cala,
6. Rozdzielczość ekranu 1920x1080 px lub wyższa,
7. Wbudowany napęd optyczny: nagrywarka DVD+/- RW DualLayer,
8. Łączność LAN, Wi-Fi, Bluetooth,
9. Kamera internetowa do wideo-rozmów.
10. Złącza: USB 3.0 lub 3.1, HDMI, VGA, RJ-45, Audio,
11. Zainstalowany system operacyjny: Microsoft Windows 10 Pro PL (64-bit) lub równoważny
12. Zainstalowane oprogramowanie biurowe Office 2019 Home & Business lub równoważne zapewniające poprawną wymianę dokumentów biurowych w jednostce oraz zapewniające klienta poczty wspierającego integrację z pakietem biurowym oraz wbudowanym kalendarzem pozwalającym na przesyłanie drogą elektroniczną planowanych spotkań.
13. Stacja dokująca z replikacja portów
14. Torba do przenoszenia

15. Zamawiający wymaga Gwarancji min 36 miesięcy. Ostateczną długość gwarancji określa wykonawca jako jedno z kryterium oceny ofert.

RÓWNOWAŻNOŚĆ

Oprogramowanie typu MS Windows 10 Professional 64bit PL lub równoważne, spełniające poniższe warunki:

1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika,
2. System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016;MS Visio 2007, 2010, 2016;MS Project 2007, 2010, 2016;
3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
4. Interfejsy użytkownika dostępne w wielu językach do wyboru -w tym Polskim i Angielskim,
5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
6. Wbudowany system pomocy w języku polskim,
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe -przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa -polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:
a. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
21. Obsługa standardu NFC (near field communication),
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);

23. Wsparcie dla IPSEC oparte na politykach -wdrażanie IPSECoparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
24. Mechanizmy logowania do domeny w oparciu o:
a. Login i hasło,
b. Karty z certyfikatami (smartcard),
c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
25. Mechanizmy wieloelementowego uwierzytelniania.
26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
27. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v.2 (IKEv2) dla warstwy transportowej IPsec,
28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
29. Wsparcie dla środowisk Java i .NET Framework 4.x -możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
30. Wsparcie dla JScript i VBScript -możliwość uruchamiania interpretera poleceń,
31. Zdalna pomoc i współdzielenie aplikacji -możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
32. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
33. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
34. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
35. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
36. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
37. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
38. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
39. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
40. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
42. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
43. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
44. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
45. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

RÓWNOWAŻNOŚĆ

Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
2. Wymagania odnośnie interfejsu użytkownika:

" Pełna polska wersja językowa interfejsu użytkownika.

" Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

a. Posiada kompletny i publicznie dostępny opis formatu.

b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

c. Pozwala zapisywać dokumenty w formacie XML

4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać :

a. Edytor tekstów.

b. Arkusz kalkulacyjny.

c. Narzędzie do przygotowywania i prowadzenia prezentacji.

d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

8. Edytor tekstów musi umożliwiać:

a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.

b. Wstawianie oraz formatowanie tabel.

c. Wstawianie oraz formatowanie obiektów graficznych.

d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).

e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

f. Automatyczne tworzenie spisów treści.

g. Formatowanie nagłówków i stopek stron.

h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.

i. Nagrywanie, tworzenie i edycję makrautomatyzujących wykonywanie czynności.

j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.

k. Wydruk dokumentów.

l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.

n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.

p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
9. Arkusz kalkulacyjny musi umożliwiać:
a. Tworzenie raportów tabelarycznych.
b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących nadanych z tabeli przestawnych.
g. Wyszukiwanie i zamianę danych.
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
k. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a. Przygotowywanie prezentacji multimedialnych, które będą:
b. Prezentowanie przy użyciu projektora multimedialnego.
c. Drukowanie w formacie umożliwiającym robienie notatek.
d. Zapisanie jako prezentacja tylko do odczytu.
e. Nagrywanie narracji i dołączanie jej do prezentacji.
f. Opatrywanie slajdów notatkami dla prezentera.
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
j. Możliwość tworzenia animacji obiektów i całych slajdów.
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.
11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.

e. Automatyczne grupowanie wiadomości poczty o tym samym tytule.
f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
i. Zarządzanie kalendarzem.
j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
k. Przeglądanie kalendarza innych użytkowników.
l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
m. Zarządzanie listą zadań.
n. Zlecanie zadań innym użytkownikom.
o. Zarządzanie listą kontaktów.
p. Udostępnianie listy kontaktów innym użytkownikom.
q. Przeglądanie listy kontaktów innych użytkowników.
r. Możliwość przesyłania kontaktów innym użytkowników.
s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

Część nr 6

Urządzenie wielofunkcyjne (2szt.)

1. Technologia druku: kolorowa LED-owa,
2. Kopiowanie w kolorze, faksowanie w kolorze, drukowanie w kolorze, skanowanie w kolorze, skanowanie sieciowe w kolorze,
3. Wyświetlacz kolorowy dotykowy,
4. Obsługiwane rozmiary: A6, Oficio, Super-Tabloid (305 x 457 mm), koperta 7 ¾, JIS-B4, JIS-B5, A3, Ledger, A4, A5, Letter, Statement, Koperta C5, Executive, Universal, Koperta DL, Folio, Koperta 10,
5. Interfejsy standardowe: Port USB Ethernet 10/100/1000 RJ-45,
6. Szybkość kopiowania/drukowania min: mono – 45 kopii/min. (A4), kolor: 40 kopii/min. (A4),
7. Czas kopiowania pierwszej strony: mono: 7.1 sek., kolor: 10.4 sek.,
8. Zakres zmniejszenia/powiększenia: 25 – 400%,
9. Szybkość modemu (fax): 33,6 Kb/s,
10. Druk dwustronny, zintegrowany duplex,
11. Rodzaj skanera: flatbed scanner width ADF, skanowanie dwustronne rewersyjne,
12. Maksymalny obszar skanowania: 297 x 432 mm,
13. Technologia skanowania: CCD,
14. Rozdzielczość skanowania min.: 600 x 600 dpi,
15. Formaty zeskanowanych plików: XPS, TIFF, Archival PDF (A-1a, A-1b), secure PDF, PDF, JPEG, JPG,
16. Miejsca docelowe skanu: e-mail, USB Flash drive, miejsce sieciowe,
17. Automatyczny podajnik dokumentów (skanowanie),
18. Obsługiwane rodzaje nośników: etykiety, karty, papier zwykły, folie, koperty, papier błyszczący,
19. Standardowa liczba podajników: min 3
20. Obsługiwana gramatura nośników: 60 – 256 g/m2

21. Obsługa papieru standardowo: wbudowany moduł druku dwustronnego, taca wejściowa na 520 arkuszy, moduł podwójnego podajnika na 2500 arkuszy, podajnik uniwersalny na 100 arkuszy, odbiornik na 500 arkuszy,
22. Wydajność materiałów eksploatacyjnych: kasety z tonerami CMY co najmniej o wydajności 22 000 stron, kaseta z tonerem czarnym o wydajności co najmniej 32 000 stron,
23. W dostawie tonery startowe i dwa komplety tonerów eksploatacyjnych
24. Energy Star: tak,
25. Zamawiający wymaga Gwarancji min 36 miesięcy. Ostateczną długość gwarancji określa wykonawca jako jedno z kryterium oceny ofert.

Część nr 7

Stacja robocza z monitorem (10szt.)

1. Procesor Intel Core i5 lub wyższy, lub AMD ryzen 5 lub wyższy,
2. Pamięć operacyjna RAM 8GB DDR4 2666MHz non-ECC możliwość rozbudowy do min. 32GB, jeden slot wolny;
3. Dysk minimum 256GB SSD;
4. Karta graficzna dedykowana obsługująca co najmniej rozdzielczość 1920x1080;
5. Zainstalowany system operacyjny Windows 10 Professional PL lub równoważny zapewniający poprawne funkcjonowanie usługi katalogowej oraz spełnianie polityki bezpieczeństwa jednostki.
6. Oprogramowanie biurowe Office 2019 Home & Business lub równoważny zapewniający poprawną wymianę dokumentów biurowych w jednostce oraz zapewniający klienta poczty wspierającego integrację z pakietem biurowym oraz wbudowanym kalendarzem pozwalającym na przesyłanie drogą elektroniczną planowanych spotkań.
7. Zintegrowana karta sieciowa 10/100/1000 Mbits/s
8. Interfejsy min.:
    - 6 x USB, w tym min.: 2 x USB 3.0 na przednim panelu
    - 1 x RJ45 LAN
    - 1 x HDMI/DP
    - 1 x VGA
    - 1 x audio (mikrofon, słuchawki)
9. Napęd optyczny DVD-+RW
10. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego.
11. Rodzaj obudowy SFF
12. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz musi być wpisany na stałe w BIOS.
13. Zgodność z systemami operacyjnymi Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi
14. Wirtualizacja Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
15. BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera.
16. Pełna obsługa BIOS za pomocą klawiatury i myszy.
17. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji.

18. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.
19. Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem).
20. Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN.
21. Certyfikat ISO9001 dla producenta sprzętu.
22. W zestawie klawiatura i mysz.
23. Monitor o rozdzielczości min full HD i przekątnej minimum 23,8".
24. Zamawiający wymaga Gwarancji min 36 miesięcy. Ostateczną długość gwarancji określa wykonawca jako jedno z kryterium oceny ofert.

RÓWNOWAŻNOŚĆ

Oprogramowanie typu MS Windows 10 Professional 64bit PL lub równoważne, spełniające poniższe warunki:

1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika,
2. System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016;MS Visio 2007, 2010, 2016;MS Project 2007, 2010, 2016;
3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:

a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,

4. Interfejsy użytkownika dostępne w wielu językach do wyboru -w tym Polskim i Angielskim,
5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
6. Wbudowany system pomocy w języku polskim,
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe -przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa -polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:

a. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
21. Obsługa standardu NFC (near field communication),
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
23. Wsparcie dla IPSEC oparte na politykach -wdrażanie IPSECoparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
24. Mechanizmy logowania do domeny w oparciu o:
a. Login i hasło,
b. Karty z certyfikatami (smartcard),
c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
25. Mechanizmy wieloelementowego uwierzytelniania.
26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
27. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v.2 (IKEv2) dla warstwy transportowej IPsec,
28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
29. Wsparcie dla środowisk Java i .NET Framework 4.x -możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
30. Wsparcie dla JScript i VBScript -możliwość uruchamiania interpretera poleceń,
31. Zdalna pomoc i współdzielenie aplikacji -możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
32. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
33. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
34. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
35. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
36. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
37. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
38. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
39. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
40. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
42. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
43. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
44. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

45. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

RÓWNOWAŻNOŚĆ

Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
2. Wymagania odnośnie interfejsu użytkownika:

" Pełna polska wersja językowa interfejsu użytkownika.

" Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:

a. Posiada kompletny i publicznie dostępny opis formatu.

b. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

c. Pozwala zapisywać dokumenty w formacie XML

4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać :

a. Edytor tekstów.

b. Arkusz kalkulacyjny.

c. Narzędzie do przygotowywania i prowadzenia prezentacji.

d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

8. Edytor tekstów musi umożliwiać:

a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.

b. Wstawianie oraz formatowanie tabel.

c. Wstawianie oraz formatowanie obiektów graficznych.

d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).

e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

f. Automatyczne tworzenie spisów treści.

g. Formatowanie nagłówków i stopek stron.

h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.

i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.

k. Wydruk dokumentów.

l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
9. Arkusz kalkulacyjny musi umożliwiać:
a. Tworzenie raportów tabelarycznych.
b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących nadanych z tabeli przestawnych.
g. Wyszukiwanie i zamianę danych.
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
k. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a. Przygotowywanie prezentacji multimedialnych, które będą:
b. Prezentowanie przy użyciu projektora multimedialnego.
c. Drukowanie w formacie umożliwiającym robienie notatek.
d. Zapisanie jako prezentacja tylko do odczytu.
e. Nagrywanie narracji i dołączanie jej do prezentacji.
f. Opatrywanie slajdów notatkami dla prezentera.
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
j. Możliwość tworzenia animacji obiektów i całych slajdów.
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.

11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.

b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.

c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.

d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.

e. Automatyczne grupowanie wiadomości poczty o tym samym tytule.

f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.

g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.

h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.

i. Zarządzanie kalendarzem.

j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.

k. Przeglądanie kalendarza innych użytkowników.

l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.

m. Zarządzanie listą zadań.

n. Zlecanie zadań innym użytkownikom.

o. Zarządzanie listą kontaktów.

p. Udostępnianie listy kontaktów innym użytkownikom.

q. Przeglądanie listy kontaktów innych użytkowników.

r. Możliwość przesyłania kontaktów innym użytkowników.

s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.