|  |  |
| --- | --- |
|  | Szczegółowy OpisPrzedmiotu Zamówienia |
|  | Projekt:*Budowa usług e-ZdrowiaSzpitala Psychiatrycznego SP ZOZ w Węgorzewie* |

Zatwierdził: Agnieszka Szałko

Węgorzewo, 12 października 2018 r.

Spis treści

[Wstęp 3](#__RefHeading__6020_2029055438)

[Ogólny zarys projektu 3](#__RefHeading__6022_2029055438)

[Słownik pojęć 3](#__RefHeading__6024_2029055438)

[Wymagania ogólne 6](#__RefHeading__6026_2029055438)

[Zakres 1 – Dostawa sprzętu i oprogramowania systemowego 7](#__RefHeading__6028_2029055438)

[Serwery 7](#__RefHeading__6030_2029055438)

[Typ 1 7](#__RefHeading__6032_2029055438)

[Typ 2 8](#__RefHeading__6034_2029055438)

[Typ 3 8](#__RefHeading__6036_2029055438)

[Macierz dyskowa 8](#__RefHeading__6038_2029055438)

[Serwer NAS 9](#__RefHeading__6040_2029055438)

[Zasilanie awaryjne – UPS 9](#__RefHeading__6042_2029055438)

[Typ 1 10](#__RefHeading__6044_2029055438)

[Typ 2 –zapasowy 13](#__RefHeading__6046_2029055438)

[Typ 3 – do szafki punktów dystrybucyjnych 14](#__RefHeading__6048_2029055438)

[Przełączniki sieciowe 14](#__RefHeading__6050_2029055438)

[Typ 1 14](#__RefHeading__6052_2029055438)

[Typ 2 15](#__RefHeading__6054_2029055438)

[Typ 3 15](#__RefHeading__6056_2029055438)

[Punkty dostępowe WLAN 15](#__RefHeading__6058_2029055438)

[Typ 1 – wewnętrzne 16](#__RefHeading__6060_2029055438)

[Typ 2 – zewnętrzne 16](#__RefHeading__6062_2029055438)

[Stanowiska robocze stacjonarne 16](#__RefHeading__6064_2029055438)

[Stanowiska robocze mobilne 17](#__RefHeading__6066_2029055438)

[Tablety medyczne 17](#__RefHeading__6068_2029055438)

[Urządzenia wielofunkcyjne A3 18](#__RefHeading__6070_2029055438)

[Drukarki laserowe A4 21](#__RefHeading__6072_2029055438)

[Skanery dokumentów 21](#__RefHeading__6074_2029055438)

[Drukarki opasek dla pacjentów 22](#__RefHeading__6076_2029055438)

[Zabezpieczenie e-Usług 22](#__RefHeading__6078_2029055438)

[Firewall – UTM 22](#__RefHeading__6080_2029055438)

[Antywirus 26](#__RefHeading__6082_2029055438)

[Kopie zapasowe 26](#__RefHeading__6084_2029055438)

[System zarządzania i monitorowania infrastruktury serwerów 28](#__RefHeading__6086_2029055438)

[Licencje 30](#__RefHeading__6088_2029055438)

[Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego 32](#__RefHeading__6090_2029055438)

[Serwery 32](#__RefHeading__6092_2029055438)

[Macierz dyskowa 32](#__RefHeading__6094_2029055438)

[Serwer NAS 32](#__RefHeading__6096_2029055438)

[Zasilanie awaryjne – UPS 32](#__RefHeading__6098_2029055438)

[Przełączniki sieciowe 32](#__RefHeading__6100_2029055438)

[Typ 1 32](#__RefHeading__6102_2029055438)

[Typ 2 32](#__RefHeading__6104_2029055438)

[Typ 3 32](#__RefHeading__6106_2029055438)

[Punkty dostępowe WLAN 32](#__RefHeading__6108_2029055438)

[Typ 1 – wewnętrzne 32](#__RefHeading__6110_2029055438)

[Typ 2 – zewnętrzne 32](#__RefHeading__6112_2029055438)

[Stanowiska robocze stacjonarne 32](#__RefHeading__6114_2029055438)

[Stanowiska robocze mobilne 33](#__RefHeading__6116_2029055438)

[Tablety medyczne 33](#__RefHeading__6118_2029055438)

[Urządzenia wielofunkcyjne A3 33](#__RefHeading__6120_2029055438)

[Drukarki laserowe A4 33](#__RefHeading__6122_2029055438)

[Skanery dokumentów A4 34](#__RefHeading__6124_2029055438)

[Zabezpieczenie e-Usług 34](#__RefHeading__6126_2029055438)

[Firewall – UTM 34](#__RefHeading__6128_2029055438)

[Antywirus 34](#__RefHeading__6130_2029055438)

[Systemy monitorowania serwerów i usług 34](#__RefHeading__6132_2029055438)

[Kopie zapasowe 34](#__RefHeading__6134_2029055438)

[Architektura HA dla serwera aplikacji 35](#__RefHeading__6136_2029055438)

[Architektura HA dla serwera bazy danych 35](#__RefHeading__6138_2029055438)

[Architektura Active Directory 35](#__RefHeading__6140_2029055438)

[Architektura RDP 35](#__RefHeading__6142_2029055438)

[Architektura prywatnego CA 35](#__RefHeading__6144_2029055438)

[Usługi wspomagające 35](#__RefHeading__6146_2029055438)

[Zakres 3 – Modernizacja sieci LAN i WLAN 36](#__RefHeading__6148_2029055438)

[Rozbudowa sieci LAN 36](#__RefHeading__6150_2029055438)

[Parametry minimalne szafek RACK 36](#__RefHeading__6152_2029055438)

[Budowa sieci WLAN 37](#__RefHeading__6154_2029055438)

[Zakres 4 – Dostawa oprogramowania e-Usług 38](#__RefHeading__6156_2029055438)

[Wdrożenie portalu e-Usług. 38](#__RefHeading__6158_2029055438)

[Dostawa systemu e-Usług 39](#__RefHeading__6160_2029055438)

[1. Rozbudowa obecnej usługi E-rejestracji do poradni 39](#__RefHeading__6162_2029055438)

[2. Wstępna e-kwalifikacja pacjentów do 8 tygodniowego programu terapii uzależnień 39](#__RefHeading__6164_2029055438)

[3. E-recepta 40](#__RefHeading__6166_2029055438)

[4. E-zlecenie 40](#__RefHeading__6168_2029055438)

[5. E-skierowanie 41](#__RefHeading__6170_2029055438)

[6. Pakiet wiadomości SMS 41](#__RefHeading__6172_2029055438)

[Zakres 5 – Konfiguracja i uruchomienie e-Usług 42](#__RefHeading__6174_2029055438)

[Wdrożenie portalu e-Usług. 42](#__RefHeading__6176_2029055438)

[Integracja portalu e-Usług z HIS 42](#__RefHeading__6178_2029055438)

[Uwierzytelnianie dostępu do e-Usług 42](#__RefHeading__6180_2029055438)

[Uruchomienie e-Usług 43](#__RefHeading__6182_2029055438)

[Moduł integracji z P1, P2 [z EDM] 43](#__RefHeading__6184_2029055438)

[Inne integracje Systemu 43](#__RefHeading__6186_2029055438)

[Zakres 6 – Szkolenia 45](#__RefHeading__6188_2029055438)

[Zakres 7 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej 46](#__RefHeading__6190_2029055438)

[Zakres 8 – Gwarancja i wsparcie 47](#__RefHeading__6192_2029055438)

Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (SzOPZ) w zakresie dostawy i wdrożenia sprzętu oraz oprogramowania służącego uruchomieniu i zabezpieczeniu działania e-Usług w Szpitalu Psychiatrycznym w Węgorzewie oraz jego jednostkach terenowych. Prezentowany poniżej ogólny schemat organizacji serwerowni stanowi jedynie zarys całego rozwiązania – Wykonawca może zaproponować swoją wersję organizacji serwerowni o ile proponowane rozwiązanie gwarantowało będzie wyższy poziom bezpieczeństwa i lepsze wykorzystanie mocy obliczeniowej serwerów fizycznych przy czym nie może udostępniać mniejszej szybkości działania. Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne wymagania stawiane oferowanym urządzeniom i oprogramowaniu.

Ogólny zarys projektu

Celem projektu jest wdrożenie nowoczesnych i bezpiecznych e-Usług w Szpitalu Psychiatrycznym w Węgorzewie. W tym celu wszystkie obecne i nowe systemy oraz usługi muszą zostać uruchomione w trybie wysokiej dostępności (HA). Aby sprostać temu wymogowi w Szpitalu zostaną zainstalowane nowe serwery z usługami wirtualizacji zabezpieczone niezależnym zasilaniem bateryjnym (UPS). Wszystkie nowe i obecne usługi zostaną uruchomione w środowisku wirtualnym w trybie HA. Dodatkowym zabezpieczeniem funkcjonowania e-Usług w trybie wysokiej dostępności będzie uruchomienie drugiej zapasowej serwerowni.

Fizycznym miejscem instalacji e-Usług będzie lokalizacja główna, tj. Szpital Psychiatryczny w Węgorzewie, jednakże część e-Usług świadczona będzie w pozostałych lokalizacjach należących do Szpitala, tj.:

* WOTUW Giżycko, ul. Warszawska 41a,
* PZP Giżycko, ul. Westerplatte 4,
* PZP Pisz, ul. Sienkiewicza 5,
* ZOLP w Rudziszkach, Rudziszki 5.

Aby usługi elektroniczne świadczone były w sposób bezpieczny, wszystkie lokalizacje zewnętrzne oraz lokalizacja centralna zostaną wyposażone w urządzenia typu UTM zabezpieczające ruch sieciowy zarówno pomiędzy placówkami jak i pomiędzy pacjentami i placówką główną oraz gwarantującymi ciągłość dostępności e-Usług.

Niniejszy Przedmiot Zamówienia podzielony jest na następujące zakresy:

|  |  |  |
| --- | --- | --- |
| Lp. | Opis prac wykonanych w ramach zakresu | Maksymalny czas realizacji |
| Zakres 1 | Dostawa sprzętu i oprogramowania systemowego | 40 dni[[1]](#footnote-2) |
| Zakres 2 | Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego | 15 dni[[2]](#footnote-3) |
| Zakres 3 | Modernizacja sieci LAN i WLAN | 30 dni1 |
| Zakres 4 | Dostawa oprogramowania e-Usług | 30 dni1 |
| Zakres 5 | Konfiguracja i uruchomienie e-Usług | 90 dni2 |
| Zakres 6 | Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania e-usługami. | 14 dni2 |
| Zakres 7 | Przygotowanie oraz dostarczenie dokumentacji projektowej i powykonawczej | 14 dni2 |
| Zakres 8 | Świadczenie usług gwarancji i rękojmi w ramach dostarczonego rozwiązania | 60 miesięcy[[3]](#footnote-4) |



Rysunek 1 Ogólny schemat docelowej organizacji serwerowni

Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

1. **Strony Umowy** – uogólnione pojęcie stosowane zamiennie do określenia Zamawiającego i Wykonawcy jednocześnie.
2. **Cel Umowy** – przyczyny oraz oczekiwane wyniki, dla osiągnięcia których Strony podjęły współpracę i zawarły Umowę.
3. **Przedmiot Umowy** – całokształt zagadnień realizowanych w ramach Umowy ukierunkowanych na osiągnięcie Celu Umowy.
4. **Dysfunkcja** – zbiorcze określenie dla nieprawidłowości rozumianych jako niezgodność z Dokumentacją lub też uciążliwość w pracy z Systemem.
5. **Kategoria Dysfunkcji** - kategoria, do której kwalifikowane jest Zgłoszenie Serwisowe dotyczące Dysfunkcji. Opisane szczegółowo w Załączniku nr 6 do Umowy.
6. **Prace Serwisowe** - działania Wykonawcy mające na celu realizację Zgłoszenia Serwisowego.
7. **Naprawa** – modyfikacja Systemu usuwająca Dysfunkcję Systemu.
8. **Obejście** - tymczasowe rozwiązanie pozwalające na prawidłowe wykorzystanie oprogramowania bez usuwania wykrytego błędu przy zachowaniu integralności bazy danych.
9. **Realizacja Zgłoszenia Serwisowego** - zakończenie Prac Serwisowych, w wyniku których przywrócono Stan Funkcjonalności.
10. **Analiza** – dokumenty opracowane przez Wykonawcę, mające na celu doprecyzowanie sposobu realizacji wymagań Zamawiającego, zasad i metod realizacji Umowy oraz wskazanie i szczegółowe opisanie Produktów;
11. **Backup** – wykonanie kopii bezpieczeństwa danych pozwalających na odtworzenie i przywrócenie Bazy Danych i Systemu po wystąpieniu awarii w przypadku utraty lub uszkodzenia oryginalnych danych; jakość odtworzonych danych powinna być dostosowana do ustalonego uprzednio poziomu ryzyka, który poniesie Zamawiający (poziom ryzyka determinuje cykliczność wykonywania backup'ów).
12. **Baza Danych** – zbiór wszystkich danych zewidencjonowanych za pomocą Systemu.
13. **Czas Roboczy** – czas pracy liczony w Dni Robocze, w którym świadczona jest pomoc telefoniczna przy eksploatacji Systemu.
14. **Dzień Roboczy** – dzień kalendarzowy od poniedziałku do piątku z wyłączeniem świąt i dni ustawowo wolnych od pracy.
15. **Dokumentacja** – dokument papierowy lub elektroniczny opisujący System i zasady użytkowania Systemu. Wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy.
16. **Godziny robocze** – czas pracy liczony w Dni Robocze w godzinach 7:30 – 15:30.
17. **Konsultant serwisowy** – osoba fizyczna posiadająca odpowiednie kwalifikacje uprawniające do realizowania Serwisu.
18. **Pomoc Telefoniczna** – świadczenie konsultacji telefonicznej dotyczące szeroko pojętej eksploatacji Systemu.
19. **Procedura** – schemat postępowania w jaki winien być realizowany określony fragment Przedmiotu Umowy.
20. **Publikacja** – udostępnienie Systemu zawierającego zmienioną funkcjonalność.
21. **Serwer** – sprzęt komputerowy, na którym zainstalowana jest baza danych lub aplikacje wykorzystywane przez System.
22. **Serwis** – usługa o charakterze technicznym, organizacyjnym, doradczym i szkoleniowym, przeznaczona do zapewnienia stabilnej pracy Systemu.
23. **Stan Funkcjonalności** - stan Systemu, w którym nie występują Dysfunkcje.
24. **Upgrade** – nowa  wersja Systemu związana ze stworzeniem nowej funkcjonalności.
25. **Update** – aktualizacja Systemu w wyniku zmian przepisów, związanych bezpośrednio i pośrednio z systemem ochrony zdrowia, w zakresie tej samej wersji Systemu.
26. **Wdrożenie** – opisane Umową świadczenia Wykonawcy mające na celu wykonanie Systemu
27. **Wersja** – okresowa Publikacja Systemu uwzględniająca Naprawy i zmiany dokonane w okresie od poprzedniej Publikacji Systemu. Wydanie Wersji obejmuje również opis nowej Funkcjonalności Systemu.
28. **Zgłoszenie Serwisowe** – Dysfunkcja, o której Wykonawca został powiadomiony drogą mailową.
29. **Administrator** - Użytkownik konfigurujący i zarządzający Systemem i Infrastrukturą.
30. **API** - Application Programming Interface, interfejs programowania aplikacji – jest to sposób rozumiany, jako ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.
31. **Architektura systemu teleinformatycznego** – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami.
32. **Czas dostarczenia rozwiązania** - Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Rozwiązania Zastępczego.
33. **Dane typu on-line** – dane dostępne w czasie rzeczywistym tzn. natychmiast po wprowadzaniu do określonego modułu systemu.
34. **Dane typu off-line** – dane pochodzące z migracji z innych modułów systemu lub zarchiwizowane, dostępne w czasie zdefiniowanym przez Administratora systemu.
35. **Dane referencyjne** - dane opisujące cechę informacyjną obiektu pierwotnie wprowadzone do bazy danych w wyniku określonego zdarzenia, z domniemania opatrzone atrybutem autentyczności .
36. **Dostępność** – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym .
37. **ePUAP** – Elektroniczna Platforma Usług Administracji Publicznej https://epuap.gov.pl
38. **Integralność** – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony .
39. **Kierownik Projektu Wykonawcy** (KPW) – Osoba ze strony Wykonawcy upoważniona do bezpośredniej koordynacji zadań objętych umową. Do zadań Kierownika Projektu Wykonawcy należy m.in. podpisywanie dokumentów w zakresie Protokołów Odbioru Zadań, Protokołów Odbioru Końcowego.
40. **Kierownik Projektu Zamawiającego** (KPZ) - Osoba ze strony Zamawiającego upoważniona do bezpośredniej koordynacji zadań objętych umową. Do zadań Kierownika Projektu Zamawiającego należy m.in. podpisywanie dokumentów w zakresie Protokołów Odbioru Zadań, Protokołów Odbioru Końcowego.
41. **Moduł systemu** – kompletny zestaw narzędzi informatycznych obejmujących wszystkie warstwy architektury systemu, który dostarcza aplikację przeznaczoną dla użytkownika końcowego do realizacji określonych dziedzin działalności Zamawiającego.
42. **Okno Serwisowe** – przerwa w działaniu systemu w godzinach pracy [tj. pomiędzy 7:30 a 15:30] w dni robocze Zamawiającego, mająca na celu umożliwienie prowadzenie prac serwisowych wymagających czasowego wyłączenia systemu [np. aktualizacja]. Poza tymi godzinami aktywny 365/24/7 system HelpDesk. Okno serwisowe dotyczy usług serwisowych z wyłączeniem zadań bezpieczeństwa sieci.
43. **Oprogramowanie aplikacyjne** – Dziedzinowy system informatyczny klasy HIS [Hospital Information System] na którego bazie zbudowane będą e-Usługi jak również samo oprogramowanie e-Usług i Portalu.
44. **Oprogramowanie standardowe** – Każde oprogramowanie niezbędne, poza oprogramowaniem aplikacyjnym niezbędne do działania Systemu.
45. **Portal Usług Elektronicznych** – portal udostępniający usługi elektroniczne dostarczane przez System dla użytkowników wewnętrznych i zewnętrznych
46. **PKI** – Infrastruktura Klucza Publicznego
47. **PZ ePUAP** – Profil Zaufany ePUAP
48. **Rozwiązanie zastępcze** - proponowane przez Wykonawcę rozwiązanie tymczasowe, usuwające lub niwelujące czasowo do akceptowalnego poziomu skutki wystąpienia Wady, wprowadzone do czasu usunięcia Wady.
49. **System** – Łączne określenie dla oprogramowania – występującego u Zamawiającego, objętego wdrożeniem oraz umową serwisową z Wykonawcą, bez względu na nazwę handlową. Obejmujący Platformę systemowo-sprzętową, Oprogramowania aplikacyjne oraz inne oprogramowanie niezbędne do działania e-Usług realizowanych w niniejszym zamówieniu.
50. **System zewnętrzny** - Każdy System informatyczny niebędący przedmiotem Zamówienia a oddziaływujący na przedmiot zamówienia.
51. **Usługi elektroniczne (eUsługi)** – usługi, których świadczenie odbywa się za pomocą Internetu, jest zautomatyzowane (może wymagać niewielkiego udziału człowieka) i zdalne. Od usługi w ujęciu tradycyjnym, eUsługę odróżnia brak udziału człowieka po drugiej stronie oraz świadczenie na odległość.
52. **Użytkownik** - Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło.
53. **Web Service** - Usługa sieciowa dostarczająca określoną funkcjonalność poprzez sieci Internet, niezależnie od platformy sprzętowej i implementacji.
54. **Wzór dokumentu elektronicznego** - Wzór pisma w formie Dokumentu Elektronicznego w rozumieniu Art.19 b) ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005r. Nr 64 z późn. zm.) oraz §18 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych. (Dz.U. z 2011, Nr206, poz.1216).
55. **Wykonawca** – wybrany w drodze zamówienia publicznego podmiot realizujący niniejszy przedmiot zamówienia.
56. **Zamawiający** – Szpital Psychiatryczny SP ZOZ w Węgorzewie
57. **Zdalny dostęp** – możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.
58. **XML** – Format XML jest to obecnie powszechnie uznany standard publiczny, umożliwiający wymianę danych między różnymi systemami.
59. **EDM** – Elektroniczna Dokumentacja Medyczna zgodnie z zapisami ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.
60. **P1, P2** – Programy monitorowane i realizowane przez CSIOZ
61. **ASI** – Administrator Systemów Informatycznych w Szpitalu
62. **PD –** Punkt dystrybucyjny sieci LAN

Wymagania ogólne

System musi być zbudowany i wdrożony zgodnie z obowiązującymi przepisami prawa, zgodnie ze strukturą organizacyjną i regulaminami Zamawiającego oraz dobrymi praktykami.

Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).

System musi być zbudowany w architekturze wysokiej dostępności (HA).

System musi umożliwiać definiowanie dowolnej ilości użytkowników.

System musi być w całości spolonizowany, a więc posiadać polskie znaki i instrukcję obsługi po polsku dla użytkownika oraz administratora. Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, punkty wifi, itp. dla których wymogiem minimalnym jest posiadanie interfejsów w języku minimum angielskim.

System musi posiadać graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po dowolnych kryteriach. Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, punkty wifi, itp. dla których wymogi minimalne co do posiadanych interfejsów zostały opisane odrębnie.

System musi gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych.

System musi pracować w środowisku sieciowym i posiadać wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników bez ograniczeń na ich liczbę.

System musi posiadać mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych.

System musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji.

System musi posiadać modyfikowalne słowniki wewnętrzne.

System musi działać w środowisku zintegrowanych baz danych posiadającym następujące cechy: relacyjność i transakcyjność, komunikacja z aplikacjami w standardzie SQL.

Na dzień składania oferty dostarczany w ramach Projektu System nie może być przeznaczony do wycofania z produkcji, sprzedaży lub wsparcia technicznego.

Dostarczone oprogramowanie musi być oprogramowaniem w wersji aktualnej.

Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

System powinien być zintegrowany pod względem przepływu informacji - informacja raz wprowadzona do systemu jest wykorzystywana w pozostałych modułach programowych.

Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne, okresowe [np. na aktualizację sygnatur wirusów] na min. okres trwałości projektu, tj. 60 msc; nośniki instalacyjne, instrukcje.

Zakres 1 – Dostawa sprzętu i oprogramowania systemowego

Poniżej przedstawiono parametry minimalne jaki dostarczany sprzęt musi spełniać. W przypadku gdy do realizacji Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nie ujęte w poniższym zestawieniu Wykonawca musi go dostarczyć i wykazać w wykazie asortymentowo-cenowym.

Serwery

Parametry wspólne

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Obudowa | RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia), maksymalnie 2U |
| Procesor | Dwa procesory.Płyta główna wspierająca zastosowanie procesorów min. od 4 do 28rdzeniowych. |
| Pamięć operacyjna | min. RDIMM DDR4 2666 MT/s w modułach o pojemności 8GB lub 16GB każdy.Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB.Obsługa zabezpieczeń: Advanced ECC i Online Spare.Serwer z obsługą pamięci typu NVDIMM. |
| Sloty rozszerzeń | 2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16pełnej wysokości.  |
| Interfejsy sieciowe | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcjąWake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.Minimum 2 porty FC 16Gb wraz z zainstalowanymi wkładkami.Możliwość instalacji dodatkowej karty 2 portowej obsługującej prędkości 10/25Gb/s (możliwość konfiguracji pracy z prędkościami min. 25Gb/s), przez zastosowanie karty nie zajmującej gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | Min.: 4 x USB 3.0 (co najmniej jeden z przodu obudowy); 1x VGA; Wewnętrzny slot na kartę micro SD.Możliwość rozbudowy o:- dodatkowy port typu DisplayPort/HDMI dostępny z przodu serwera- port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony nazewnątrz obudowy |
| Zasilacz | 2 szt., typu Hot-plug, redundantne. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug.Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia do 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4 |
| Pamięć microSD/FLASH  | Zainstalowana karta pamięci micro SD/FLASH minimum 8GB. |
| Napęd | Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW |
| Diagnostyka | Możliwość instalacji elektronicznego panelu diagnostycznego dostępnego z przodu serwera, pozwalającego uzyskać informacje min. o stanie: procesora, pamięci, wentylatorów, kary sieciowej, zasilaczy, kartach rozszerzeń, temperaturze. |
| Karta/modułzarządzający | Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP dostęp do karty zarządzającej poprzez  dedykowany port RJ45  przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy  z poziomu przeglądarki webowej (GUI)  z poziomu linii komend  poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)  wbudowane narzędzia diagnostyczne zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego  obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników  przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)  obsługa zdalnego serwera logowania (remote syslog) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów  mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie funkcja zdalnej konsoli szeregowej - przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności  monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji  konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)  zdalna aktualizacja oprogramowania (firmware)  zarządzanie grupami serwerów, w tym:  tworzenie i konfiguracja grup serwerów sterowanie zasilaniem (wł/wył)  ograniczenie poboru mocy dla grupy (power caping)  aktualizacja oprogramowania (firmware)  wspólne wirtualne media dla grupy  możliwość równoczesnej obsługi przez min. 3 administratorów  autentykacja dwuskładnikowa (Kerberos) wsparcie dla Microsoft Active Directory  obsługa SSL i SSH  enkrypcja AES/3DES dla zdalnej konsoli  wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 wsparcie dla Integrated Remote Console for Windows clients  możliwość autokonfiguracji sieci karty zarządzającej (DHCP)Rozwiązanie sprzętowe posiadające dedykowany port RJ45. |
| Wsparcie dla systemów operacyjnych i wirtualizacyjnych | Min.: Microsoft Windows Server 2016, Red Hat Enterprise Linux (RHEL) 6.9 oraz 7.3, SUSE Linux Enterprise Server (SLES) 11 SP4 oraz 12 SP2, ClearOS, CentOS, VMware ESXi 6.7 |
| Gwarancja | Z czasem reakcji NBD.Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. |

Typ 1

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor | Min. 10-rdzeniowe[[4]](#footnote-5) klasy x86 - 64 bity, osiągające w testach SPECint\_rate\_base2006 wynik nie gorszy niż 910 punktów w konfiguracji dwuprocesorowej oferowanego modelu serwera. Wynik testu musi być opublikowany na stronie www.spec.org. |
| Pamięć operacyjna | Min. 192 GB |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania min 11 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 8GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Karty Flash 8GB należy dostarczyć. |
| Kontroler | Serwer wyposażony w kontroler SATA obsługujący poziomy: RAID 0/1/10/5.Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. |
| Zasilacz | każdy o mocy minimum 500W. |

Typ 2

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor | Min. 6-rdzeniowe4 klasy x86 - 64 bity, osiągające w testach SPECint\_rate\_base2006 wynik nie gorszy niż 835 punktów w konfiguracji dwuprocesorowej oferowanego modelu serwera. Wynik testu musi być opublikowany na stronie [www.spec.org](http://www.spec.org/) |
| Pamięć operacyjna | Min. 128 GB. |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania 11 dysków SFF typu HotSwap, SAS/SATA/SSD, 2,5”Zainstalowane cztery dyski min. 480GB SSD typu MU. Zainstalowane cztery dyski min. 240GB SSD typu MU. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 8GB i redundancję danych RAID-1. Karty Flash 8GB należy dostarczyć Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. |
| Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0,1,5,6,10,50,60.Kontroler umożliwiający pracę z dyskami w trybach RAID i JBODjednocześnie |
| Zasilacz | każdy o mocy minimum 600W. |

Typ 3

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor | Min. 8-rdzeniowe4 klasy x86 - 64 bity, osiągające w testach SPECint\_rate\_base2006 wynik nie gorszy niż 906 punktów w konfiguracji dwuprocesorowej oferowanego modelu serwera. Wynik testu musi być opublikowany na stronie [www.spec.org](http://www.spec.org/) |
| Pamięć operacyjna | Min. 128 GB  |
| Sloty rozszerzeń | 3 aktywne gniazda PCI-Express Generacji 3, w tym jeden slot x16pozwalające na instalacje kart o pełnej wysokości i długości. Możliwość rozbudowy do min. 4 slotów PCI-Express generacji 3. |
| Dysk twardy | Obudowa serwera na minimum 24 dyski SFF 2,5’’ typu Hot Swap,SAS/SATA/SSD i opcja rozbudowy/rekonfiguracji o dodatkowe 6dysków typu Hot Swap, SAS/SATA/SSD.Serwer umożliwiający instalację pamięci flash w postaci kartmicroSD/SD zapewniających minimalną pojemność 8GB iredundancję danych RAID-1. Karty Flash 8GB należy dostarczyć Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.Zainstalowane minimum 8x 2.4TB SAS 10K SFF 2,5” |
| Kontroler | Kontroler sprzętowy wyposażony w 2GB cache, z mechanizmempodtrzymywania zawartości pamięci cache w razie braku zasilania,zapewniający obsługę wszystkich napędów dyskowych SAS/SATAoraz obsługujący poziomy: RAID 0,1,5,6,10,50,60.Serwer umożliwiający rozbudowę o sprzętowy kontroler RAIDzapewniający obsługę RAID 0,1,5,6,10,50,60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. |
| Zasilacz | każdy o mocy minimum 600W. |

Macierz dyskowa

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U. |
| Przestrzeń dyskowa | Macierz musi udostępniać minimum 19 TB przestrzeni RAW zbudowanej w oparciu o minimum 11 dysków w technologii SAS o prędkości obrotowej min. 10k obr/min, min. 1,5 TB przestrzeni RAW zbudowanej w oparciu o min. 2 dyski SSD. |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 180 dysków twardych.  |
| Obsługa dysków | Macierz musi obsługiwać dyski SSD, SAS i NLSAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NLSAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.  |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5 oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych.Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC.  |
| Pamięć cache | Każdy kontroler macierzowy musi być wyposażony w minimum 6 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM – nie zezwala się użycia dysków SSD.Pamięć zapisu musi być mirrorowana pomiędzy kontrolerami dyskowymi.Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 1 roku. |
| Rozbudowa pamięci cache | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy  | Macierz musi posiadać, co najmniej 4 porty FC 16 Gb/s oraz umożliwiać rozbudowę do min. 8 portów FC 16Gb/s |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i konsoli CLI. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 200 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 200 kopii migawkowych.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.  |
| Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą relokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Zdalna replikacja danych | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem. |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, Vmware. Macierz musi posiadać wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server i Microsoft Cluster. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów.Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych lub wielu serwerów. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.Wraz z macierzą mają zostać dołączone kable LC/LC OM4 o długości co najmniej 5m w ilości 8 szt.  |
| Gwarancja | Producenta, z czasem reakcji NBD. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. |

Serwer NAS

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor | Min. cztero-rdzeniowy |
| Obudowa | Rack 1U, szyny montażowe 1U w zestawie |
| Pamięć RAM | min. 4 GB RAM – możliwość rozszerzenia do min. 16 GB |
| Ilość obsługiwanych dysków | 4 dyski min. SATA III o pojemności min. 12TB każdy |
| Interfejsy sieciowe | Min: 4 x Gigabit (10/100/1000); 1 x 10GbE BASE-T |
| Porty | Min. 2x USB w tym 1x USB 3.0 |
| Wskaźniki LED | Min. status HDD 1-4, Power |
| Obsługa RAID | Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk. |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Wspierane systemy operacyjne | Microsoft Windows Server 2016, Linux, Vmware |
| Protokoły | CIFS, AFP, NFS, FTP, iSCSI, Telnet, SSH, SNMP |
| Wirtualizacja | Certyfikat zgodności Vmware Ready, Citrix Ready, Windows Server 2016 Certified. możliwość uruchomienia maszyn wirtualnych bezpośrednio na macierzy bez konieczność posiadania zewnętrznych wirtualizatorów. |
| Szyfrowanie | Szyfrowanie ze wsparciem sprzętowym całych woluminów oraz wybranych udziałów sieciowych |
| iSCSI | Wbudowany inicjator i target iSCSI |
| Replikacja | Replikacja między urządzeniami w czasie rzeczywistym |
| Kontroler domeny | Możliwość podłączenia do kontrolera domeny Microsoft |
| Liczba iSCSI LUN | Min. 64 |
| Liczba kont użytkowników | Min. 1000 |
| Liczba grup | Min. 100 |
| Liczba udziałów | Min. 100 |
| Liczba jednoczesnych połączeń | Min. 500 |
| Zasilanie | Redundantne 2x max. 350W  |
| UPS  | Obsługa sieciowych awaryjnych zasilaczy UPS. |
| Dyski | 4 dyski o pojemności: min. 6TB każdyPamięć podręczna: min. 128MBPrędkość obrotowa: min. 7200RPMMTBF: min. 2 000 000 hMaks. wew. szybkość przesyłania: min. 210 MB/s |

Zasilanie awaryjne – UPS

Typ 1

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc rzeczywista  | Min. 4200 W |
| Topologia | Podwójna konwersja on-line z korekcją współczynnika mocy (PFC) |
| Sprawność przy pracy normalnej (100% obc.) | >90 % |
| Sprawność w trybie podwyższonej sprawności (100% obc.) | >95% |
| Czas przełączenia na baterię  | Max. 1 ms |
| Możliwość pracy równoległej  | Tak |
| Czas podtrzymania dla 100% obciążenia dla pf=0,9  | Min. 15 minut |
| Czas podtrzymania przy 50% obciążenia dla pf=0,9 | Min. 40 minut |
| Dodatkowe baterie  | Możliwość dodania do min. 4 dodatkowych modułów bateryjnych w celu wydłużenia czasu podtrzymania |
| Napięcie znamionowe | Min. 200~240 V |
| Tolerancja napięci prostownika | Min. 180V – 270V |
| Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| Tolerancja częstotliwości | 40–70 Hz |
| Kształt napięcia  | Sinusoidalny |
| Napięcie znamionowe wyjściowe | Min. 220/230/240V do wyboru przez użytkownika |
| Zakres zmian napięcia przy pracy autonomicznej | +/-1% napięcia nominalnego |
| Zdolność przeciążeniowa | Min. 102–110%: 120s, 110–125%: 60s, 125–150%: 10s, >150%: 900ms |
| Częstotliwość wyjściowa przy pracy autonomicznej | 50/60 Hz +/-0,5%  |
| Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| Ochrona przed przeładowaniem | Tak |
| Ochrona przed głębokim rozładowaniem | Tak |
| Okresowy automatyczny test baterii | Tak  |
| System zarządzania pracą baterii | System nieciągłego ładowania baterii.  |
| Zdolność zwarciowa | Min. 80A |
| Możliwość uruchomienia bez napięcia w sieci | Tak |
| Baterie wewnętrzne w zestawie  | Tak |
| Interfejs komunikacyjny  |  • USB • RS232 DB-9 (HID) • styki przekaźnikowe • miniport wyłącznik ON/OFF • SNMP/Ethernet |
| Panel sterowania z wyświetlaczem LCD |  • Panel LCD obrotowy dostarczający informacji o min.: stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. • Funkcje ustawień i odczytów: lokalne wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii. • Funkcja pomiaru zużycia energii w kWh. • przyciski sterowania • wskaźniki stanu, min.: zasilanie z sieci, trybu bateryjnego, usterki  • Sygnalizator akustyczny |
| Sygnały akustyczne, min: |  • Awaria • Niski stan naładowania baterii • Przeciążenie • Serwis |
| Typ obudowy  | Uniwersalna Tower/Rack maks. 4U  |
| Wyposażenie standardowe  | * instrukcja obsługi, instrukcja bezpieczeństwa,
* 1 x kabel szeregowy RS-232,
* 1 x kabel komunikacyjny USB
* 1 x CD Oprogramowanie
* uchwyty kablowe
* zestaw szyn montażowych 19”
* podstawki do montażu wieżowego
* 1x karta sieciowa SNMP/Ethernet
 |
| Dołączone oprogramowanie  | Monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą wszystkich głównych OS, włącznie z oprogramowaniem wirtualizacyjnym, takim jak Vmware i Hyper-V.Oprogramowanie dla środowiska Vmware w formie wirtualnego dedykowanego urządzenia (Virtual Appliance) z możliwością integracji z serwerem VMware vCenter, umożliwiające zarządzanie z jednej konsoli serwerami zwirtualizowanymi oraz urządzeniami do ich zasilania. Oprogramowanie z funkcją zawieszania działania niekrytycznych maszyn wirtualnych, konsolidowania krytycznych maszyn wirtualnych, wyłączania nieużywanych serwerów i wydłużania przez to czasu pracy z akumulatora, przenoszenia maszyny wirtualnej lub łagodnego wyłączania systemu w przypadku długotrwałej przerwy w dostawie energii. |
| Zgodność ze standardem Energy Star | Tak |
| Maksymalna głębokość  | 740 mm |
| Maksymalny ciężar  | 100 kg |
| Poziom hałasu  | Max. 50 dBA dla pracy normalnej |
| Znaki bezpieczeństwa | Min. CE |
| Gwarancja producenta na baterie | Minimum 2 lata  |
| Bypass elektroniczny automatyczny i zewnętrzny bypass mechaniczny | Tak |
| Liczba, typ gniazd wyjściowych zewnętrznego bypassu mechanicznego | Min. Listwa zaciskowa, 4szt. IEC-320-C13, 2szt. IEC-320-C19 (16A) |
| Akcesoria | Czujnik monitorowania środowiska UPS umożliwiający zdalne monitorowanie temperatury, wilgotności i dwóch urządzeń stykowych podłączany do karty sieciowej SNMP.Zestawów gniazd wyjściowych PDU o prądzie nominalnym 16A podłączanych do gniazd wyjściowych IEC-320-C19 w zasilaczu awaryjnym UPS. Obudowa 0U do pionowego montażu w szafie Rack (19”) z min. 20 szt. gniazd IEC-320-C13 (10A) i 4 szt. gniazd IEC-320-C19 (16A) z blokadą przed przypadkowym wyciagnięciem kabla zasilającego na gniazdkach wyjściowych. |

Typ 2 –zapasowy

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc znamionowa | Min. 1900W |
| Topologia | Line-interactive |
| Obudowa | Do montażu w szafie Rack 19” |
| Maksymalna wysokość | Maks. 3U |
| Maksymalna głębokość | Maks. 700 mm |
| Zakres napięcia wejściowego | 180–270 V |
| System korekcji współczynnika mocy (PFC) | TAK |
| Zakres częstotliwości wejściowej | 47-70 Hz (sieć 50 Hz) / 56,5 do 70 Hz (sieć 60 Hz) |
| Napięcie nominalne wyjściowe | 220/230/240 V |
| Gniazda wyjściowe | Min. 6 szt. IEC-320-C13 (10A) |
| Sprawność | Min. 95% |
| Częstotliwość wyjściowa | 50/60 Hz +/- 0,1% (autodetekcja) |
| Możliwość dołączenia zewnętrznych modułów bateryjnych  | Min. 2 moduły bateryjne |
| Maksymalna wysokość jednego dodatkowego modułu bateryjnego | 3U |
| Czas podtrzymania dla obciążenia 100% | Min. 2 minuty |
| Czas podtrzymania dla odciążenia 50% | Min. 5 minut |
| Zarządzanie akumulatorami | System ładowania nieciągłego baterii z kompensacją temperatury, automatyczne sprawdzanie akumulatorów, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie dodatkowych zewnętrznych modułów bateryjnych, wymiana akumulatorów „na gorąco” bez konieczności wyłączania podłączonych urządzeń. |
| Interfejs użytkownika | Wyświetlacz LCD (informacje o statusie i pomiarach UPS, możliwość pomiaru zużycia energii w kWh) |
| Standardowe gniazda komunikacyjne | Karta sieciowa + 1 x styki przekaźnikowe + 1 mini złącze zdalnego zał./wył. i wyłączenia |
| Zdalne zarządzanie | * Kompatybilność z HTTP, SNMP, SMTP, Telnet, SSL, SSH
* Zdalne sterowanie i ponowne uruchamianie urządzeń chronionych przez UPS, poprzez sieć SNMP/Web,
* Konfigurowalne akcje zawierające automatyczne zamykanie systemów w przypadku przedłużających się przerw w zasilaniu
* Powiadamianie e-mailowe o alarmach
* Kompatybilność z SNMPv3 i IPv6
* Konfigurowalne automatycznie powiadamiania e-mail w odpowiedzi na alarmy UPS oraz przesyłanie raportów okresowych
* Sterowanie załączaniem i wyłączaniem UPS poprzez przeglądarkę internetową
* Ustawianie i sterowanie segmentami odbiorników poprzez interfejs przeglądarki internetowej, z sekwencyjnym załączaniem i optymalizacją czasu podtrzymania bateryjnego poprzez wcześniejsze zamykanie systemów o mniejszym znaczeniu.
* Pomiar wilgotności i temperatury z opcjonalnym czujnikiem monitorowania środowiska
* Automatyczne ustawienia daty i godziny poprzez serwer NTP
* Zabezpieczenie hasłem
* Transmisja SSL
* Zapis dziennika zdarzeń w pamięci trwałej
 |
| Poziom hałasu | Max. 50 dB |
| Temperatura pracy | Min. od 10°C do 40°C |
| Bezpieczeństwo, zakłócenia elektromagnetyczne | IEC/EN 62040-1-1 (Bezpieczeństwo), IEC/EN 62040-2 (EMC), IEC/EN 62040-3 (Charakterystyka) |
| Certyfikaty | CE, raport CB, TÜV |
| Gwarancja na akumulator | Min. 2 lata  |
| Oprogramowanie do zarządzania i monitoringu UPS | Pakiet oprogramowania kompatybilny ze wszystkimi głównymi OS, włącznie z oprogramowaniem wirtualizacyjnym, takim jak Vmware i Hyper-V. |

Typ 3 – do szafki punktów dystrybucyjnych

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc znamionowa | Min. 800W |
| Topologia | Line-interactive |
| Obudowa | Do montażu w szafie Rack 19” |
| Maksymalna wysokość | Maks. 2U |
| Maksymalna głębokość | Maks. 525 mm |
| Zakres napięcia wejściowego | 180–270 V |
| Napięcie nominalne wejściowe | 200-240 V |
| Zakres częstotliwości wejściowej | 47-70 Hz (sieć 50 Hz) / 56,5 do 70 Hz (sieć 60 Hz) |
| Napięcie nominalne wyjściowe | 220/230/240 V |
| Gniazda wyjściowe | Min. 4 szt. IEC-320-C13 (10A) |
| Sprawność | Min. 90% |
| Częstotliwość wyjściowa | 50/60 Hz +/- 0,1% (autodetekcja) |
| Możliwość dołączenia zewnętrznych modułów bateryjnych  | Min. 1 moduł bateryjny |
| Czas podtrzymania dla obciążenia 100% | Min. 3 minut |
| Czas podtrzymania dla odciążenia 50% | Min. 5 minut |
| Standardowe gniazda komunikacyjne | Min. Karta sieciowa  |
| Zdalne zarządzanie | * Kompatybilność z HTTP, SNMP, SMTP, Telnet, SSL, SSH
* Zdalne sterowanie i ponowne uruchamianie urządzeń chronionych przez UPS, poprzez sieć SNMP/Web,
* Konfigurowalne akcje zawierające automatyczne zamykanie systemów w przypadku przedłużających się przerw w zasilaniu
* Powiadamianie e-mailowe o alarmach
* Kompatybilność z SNMPv3 i IPv6
* Konfigurowalne automatycznie powiadamiania e-mail w odpowiedzi na alarmy UPS oraz przesyłanie raportów okresowych
* Sterowanie załączaniem i wyłączaniem UPS poprzez przeglądarkę internetową
* Ustawianie i sterowanie segmentami odbiorników poprzez interfejs przeglądarki internetowej, z sekwencyjnym załączaniem i optymalizacją czasu podtrzymania bateryjnego poprzez wcześniejsze zamykanie systemów o mniejszym znaczeniu.
* Pomiar wilgotności i temperatury z opcjonalnym czujnikiem monitorowania środowiska
* Automatyczne ustawienia daty i godziny poprzez serwer NTP
* Zabezpieczenie hasłem
* Transmisja SSL
* Zapis dziennika zdarzeń w pamięci trwałej
 |
| Poziom hałasu | <50 dB |
| Temperatura pracy | Min. od 10°C do 40°C |
| Bezpieczeństwo, zakłócenia elektromagnetyczne | IEC/EN 62040-1-1, IEC/EN 62040-2, IEC/EN 62040-3  |
| Certyfikaty | CE, raport CB, TÜV |
| Gwarancja na akumulator | Min. 2 lata  |
| Wyposażenie dodatkowe | Zestaw gniazd wyjściowych PDU o prądzie nominalnym min. 16A podłączany do gniazda wyjściowego IEC-320-C19 w zasilaczu awaryjnym UPS, obudowa 1U do montażu w szafie Rack (19”) z możliwością montażu w wielu położeniach z 6 szt. gniazd polskich. |

Przełączniki sieciowe

Typ 1

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Przełącznik FC o wysokości maksymalnie 1U dostosowany do montażu w szafie RACK 19” |
| Ilość portów | Przełącznik powinien posiadać minimum 24 porty z czego minimum 12 aktywnych. Możliwość pracy portów z prędkościami 16Gbps, 8Gbps, 4Gbps. |
| Wkładki fiber channel | Min. 14 wkładek fiber channel SFP+, wielomodowe, krótkodystansowe o prędkości 16 Gbit każda |
| Klasa usług | Class 2, Class 3, Class F |
| Bezpieczeństwo | SSHv2, SNMPv3, IP ACLs |
| Zarządzanie  | Oferowany przełącznik musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet RJ-45.Protokoły dostępu: CLI, SNMP, SMI-S |
| Zasilanie | Dwa redundantne zasilacze, których montaż i wymiana jest możliwa bez przerywania pracy urządzenia.  |
| Gwarancja | 5 lat z czasem reakcji NBD.Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. |
| Zgodność znormami | Zgodność z europejskimi normami:EN 60950-1, EN 55024, EN 60825, EN50082-1, EN61000-3-2, EN61000-3-3, EN61000-6-1 |

Typ 2

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Przełącznik dostosowany do montażu w szafie Rack 19”, obudowa 1U |
| Ilość portów | a) 24 porty GE, RJ-45 (w tym porty PoE w ilości co najmniej: 12, zgodne ze standardem: 802.3af oraz 802.3at.)b) 4 porty GE, SFP lub SFP+ (nie dopuszcza się portów typu combo) |
| Wkładki SFP | Min. 2 wkładki min. 1Gb |
| Wydajność | * Przepustowość urządzenia - min. 56 Gbps (pełna prędkość, na wszystkich portach) oraz min. 80 Mpps.
* Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 4 mikrosekund.
 |
| Wymagane funkcje | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
 |
| Zarządzanie  | * Wbudowany port konsoli szeregowej do zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.
 |
| Zasilanie | * Zasilanie AC 230V.
* Budżet mocy dla portów PoE min.: 180 W.
* Maksymalny pobór mocy: 220 W.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | * Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
* Routing statyczny i dynamiczny (co najmniej OSPF).
* Policy Based Routing.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
* Centralne zarządzanie sieciami VLAN.
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji pracujących w sieci.
 |

Typ 3

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Przełącznik dostosowany do montażu w szafie Rack 19”, obudowa 1U |
| Ilość portów | a) 48 portów GE, RJ-45 (w tym porty PoE w ilości co najmniej: 12, zgodne ze standardem: 802.3af oraz 802.3at.) [zezwala się na dostarczenie jednego przełącznika bez obsługi PoE – do serwerowni]b) 4 porty GE, SFP lub SFP+ (nie dopuszcza się portów typu combo) |
| Wkładki SFP | Min. 2 wkładki min. 1Gb single mode |
| Wydajność | * Przepustowość urządzenia - min. 100 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 150 Mpps.
* Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekundy
 |
| Wymagane funkcje | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
* Wsparcie dla Private VLAN.
* Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.
 |
| Zarządzanie  | * Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez GUI z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach min. 2-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.
 |
| Zasilanie | * Zasilanie AC 230V.
* Budżet mocy dla portów PoE min.: 220 W.
* Opcjonalny redundantny zasilacz.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | * Stateful firewall, umożliwiający kontrolę pomiędzy sieciami vLan.
* Routing statyczny i dynamiczny (co najmniej OSPF).
* Policy Based Routing.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC | Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: * Centralne zarządzanie sieciami VLAN.
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji pracujących w sieci.
 |

Punkty dostępowe WLAN

Parametry wspólne:

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej |
| Moduły radiowe | Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:* 1. 2.4 GHz - 802.11b/g/n,
	2. 5 GHz - 802.11a/n/ac,
 |
| Sieci WLAN | Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 8 SSID |
| Zasilanie | Urządzenie musi być zasilane poprzez interfejs ETH obsługujący 802.3af |
| Tryby pracy | * 1. Tunnel,
	2. Bridge,
	3. Mesh
 |
| QoS | 802.11e, WME/WMM Multimedia Extensions, konfigurowalne polityki QoS per użytkownik/aplikacja |
| Uwierzytelnianie | 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). |
| Interfejs radiowy | musi wspierać następujące funkcje:* 1. MIMO – 2x2,
	2. Transmit Beam Forming (TxBF),
	3. Maksymalna przepustowość dla poszczególnych modułów radiowych:
		+ 2.4GHz min. 400 Mbps;
		+ 5GHz mn. 867 Mbps;
	4. Wymagana moc nadawania min. 23 dBm,
	5. Wsparcie dla 802.11n 20/40Mhz HT,
	6. Wsparcie dla kanału 80 MHz dla 802.11ac,
	7. Anteny – 4 wbudowane anteny.
	8. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
	9. Maksymalna deklarowana liczba klientów per moduł radiowy – min. 256.
 |
| Funkcje interfejsu radiowego | 1. Skaner częstotliwości 2.4 oraz 5 GHz,
2. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
 |
| Funkcje dodatkowe | * 1. Low-Density Parity Check (LDPC) Encoding,
	2. Maximum Likelihood Demodulation (MLD),
	3. Maximum Ratio Combining (MRC),
	4. A-MPDU and A-MSDU Packet Aggregation,
	5. MIMO Power Save,
	6. Short Guard Interval,
	7. WME Multimedia Extensions
 |
| Certyfikaty | WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac); DFS |
| Uwagi | Urządzenie musi być dostarczone z elementami mocującymi |

Typ 1 – wewnętrzne

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Obudowa | Musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:* + Temperatura 10–50°C,
	+ Wilgotność 10–90%.
 |
| Interfejsy sieciowe | * 1x Ethernet – 10/100/1000 Base-TX,
* 1x USB – Typ A.
 |
| Anteny | Min. 4 wbudowane dla nadajników o zysku min. 4dBi |
| Zasilanie  | Zasilanie POE za pomocą zewnętrznych zasilaczy w jednostkach terenowych (4 szt). |

Typ 2 – zewnętrzne

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Obudowa | Musi umożliwiać montaż na słupie lub ścianie na zewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:* Temperatura -20–65°C,
* Wilgotność 10–90%.
 |
| Interfejsy sieciowe | * 2x Ethernet – 10/100/1000 Base-TX,
* 1x Optyczne – SFP 10/100/1000 Base-X
 |
| Anteny | Min. 4 wbudowane anteny standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, min. 6dBi dla pasma 5GHz |

Stanowiska robocze stacjonarne

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor/Chipset | Odpowiednie dla urządzeń typu terminal, min. 700 pkt. w teście PassMark - CPU Mark |
| Karta graficzna | Odpowiednie dla urządzeń typu terminal, min. 100 pkt. w teście PassMark - G3D Mark |
| Ekran | min. 21 cali, Full HD 1920 x 1080 @ 60 Hz, proporcje: 16:9, Powłoka antyodblaskowa/matowa |
| System operacyjny | Dostosowany do urządzeń typu cienki klient w najnowszej wersji |
| Wspierane protokoły | min.: Citrix ICA, HDX 3D & 3D Pro, Microsoft RDP 8.0, vWorkspace |
| Pamięć masowa | Min. 8GB |
| Pamięć RAM | Min. 2GB DDR3 |
| Sieć | 10/100/1000 Ethernet, możliwość dołączenia dedykowanej wewnętrznej karty bezprzewodowej – 802.11 a/b/g/n |
| Porty | min. 4 USB 2.0, 1 RJ45, 1 VGA (do podłączenia zewnętrznego komputera PC), 1 DisplayPort (do podłączenia drugiego monitora), audio jack: 1/8-cala mini, kamera HD, wbudowane głośniki i mikrofon  |
| Zarządzanie | dołączone oprogramowanie do zarządzania urządzeniami w sieci |
| Akcesoria w zestawie | Klawiatura i mysz przewodowe, Podstawka stała lub z regulacją wysokości, złącze VESA |
| Moc pobierana | <35W średnio |
| Zasilanie: | 220-240V @ 50Hz |
| Wymiary (szer. x głęb. x wys) | 550mm x 200mm x 420mm  |
| Waga | max. 6,5kg  |
| Temperatura pracy | min. 10° do 40° C  |
| Certyfikaty | TÜV-GS, EN 60950 RF Interference: FCC Class B, Ergonomics CE, VCCI, RoHS Compliant  |

Stanowiska robocze mobilne

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Przekątna ekranu LCD | od 14 do 16 cali  |
| System operacyjny | 64-bitowy, okienkowy z wbudowaną przeglądarką internetową, pozwalający na podłączenie do domeny i zarządzanie z jej poziomu logowaniem do konta użytkownika i administratora oraz konfigurację systemu za pomocą Active Directory Group Policy |
| Ekran LCD | min. 1366 x 768 pikseli, antyrefleksyjna / matowa |
| Procesor | min. 3100 pkt. w teście PassMark - CPU Mark. 64-bit |
| Pojemność dysku SSD | min. 100 GB  |
| Wielkość pamięci RAM | min. 6 GB  |
| Karta graficzna | min. zintegrowana |
| Interfejsy, min. | 1 x D-Sub 1 x HDMI 1 x USB i 2 x USB 31 x LAN 1 Gbps 1 x WiFi IEEE 802.11ac  |
| Czytnik kart pamięci | Min. SD |
| Napęd optyczny | DVD+/-RW DL  |
| Zasilanie | Akumulator, min czas pracy na akumulatorze 4h |
| Dźwięk | stereo |
| Kolor obudowy | ciemny  |
| Klawiatura | wydzielona klawiatura numeryczna  |
| Wymiary (szer. x głęb. x wys.) | max. 400mm x 270mm x 25mm |
| Waga | max. 2,3 kg  |
| Dodatkowe wyposażenie | kamera 0.3 Mpix; wbudowany mikrofon; możliwość zabezpieczenia linką Kensington Lock; szyfrowanie TPM |

Tablety medyczne

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Ekran | dotykowy min.: 10 cali, max. 11 cali rozdzielczość min.: 1280x800 z digitizerem, jasność min.: 600 nitów |
| Procesor | min.: 2 rdzeniowy @ min. 1.5GHz |
| Bateria | zapewniająca do 8 godzin pracy, łatwa do wymiany bateria typu hot-swap |
| Pamięć RAM | min.: 1GB |
| Pamięć masowa | wewnętrzna min.: 16GB, zewnętrzna: MicroSD SDH do min: 16GB |
| Łączność bezprzewodowa | 802.11 a/b/g/n, Bluetooth® 4.0 + EDR, HF RFID/NFC |
| Porty | USB Type A & Type B (microUSB) |
| Czytnik kodów kreskowych | 1D i 2D |
| Czujniki | temperatury, oświetlenia, akcelerometr, GPS |
| Wytrzymałość | IP67, odporność na upadek z 1m, standard MIL-STD-810G |
| Kamera | min.: tył 5.0Mp AF z lampą błyskową |
| Audio | głośniki, złącze słuchawkowe jack 3.5mm, mikrofon |
| Zasilanie | wewnętrzne 240VAC. zewnętrzne: 5VDC, min. 1.5A DC |
| Temperatura pracy | min.: 0 do +40°C |
| Certyfikaty | CE/CB - CE (R&TTE), FCC, NCC/BSMI, CCC, IP67 |
| Waga | poniżej 1kg |

Urządzenia wielofunkcyjne A3

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Wielofunkcyjny kolor A3 |
| Technologia | Laser Kolor |
| Prędkość drukowania i kopiowania | min. 20 str. A4 / 10 str. A3 na minutę w kolorze i mono |
| Rozdzielczość | min. 1200 x 1200 dpi |
| Czas nagrzewania | max. 30 sekund |
| Czas pierwszego wydruku | max. 12 sekund |
| Czas pierwszej kopii | max. 12 sekund |
| Waga | max. 100 kg |
| Maksymalny pobór mocy | drukowanie: 1600 W, tryb gotowości: 75 W, tryb uśpienia: 5 W |
| Napięcie zasilania | AC 220 V – 240 V, 50/60 Hz |
| Poziom hałasu (ISO 7779) | max. 62 dB(A) |
| Certyfikaty | min. CE |
| Pamięć | min. 2 GB RAM + min. 16 GB dysk |
| Pojemność wejściowa | taca uniwersalna na min. 100 ark. podajnik kasetowy min. 2 x min. 500 ark. |
| Moduł dupleksu | W standardzie, obsługa papieru min. 75–220 g/m² |
| Pojemność wyjściowa | min. 500 arkuszy |
| Rozmiar papieru | A6 - A3  |
| Emulacje | PCL 6 (PCL5c / PCL-XL), zgodna z Postscript 3, bezpośrednie drukowanie XPS, PDF oraz Open XPS |
| Dodatkowe możliwości drukowania | druk bezpośredni PDF, drukowanie IPP, e-mail printing, wydruk bezpieczny przez SSL, SNMPv2 i 3, wydruk prywatny |
| Obsługiwane Systemy Operacyjne (wydruk) | Wszystkie bieżące wersje Microsoft Windows, Mac OS X wersja 10.5 lub wyższa, UNIX, LINUX  |
| Maksymalny rozmiar oryginału | A3 |
| Dodatkowe możliwości kopiowania | pomijanie pustych stron |
| Typy ekspozycji | Automatyczna, ręczna: min. 6 stopni |
| Zakres zoom | min. 25 - 200 % |
| Rozpoznawanie oryginału | Tekst + zdjęcie, zdjęcie, tekst, jasny tekst, tekst (zoptymalizowany pod OCR) |
| Maksymalny format skanowania | A3 |
| Funkcjonalności skanera | Skan do e-mail, skan do FTP, skan do SMB, skan do USB Host, skan do skrzynki, TWAIN sieciowy, skan WSD |
| Maksymalna rozdzielczość skanowania | min. 600 x 600 dpi |
| Prędkość skanowania | min. 120 obrazów na minutę w kolorze i mono (A4, 300dpi) |
| Interfejsy | min. 2 x USB 2.0 (Hi-Speed), USB Host 2.0, Fast Ethernet 10Base-T/100BaseTX/1000BaseT, gniazdo na kartę SD |
| Funkcjonalność niszczenia niechcianych wydruków |
| Ilość jednorazowo niszczonych kartek | min. 8 arkuszy |
| Rodzaj cięcia | Ścinki |
| Pojemność kosza | min. 12 l |
| Niszczenie zszywek i małych spinaczy | Tak |
| Rozmiar ścinek | maks. 5 x 40 mm |
| Dodatkowe | Do urządzenia musi zostać dostarczony komplet tonerów [nie „startowych”] i innych materiałów eksploatacyjnych pozwalających na używanie drukarki od razu po instalacji.Urządzenie musi zostać zainstalowane na dedykowanej szafce z kółkami. [dostarczonej wraz z urządzenem] |

Drukarki laserowe A4

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ drukarki | Monochromatyczna - A4  |
| Technologia | Laser |
| Szybkość | min. 12 stron na minutę - A4 |
| Rozdzielczość | min. 1200 dpi |
| Czas nagrzewania | max. 20 sek. |
| Czas do pierwszego wydruku | max. 12 sek. |
| Wymiary maksymalne (Szer. x Głęb. x Wys.) | 370 × 300 × 250 mm |
| Waga | max. 10 kg |
| Pobór mocy | Drukowanie: max 550 W, Stand-by: max 15 W, Sleep: max. 5 W |
| Napięcie zasilania | AC 220 ~ 240 V, 50/60 Hz |
| Hałas zgodność (ISO 7779) | max. 63 dB(A) |
| Certifikaty | min. CE |
| Ogólnie o pamięci | min. 8 MB RAM |
| Pojemność wejściowa | min. 250 arkuszy A4 |
| Moduł dwustronny | Standard |
| Pojemność wyjściowa | min. 120 arkuszy A4 |
| Obsługiwane Systemy Operacyjne (Wydruk) | min. Windows XP/Vista/7/8/Server 2003/Server 2008/Server 2012 |
| Standardowe interfejsy | min. USB 2.0, FastEthernet (10/100BaseTX) |
| Funkcjonalność niszczenia niechcianych wydruków |
| Ilość jednorazowo niszczonych kartek | min. 5 arkuszy |
| Rodzaj cięcia | min. paski |
| Pojemność kosza | min. 10 l |
| Dodatkowe | Do urządzenia musi zostać dostarczony komplet tonerów [nie „startowych”] i innych materiałów eksploatacyjnych pozwalających na używanie drukarki od razu po instalacji. |

Skanery dokumentów

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ skanera | płaski |
| Element światłoczuły | CIS |
| Rozdz. optyczna w pionie | min. 2400 dpi  |
| Rozdz. optyczna w poziom. | min. 4800 dpi  |
| Wewnętrzna głębia koloru | min. 48 bit  |
| Zewnętrzna głębia koloru | min. 24 bit |
| Głębia szarości | min. 16 bit |
| Przyciski funkcyjne | min. 3 |
| Maks. obszar skanowania | min. A4 |
| Interfejs | min. USB 2.0 |
| Waga | max. 4 kg |

Drukarki opasek dla pacjentów

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Termiczny druk kodów kreskowych, tekstu i grafiki |
| Obudowa | Podwójne ścianki, odporne na uderzenia tworzywo sztuczne odporne na działanie środków czyszczących stosowanych w placówkach medycznych, odporne na różne środki odkażające, chemiczne i czyszczące |
| Pamięć Flash  | min. 512 MB |
| Pamięć RAM  | min. 256 MB |
| Łączność i interfejsy | min. USB, Ethernet |
| Certyfikaty | min. ENERGY STAR® |
| Wymiary (szer. × wys. × gł.)  | maks. 150mm × 200mm × 250mm |
| Maks. długość druku  | min. 500 mm |
| Min. długość druku  | min. 60 mm |
| Rozdzielczość  | min. 300 dpi (12 pkt/mm) |
| Maks. szybkość druku  | min. 50 mm/sek. |
| Obsługa opasek  | Z zapięciem samoprzylepnym lub na zatrzask; Opcje opasek jedno- i wielodniowych |
| Zasilacz  | 220-240 V AC, 50-60 Hz |
| Obsługa kodów kreskowych | Kody liniowe: Code 11, Code 39, Code 93, Code 128, EAN-8, EAN-13, EAN-14, GS1 DataBar™, Plessey, Postnet, UPC-A, UPC-E, UPC-A i UPC-E z 2- lub 5-cyfrowymi rozszerzeniami EANKody dwuwymiarowe min.: Code 49, Data Matrix, MaxiCode, MicroPDF417, PDF417, kody QR |
| Dodatkowe informacje | Licznik opasek na rękę, wskaźnik niskiego poziomu/braku nośnika, ładowanie wkładów z opaskami bez narzędzi, wymiana głowicy drukującej i wałka bez narzędzi, zgodność ze standardem Unicode™ do druku wielojęzycznego, automatyczna kalibracja nośnika, czujnik uniesienia głowicyDrukarki należy dostarczyć z min. 5 kasetami opasek białych – medycznych dla każdej drukarki. |

Zabezpieczenie e-Usług

Firewall – UTM

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Typ 1 – jednostki terenowe

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Platforma sprzętowa,  |
| Porty LAN | Min. 7 portów Gigabit Ethernet RJ45 |
| Port USB | Min. 1 szt. z możliwością podłączenia modemu 3G/4G |
| Obsługa VLAN | Min. 200 interfejsów wirtualnych 802.1Q |
| Funkcje UTM | Min.: Firewall, IPSec, Kontrola Aplikacji, IPS, DLP, IPSec VPN, SSL VPN, Antywirus, Antyspam, Routing, QoS, analiza ruchu SSL, filtrowanie stron www |
| Wydajność Firewall | Min. 1.7 mln jednoczesnych połączeń oraz 20000 nowych połączeń na sekundę,  |
| Przepustowość Stateful Firewall | Min. 2 Gbps |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji | Min. 400 Mbps |
| Wydajność szyfrowania VPN IPSec  | Min. 90 Mbps [dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256] |
| Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami min.: IPS, Application Control, Antywirus | Min. 150 Mbps |
| Wydajność skanowania ruchu z ochroną przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix | Min. 350 Mbps |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https | Min. 180 Mbps |
| Klastrowanie | Możliwość łączenia w klaster Active-Active lub Active-Passive z funkcją synchronizacji sesji firewall |
| Monitorowanie | * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
* Monitoring stanu realizowanych połączeń VPN.
 |
| Uwierzytelnianie | Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania 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.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.

Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| Chronione protokoły | * przed malware – dla protokołów min: SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
* Antyspam - dla protokołów min: SMTP, POP3, IMAP.
 |
| Polityki bezpieczeństwa | * Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
* System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu.
* W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 |
| IPSec VPN | * Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* 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. „Split tunneling” dla połączeń Client-to-Site.
 |
| SSL VPN | * Praca w trybie Portal - dostęp do chronionych zasobów realizowany za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML
* Praca w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta
 |
| Routing | Rozwiązanie musi zapewniać obsługę:* Routingu statycznego.
* Policy Based Routingu.

Wsparcie dla protokołów dynamicznego routingu w oparciu o protokoły min.: OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
| Antywirus | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).System musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR.System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| IPS | * Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
* Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
* Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
* System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS / DDoS.
* Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojanami, Exploitami, Robotami) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
* Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |
| Kontrola aplikacji | * Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów (DPA), nie bazując jedynie na wartościach portów TCP/UDP.
* Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie.
* Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
* Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa, np.: proxy, P2P.
* Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |
| Kontrola WWW | * Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
* 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 avoidance.
* Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
* Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
* System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
* Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania
 |
| Zarządzanie | * 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.
* Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
* Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
* System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach min. 2, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
* System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
* System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
 |
| Logowanie zdarzeń | * System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
* 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.
* Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
* Musi istnieć możliwość logowania do serwera SYSLOG
 |
| Zarządzanie pasmem | * System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
* Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
* System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL
 |
| Certyfikaty | * ICSA lub EAL4 dla funkcji Firewall.
* ICSA lub NSS Labs dla funkcji IPS.
* ICSA dla funkcji IPSec VPN.
* ICSA dla funkcji SSL VPN.
 |
| Licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Muszą one obejmować: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 60 miesięcy |

Typ 2 – jednostka centralna

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ urządzenia | Platforma sprzętowa,  |
| Porty LAN | Min. 16 portów Gigabit Ethernet RJ45, min. 2 porty SFP min. 1 Gbps |
| Port USB | Min. 1 szt. z możliwością podłączenia modemu 3G/4G |
| Obsługa VLAN | Min. 200 interfejsów wirtualnych 802.1Q |
| Funkcje UTM | Min.: Firewall, IPSec, Kontrola Aplikacji, IPS, DLP, IPSec VPN, SSL VPN, Antywirus, Antyspam, Routing, QoS, analiza ruchu SSH oraz SSL, filtrowanie stron www |
| Wydajność Firewall | Min. 2 mln jednoczesnych połączeń oraz 30000 nowych połączeń na sekundę,  |
| Przepustowość Stateful Firewall | Min. 7 Gbps dla pakietów 512 B. |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji | Min. 1 Gbps |
| Wydajność szyfrowania VPN IPSec  | Min. 3 Gbps [dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256] |
| Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami min.: IPS, Application Control, Antywirus | Min. 250 Mbps |
| Wydajność skanowania ruchu z ochroną przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix | Min. 500 Mbps |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https | Min. 180 Mbps |
| Klastrowanie | Możliwość łączenia w klaster Active-Active lub Active-Passive z funkcją synchronizacji sesji firewall |
| Monitorowanie | * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
* Monitoring stanu realizowanych połączeń VPN.
 |
| Uwierzytelnianie | Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania 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.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.

Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| Chronione protokoły | * przed malware – dla protokołów min: SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
* Antyspam - dla protokołów min: SMTP, POP3, IMAP.
 |
| Polityki bezpieczeństwa | * Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
* System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu.
* W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 |
| IPSec VPN | * Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* 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. „Split tunneling” dla połączeń Client-to-Site.
 |
| SSL VPN | * Praca w trybie Portal - dostęp do chronionych zasobów realizowany za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML
* Praca w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta
 |
| Routing | Rozwiązanie musi zapewniać obsługę:* Routingu statycznego.
* Policy Based Routingu.

Wsparcie dla protokołów dynamicznego routingu w oparciu o protokoły min.: OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
| Antywirus | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).System musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR.System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| IPS | * Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
* Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
* Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
* System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS / DDoS.
* Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojanami, Exploitami, Robotami) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
* Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |
| Kontrola aplikacji | * Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów (DPA), nie bazując jedynie na wartościach portów TCP/UDP.
* Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie.
* Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
* Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa, np.: proxy, P2P.
* Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |
| Kontrola WWW | * Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
* 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 avoidance.
* Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
* Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
* System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
* Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania
 |
| Zarządzanie | * 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.
* Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
* Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
* System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach min. 2, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
* System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
* System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
 |
| Logowanie zdarzeń | * System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
* 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.
* Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
* Musi istnieć możliwość logowania do serwera SYSLOG
 |
| Zarządzanie pasmem | * System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
* Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
* System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL
 |
| Certyfikaty | * ICSA lub EAL4 dla funkcji Firewall.
* ICSA lub NSS Labs dla funkcji IPS.
* ICSA dla funkcji IPSec VPN.
* ICSA dla funkcji SSL VPN.
 |
| Licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Muszą one obejmować: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 60 miesięcy |

Antywirus

W ramach postępowania Wykonawca dostarczy oprogramowanie antywirusowe wraz z oprogramowaniem centralnej konsoli lub zarządzalne z dostarczanych urządzeń UTM. Oprogramowanie antywirusowe musi pracować na systemach: Windows 10, Windows Server 2016, systemie zainstalowanych ma dostarczanym tablecie medycznym, Android ver. min. 5.

Oprogramowanie antywirusowe musi dostarczać min.:

* Ochronę antywirusową w czasie rzeczywistym i wykrywanie grayware (adware, riskware),
* Ochronę przed Ransowmare,
* Ochronę przed Malware,
* Filtr stron www bazujący na kategoryzacji stron,
* Ochronę przed stronami ze szkodliwą zawartością,
* Ochronę przed phishingiem,
* Ochronę przed spamem

Funkcja zarządzania musi pozwalać min. na zdalne wymuszenie aktualizacji klienta, zdalne wywołanie skanowania komputera.

Kopie zapasowe

Wykonawca w ramach postępowania dostarczy, zainstaluje i wdroży automatyczny system wykonywania kopii bezpieczeństwa zainstalowanych systemów wirtualnych i fizycznych. Wdrożony system kopii bezpieczeństwa musi współpracować w dostarczonym hypervisorem i spełniać następujące parametry:

* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji min. 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
* Oprogramowanie musi być licencjonowanie w modelu “per-CPU” lub „per Serwer”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczone bjaty danych , dodatkowo płatna deduplikacja) nie jest dozwolone
* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi posiadać wbudowane mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej dwóch pamięci masowych w takiej puli.
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie ASI wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez ASI poziomy latencji.
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie
* Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	+ **Linux :** ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
	+ **Windows :** NTFS, FAT, FAT32, ReFS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
* Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
* Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

System zarządzania i monitorowania infrastruktury serwerów

System zarządzania infrastrukturą wirtualizacji serwerów musi spełniać następujące kryteria:

1. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
2. Pojedynczy klaster może się skalować min. do 16 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
3. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi obsłużyć
i wykorzystać procesory fizyczne wyposażone w min 256 logicznych wątków oraz do min. 8 TB pamięci fizycznej RAM.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych min. od 1 do 64 procesorowych.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do min. 4 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć min. do 10 wirtualnych kart sieciowych.
8. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
11. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 10, Debian GNU/Linux, CentOS, FreeBSD, CoreOS.
12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem HTML.
15. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
16. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
18. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
19. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
20. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych.
21. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
22. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
23. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
24. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
25. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.
26. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do min. 4000 portów.
27. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
28. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

System monitorowania infrastruktury serwerów wirtualnych musi spełniać następujące kryteria:

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
* System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych:
	+ Microsoft Windows 2012 R2
	+ Microsoft Windows 2016
	+ Microsoft Windows 7 z SP1
	+ Microsoft Windows 10
* System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:
	+ Microsoft SQL Server 2012 R2
	+ Microsoft SQL Server 2014
	+ Microsoft SQL Server 2016
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej n
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie min. HTML
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
* Silnik raportowania powinien być oparty o SQL w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.0, vCenter Server 5.x oraz 6.0 jak również Microsoft Hyper-V 2012 R2i 2016.
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi instalować się na następujących systemach operacyjnych:
	+ Microsoft Windows 7 SP1
	+ Microsoft Windows 2012 R2
	+ Microsoft Windows 10
	+ Microsoft Windows 2016
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
* System musi mieć możliwość eksportowania raportów min. do formatów Microsoft Word, Microsoft Excel, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
* Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić 1 godzinę lub krótszy
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Licencje

W ramach postępowania należy dostarczyć wszystkie licencje wymagane do uruchomienia oraz użytkowania dostarczanych urządzeń i serwerów zgodnie z ich przeznaczeniem i niniejszym SIWZ. Licencje terminowe, subskrypcje, abonamenty, itp. muszą pozwalać na użytkowanie każdego elementu Systemu przez okres min. 60 miesięcy od dnia podpisania protokołu końcowego.

Wykonawca określi ilości i rodzaje licencji wymaganych do realizacji Projektu inne niż wymagane, tj.:

* Microsoft Windows Server – zgodnie z warunkami licencjonowania do uruchomienia co najmniej 12 maszyn wirtualnych na wszystkich dostarczonych serwerach fizycznych.
* Microsoft CAL [device] – nie mniej niż 140 szt.
* Microsoft RDP CAL [device] – nie mniej niż 140 szt.
* Antywirusowe – nie mniej niż 100 szt.
* System kopii bezpieczeństwa – zgodnie z warunkami licencjonowania do wykonywania kopii bezpieczeństwa wszystkich zainstalowanych systemów [zarówno fizycznych jak i wirtualnych].
* System wirtualizacji (jeśli wymagane) – zgodnie z warunkami licencjonowania do uruchomienia co najmniej 100 maszyn wirtualnych na wszystkich dostarczonych serwerach.

W celu realizacji funkcji powiadamiania w ramach e-Usług, wymagane jest dostarczenie i skonfigurowanie pakietu wiadomości SMS w systemie HIS. Pakiet musi pozwolić na wysyłane wiadomości SMS w okresie co najmniej 60 miesięcy.

Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego

Wszystkie dostarczane urządzenia muszą zostać zainstalowane [tj. wypakowane, zmontowane, zamontowane w szafach rack lub na biurkach, uruchomione i skonfigurowane] w docelowym miejscu pracy [wskazanym przez Zamawiającego] w terminie wskazanym przez Zamawiającego [miejsce i termin instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń]. Wszystkie opakowania zostaną zutylizowane przez i na koszt Wykonawcy.

**Wszystkie urządzenia i systemy operacyjne serwerów muszą być zsynchronizowane z lokalnym serwerem czasu.**

Serwery

Na serwerach należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy w możliwie najszybszy sposób. Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia. Wykonawca zaprojektuje i wdroży system backupu min. maszyn wirtualnych.

Macierz dyskowa

Macierz musi zostać zainstalowana w serwerowni. Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób.

Serwer NAS

Serwer NAS musi zostać zainstalowany w serwerowni. Zasoby serwera NAS posłużyć mają do przechowywania dodatkowych kopii bezpieczeństwa systemów zainstalowanych w serwerowni. NAS musi zostać podłączony do sieci wewnątrz serwerowej.

Zasilanie awaryjne – UPS

Wszystkie dostarczone urządzenia UPS muszą posiadać aktywne karty sieciowe pozwalające na monitorowania za pomocą min.: Interfejsu WEB oraz protokołu SNMP w wersji 2 oraz 3. Wszystkie zasilacze awaryjne muszą zostać skonfigurowane w taki sposób, aby w przypadku zaniku napięcia w sieci energetycznej wysyłana była wiadomość e-mail do ASI oraz aby rejestrowany był ten fakt w centralnym systemie logów lub systemie monitorowania serwerów i usług za pomocą SNMP Trap [włącznie z informacją o przywróceniu napięcia]. Dodatkowo za pomocą SNMP traps rejestrowane muszą być wszystkie inne zdarzenia mogące mieć wpływ na działanie systemów i ich bezpieczeństwo [np. konieczność wymiany baterii czy przeciążenie]. W systemie zarządzania należy utworzyć dwóch użytkowników z prawami administracyjnymi [jeden dla ASI, jeden dla serwisu]. Jeśli interfejs posiada konto „gościa” należy je wyłączyć. Wszystkie możliwe protokoły sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepowołanym dostępem. Wszystkie UPSy muszą zostać zainstalowane w szafach RACK w przeznaczony przez producenta do tego celu sposób [np. za pomocą odpowiednich szyn lub uchwytów]. UPSy muszą zostać podłączone do sieci LAN poprzez dedykowany interfejs zarządzania do odpowiedniego portu na przełączniku sieciowym [odpowiedni vlan!]

Przełączniki sieciowe

Na wszystkich przełącznikach sieciowych należy skonfigurować SNMP oraz SNMP traps do korzystania z systemu monitorowania i przesyłania alarmów do ASI. Na każdym urządzeniu należy utworzyć dwóch użytkowników z uprawnieniami administracyjnymi [jeden dla ASI, jeden dla serwisu]. Na wszystkich przełącznikach muszą zostać skonfigurowane vLany oraz reguły zabezpieczenia DHCP [jeśli wymagane]. Sieć zarządzania należy wydzielić do oddzielnego vLANu.

Typ 1

Należy skonfigurować przełączniki do obsługi ruchu iSCSI oraz FC. Serwery i macierz należy podłączyć kablami światłowodowymi. Przełączniki należy skonfigurować w trybie HA.

Typ 2

Przełączniki należy skonfigurować do obsługi AP i zasilania PoE.

Typ 3

Przełączniki należy skonfigurować do obsługi AP i zasilania PoE.

Punkty dostępowe WLAN

Wszystkie punkty dostępowe Wykonawca podłączy [zarówno fizycznie jak i logicznie] do centralnego systemu zarządzania siecią WLAN oraz zainstaluje wszystkie wymagane licencje dostępowe dla kontrolera i punktów dostępowych. Wszystkie punkty dostępowe muszą być zasilane za pomocą PoE – nie dopuszcza się stosowania zasilaczy podłączanych bezpośrednio do punktów.

Wszystkie punkty dostępowe muszą być zainstalowane w miejscach lub w sposób uniemożliwiający kradzież [np. ponad sufitem podwieszanym lub na wysokości uniemożliwiającej zdjęcie punktu bez użycia drabiny].

Jeśli punkty dostępowe posiadają własne ustawienia protokołu SNMP [poza konsolą centralną / kontrolerem] należy skonfigurować protokół w celu monitorowania urządzeń przez centralny system monitorowania.

Typ 1 – wewnętrzne

Zamawiający nie specyfikuje dodatkowych wymogów.

Typ 2 – zewnętrzne

Punkty muszą być zabezpieczone zgodnie z instrukcją instalacji producenta przed działaniem czynników zewnętrznych występujących w szerokości geograficznej instalacji sprzętu [temperatury, opady, mróz, szron, itp.].

Stanowiska robocze stacjonarne

Konfiguracja urządzeń polegać będzie na:

* Podłączeniu fizycznym do sieci LAN oraz elektrycznej
* skonfigurowaniu adresu IP na serwerze DHCP dla terminala,
* skonfigurowaniu terminala na serwerze Active Directory,
* konfiguracji SNMP oraz SNMP traps do korzystania z systemu monitorowania.
* konfiguracji interfejsu zarządzania [jeśli posiada], konfiguracji synchronizacji z lokalnym serwerem czasu.

Stanowiska robocze mobilne

Konfiguracja urządzeń polegać będzie na:

* zainstalowaniu lub przeprowadzeniu pierwszego uruchomienia systemu operacyjnego, wraz z aktywacją systemu [jeśli wymagana] oraz utworzeniem użytkowników lokalnych,
* podłączeniu komputera do domeny Active Directory,
* konfiguracji połączenia RDP,
* instalacji i konfiguracji systemu antywirusowego,
* instalacji i konfiguracji połączenia VPN,
* konfiguracji synchronizacji z lokalnym serwerem czasu.

Tablety medyczne

Konfiguracja urządzeń polegać będzie na:

* przeprowadzeniu pierwszego uruchomienia systemu operacyjnego, wraz z aktywacją systemu [jeśli wymagana] oraz utworzeniem użytkowników lokalnych,
* podłączeniu do domeny Active Directory [jeśli wymagane],
* konfiguracji połączenia do systemu HIS,
* instalacji i konfiguracji systemu antywirusowego,
* instalacji i konfiguracji połączenia VPN,
* konfiguracji synchronizacji z lokalnym serwerem czasu [jeśli możliwe].

Urządzenia wielofunkcyjne A3

Konfiguracja urządzeń polegać będzie na:

* podłączeniu fizycznym drukarek do sieci LAN lub do komputerów [lub terminali],
* skonfigurowaniu adresu IP na serwerze DHCP dla drukarki [jeśli podłączona do sieci LAN],
* skonfigurowaniu drukarki w systemach operacyjnych komputerów w miejscu użytkowania lub na serwerze RDP, oraz serwerze Active Directory,
* konfiguracji SNMP oraz SNMP traps do korzystania z systemu monitorowania.
* konfiguracji interfejsu webowego [min. utworzenie użytkownika z uprawnieniami administracyjnymi dla ASI], konfiguracja synchronizacji z lokalnym serwerem czasu.

Drukarki laserowe A4

Konfiguracja urządzeń polegać będzie na:

* podłączeniu fizycznym drukarek do sieci LAN lub do komputerów [lub terminali],
* skonfigurowaniu adresu IP na serwerze DHCP dla drukarki [jeśli podłączona do sieci LAN],
* skonfigurowaniu drukarki w systemach operacyjnych komputerów w miejscu użytkowania lub na serwerze RDP, oraz serwerze Active Directory,
* konfiguracji SNMP oraz SNMP traps do korzystania z systemu monitorowania.
* konfiguracji interfejsu webowego [min. utworzenie użytkownika z uprawnieniami administracyjnymi dla ASI], konfiguracja synchronizacji z lokalnym serwerem czasu.

Skanery dokumentów A4

Konfiguracja urządzeń polegać będzie na:

* podłączeniu fizycznym skanerów do komputerów [lub terminali] lub sieci LAN,
* skonfigurowaniu adresu IP na serwerze DHCP dla skanera [jeśli podłączony do sieci LAN],
* skonfigurowaniu skanera w systemach operacyjnych komputerów w miejscu użytkowania lub na serwerze RDP, oraz serwerze Active Directory [jeśli wymagane],
* jeśli w miejscu instalacji skaner ma służyć większej liczbie użytkowników/ komputerów należy skonfigurować odpowiedni udział sieciowy do przechowywania skanowanych dokumentów i udział ten zamontować na wszystkich niezbędnych komputerach / profilach lub skonfigurować skanowanie sieciowe jeśli skaner posiada taką funkcję.

Zabezpieczenie e-Usług

Wykonawca dokona instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.

Wykonawca wdroży [tj. zainstaluje, uruchomi, skonfiguruje i przetestuje] infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerze fizycznym Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem [np. Active Directory, DHCP, DNS, RDP, etc.].

Firewall – UTM

W konfiguracji urządzeń muszą zostać włączone min. usługi:

* ochrony przed atakami typu DoS/DDoS, itp.,
* ochrony antywirusowej,
* web filter,
* IDS/IPS.

Typ 1 – jednostki terenowe

Wszystkie zainstalowane w jednostkach terenowych urządzenia muszą łączyć się z centralnym urządzeniem za pomocą bezpiecznego kanału transmisji – VPN – połączenie musi następować automatycznie po jego zerwaniu lub uruchomieniu urządzenia.

Typ 2 – jednostka centralna

Uruchomiony w centralnej lokalizacji Firewall musi zostać skonfigurowany w taki sposób, aby jednostki terenowe łączyły się z centralą za pośrednictwem bezpiecznego kanału transmisji – VPN.

Instalowane urządzenie musi chronić zainstalowane wewnątrz sieci Zamawiającego serwery aplikacyjne e-Usług [głównie przed atakami typu DoS].

Antywirus

Dostarczony system antywirusowy musi zostać zainstalowany i skonfigurowany na wszystkich komputerach w taki sposób aby możliwe było zarządzanie wszystkimi klientami z konsoli centralnej, na wszystkich dostarczanych urządzeniach. Dodatkowo należy przekazać lokalnemu ASI pliki instalacyjne, pliki licencji oraz instrukcję instalacji i konfiguracji klienta w celu współpracy z centralną konsolą zarządzającą. Do centralnej konsoli musi mieć pełen dostęp lokalny ASI – również zdalny.

Systemy monitorowania serwerów i usług

W ramach Zamówienia należy wdrożyć (tj. zainstalować i skonfigurować) system monitorowania serwerów i usług wraz z centralnym systemem logów. System musi pozwalać na zebranie logów ze wszystkich zainstalowanych w Szpitalu systemów i usług oraz przeszukiwanie zgromadzonych logów na podstawie wbudowanych filtrów z możliwością definiowania własnych filtrów. System powinien posiadać możliwość generowania wykresów w czasie rzeczywistym z napływających danych na tzw. dashboard’zie. Wszystkie urządzenia oraz usługi sieciowe należy skonfigurować w taki sposób aby wysyłały one swoje logi systemowe do centralnego systemu. Na wszystkich urządzeniach udostępniających funkcjonalność SNMP muszą zostać skonfigurowane tzw. pułapki wysyłające alerty do systemu monitorowania. System monitorowania powinien dodatkowo pobierać okresowo informacje o urządzeniach poprzez protokół SNMP [okresy pomiędzy zapytaniami powinny być definiowane dla każdego urządzenia lub grup/typów urządzeń].

Kopie zapasowe

Wykonawca we współpracy z ASI opracuje politykę kopii bezpieczeństwa uwzględniającą możliwości techniczne po wdrożeniu Projektu. Na podstawie polityki Wykonawca skonfiguruje systemy i usługi do wykonywania kopii bezpieczeństwa zgodnie z harmonogramami. Przetestuje działanie mechanizmu automatycznego wykonywania kopii bezpieczeństwa i po okresie 30 dni od uruchomienia harmonogramu oceni skuteczność wdrożonych mechanizmów. W ramach wdrożenia musi zostać dostarczona instrukcja odtwarzania danych w różnych zakresach [np.: pojedynczy plik, cały katalog, użytkownik wraz z plikami, maszyna, itp.]. Wszystkie kopie muszą być zapisywane również na dodatkowym serwerze NAS.

Architektura HA dla serwera aplikacji

W celu zapewnienia wysokiej dostępności e-Usług należy uruchomić minimum 2 wirtualne serwery aplikacji na minimum 2 serwerach fizycznych. Serwery aplikacji musza zostać uruchomione w trybie zapewniającym bezpieczną i nieprzerwaną pracę nawet w przypadku wyłączenia 75% serwerów aplikacji. W celu wyeliminowania pojedynczego punktu awarii usługa load-balancing’u również musi zostać uruchomiona w trybie HA (np. z wykorzystaniem DNS round-robin). W celu zapewnienia rozliczalności danych w trybie HA muszą zostać uruchomione zarówno serwery load-balancing’u oraz aplikacji dla HIS jak i e-Usług. W przypadku serwerów aplikacji dla HIS liczba uruchamianych serwerów wirtualnych wynosi min. 4 na dwóch serwerach fizycznych. Wszystkie krytyczne usługi [tj. min. 1 serwer aplikacji dla e-Usług oraz min. 1 serwer aplikacji dla HIS] muszą zostać również uruchomione na serwerze zapasowym. W celu sprawnej i nieprzerwanej pracy Wykonawca zobowiązany jest do utworzenia systemu aktualizacji wszystkich serwerów aplikacji z wymogiem minimalizacji czasu przerwy w działaniu usług do max. 5 minut [nie wliczając czasu wykonywania skryptów aktualizacji systemu HIS].

Architektura HA dla serwera bazy danych

Serwer bazy danych systemu e-Usług musi zostać zabezpieczony na wypadek awarii zarówno serwera wirtualnego jak i fizycznego. Dlatego fizyczna instancja serwera PostgreSQL musi zostać uruchomiona w postaci co najmniej dwóch maszyn wirtualnych na dwóch różnych serwerach fizycznych archiwizujących dane w trybie on-line. Zamawiający nie stawia wymogu zastosowania konkretnej technologii czy konkretnego rozwiązania, wymaga jedynie spełnienie funkcjonalności w tym zakresie. Podstawowy serwer bazy danych musi zostać skonfigurowany w sposób maksymalizujący szybkość działania systemu bazodanowego [np.: podział dysków na grupy RAID, przeniesienie logów na oddzielne dyski, itp.].

Architektura Active Directory

W celu zapewnienia wysokiego poziomu bezpieczeństwa wszystkich usług i danych, należy wdrożyć usługę Active Directory – również w trybie HA, tj. min. 3 serwery wirtualne na min. 2 serwerach fizycznych, w tym przynajmniej jeden serwer musi znajdować się w zapasowej serwerowni – zgodnie z zaleceniami producenta oprogramowania. W ramach wdrożenia należy uruchomić integrację systemu HIS z usługą logowania do domeny. W ramach tego zadania Wykonawca utworzy wspólnie z ASI polityki dostępu do systemów i zaimplementuje je w GPO. Podłączenie komputerów do domeny jest obowiązkiem Zamawiającego, Wykonawca musi jednak świadczyć usługę asysty w przypadku problemów z podłączeniem do domeny.

Architektura RDP

W ramach projektu, w celu udostępnienia obsługi e-Usług personelowi szpitala niezależnie od lokalizacji, zostanie uruchomiona usługa zdalnego pulpitu [RDP]. Usługa ta musi zostać uruchomiona w trybie HA, tj. min. 4 serwerów wirtualnych na min. 2 serwerach fizycznych. Aby w pełni wykorzystać infrastrukturę, należy uruchomić serwery loadbalancingu pomiędzy tymi serwerami [również w trybie HA np. z DNS round-robin].

Architektura prywatnego CA

W ramach Projektu Wykonawca zobowiązany będzie do uruchomienia i skonfigurowania prywatnego CA na potrzeby obsługi EDM oraz wszystkich usług. CA w ramach EDM musi oferować pełną obsługę wszystkich zakresów wymaganych ustawami, rozporządzeniami i zarządzeniami. Dopuszczalna jest konfiguracja z wykorzystaniem pojedynczego podpisu kwalifikowalnego w celu podpisywania wszystkich wychodzących dokumentów elektronicznych. Architektura CA musi umożliwiać wydanie osobistego podpisu elektronicznego wszystkim pracownikom szpitala oraz unieważnienie go w przypadku zakończenia stosunku pracy z pracownikiem.

Usługi wspomagające

DNS

Należy uruchomić min. dwa serwery DNS działające w trybie HA i skonfigurować wszystkie niezbędne usługi – w tym round-robin dla load balancerów. Usługa DNS musi posiadać możliwość włączenia filtrowania kategorii stron internetowych, których adresy system DNS będzie zwracał.

NTP

Należy uruchomić min. dwa serwery NTP działające w trybie HA lub wzajemnej synchronizacji i skonfigurować wszystkie usługi i urządzenia do korzystania z tych serwerów.

DHCP

Należy uruchomić serwery DHCP przydzielające adresy jedynie urządzeniom ze statycznymi wpisami w bazie. Serwer DHCP musi działać również w trybie HA. Przełączniki sieciowe muszą zostać skonfigurowane w taki sposób aby niemożliwe było użycie nieautoryzowanych serwerów DHCP w sieci [DHCP snooping].

Aplikacja TESTOWA

W szczególności do celów podnoszenia kompetencji i samokształcenia personelu medycznego, należy uruchomić dodatkowe serwery Testowych instancji e-Usług [aplikacji i bazy danych] oraz zapewnienie możliwości łatwego aktualizowania danych z instancji głównej.

Zakres 3 – Modernizacja sieci LAN i WLAN

Rozbudowa sieci LAN

W ramach rozbudowy sieci LAN należy wykonać następujące elementy:

1. Modernizacja sieci miedzianej – cała infrastruktura w standardzie min. Cat 5e.:
	1. Ułożenie przewodów w korytach nad sufitami podwieszanymi – w miarę możliwości, w przeciwnym wypadku w korytach natynkowych,
	2. Ułożenie przewodów w korytach natynkowych lub podtynkowo – w miarę możliwości,
	3. Instalację lub wymianę szafek RACK w punktach dystrybucyjnych sieci [jeśli wymagana – tj. jeśli obecna szafka jest za mała [przewidywane min. to 9U] lub zbyt płytka aby zainstalować w niej wszystkie wymagane urządzenia], nowe szafki muszą być wyposażone w panele wentylacyjne z termostatem ustawionym na temp. o 15○C niższą od granicznej temperatury podanej przez producenta zainstalowanych wewnątrz szafki urządzeń – urządzenia z najniższą górną graniczną temp. pracy.
	4. Zakończenie przewodów w gniazdkach abonenckich, natynkowych lub podtynkowych – w miarę możliwości,
	5. Zakończenie przewodów złączami typu keystone jack w patch panelach w punktach dystrybucyjnych sieci,
	6. Trwałe i czytelne oznaczenie gniazd abonenckich [np. Za pomocą naklejek] zgodnie z opisem gniazd w punktach dystrybucyjnych,
2. Modernizacja sieci światłowodowej – JM:
	1. Wykonanie przyłączy światłowodowych pomiędzy budynkami B - G (poszczególne punkty dystrybucyjne w budynkach należy przyłączyć bezpośrednio do serwerowni głównej),
	2. Wykonanie łącza światłowodowego pomiędzy dwoma punktami dystrybucyjnymi w budynku A
	3. Zakończenie światłowodów w przełącznicach światłowodowych [złącza SC] po obu stronach przewodów,
	4. Trwałe i czytelne oznaczenie poszczególnych gniazd na przełącznicach umożliwiających szybką i jednoznaczną identyfikację odpowiedniego gniazda.
3. Wykonanie pomiarów sieci, min.: Wire Map, Lenght, Propagation delay, Delay Skew, Resistance, Insertion Loss, Return Loss, NVP, NEXT, PS NEXT, ACR, dla światłowodów należy wykonać analogiczne testy.
4. Instalacja w szafkach RACK punktów dystrybucyjnych: zasilaczy UPS, listew zasilających, przełączników sieciowych, łącznic światłowodowych, patchpaneli, organizerów kabli, półek, itp.
5. Konfiguracja przełączników sieciowych i UPSów w celu przekazywania komunikatów SNMP do systemu monitorującego – min.: temperatury i napięcia.
6. Konfiguracja przełączników sieciowych w celu prawidłowej organizacji logicznej sieci vLan.
7. Stworzenie i przekazanie dokumentacji powykonawczej, łącznie z wynikami pomiaru sieci.

W ramach modernizacji sieci należy dostarczyć Zamawiającemu patchcordy światłowodowe oraz miedziane [cat. min. 5e] w ilościach pozwalających na podłączenie wszystkich zainstalowanych w szafkach portów, oraz niezbędnych do podłączenia urządzeń sieciowych do każdego gniazda abonenckiego:

* patchcordy światłowodowe SC-SC [chyba że dostarczany sprzęt wymaga inaczej] - do PD o długości około 1m;
* patchcordy światłowodowe SC-SC [chyba że dostarczany sprzęt wymaga inaczej] - do serwerowni o długości około 2m i 3m;
* patchcordy miedziane do PD – o długości około 0,5m i 1m;
* patchcordy do podłączenia gniazd abonenckich – o długości około 2m i 3m.

Szczegóły miejsca instalacji poszczególnych punktów zawarte są w Załączniku nr 7 do SIWZ.

Wykonawca musi skonfigurować prawidłowe tabele routingu z użyciem odpowiednich poziomów dostępu wskazanych przez ASI [np. przy pomocy ACL] dla wszystkich sieci vLan.

Parametry minimalne szafek RACK

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Wysokość | 9U |
| Szerokość całkowita | 600 mm |
| Głębokość całkowita | 600 mm |
| Szerokość szyn montażowych | 19 cali |
| Ilość belek nośnych | Dwie belki nośne 19 cali z regulacją położenia |
| Otwory kablowe i wentylacyjne | otwory kablowe w postaci wyłamywanych zaślepek oraz po min. 3 otwory wentylacyjne w płycie górnej i dolnej |
| Obciążenie dopuszczalne | Min. 100 kg |
| Klasa ochrony | IP 20  |
| Dodatkowe cechy | Możliwość demontażu płyty górnej i dolnej, osłon bocznych oraz drzwi przy kompletnie wyposażonej szafce, przymocowanej do ściany.Wymagany bez narzędziowy montaż drzwi, osłon bocznych. Dwie osłony boczne, demontaż osłon bocznych możliwy po otwarciu drzwi przednich lub z własnym zamkiem. Osłona tylna z możliwością demontażu |

Budowa sieci WLAN

W ramach budowy sieci WLAN należy:

* zamontować punkty dostępowe [zgodnie z wytycznymi Zamawiającego uwzględniając strukturę budynków – maksymalizując zasięg sieci WiFi],
* wykonać fizyczne połączenie wszystkich punktów dostępowych z przełącznikami sieciowymi,
* wykonać logiczną instalację punktów dostępowych w kontrolerze/konsoli zarządzania,
* skonfigurować sieci dla odrębnych SSID, min. w zakresie:
	+ sieci otwartej, ogólnodostępnej z ograniczonym pasmem i ograniczonym zakresem usług [poczta e-mail, www] oraz z włączonymi filtrami stron www [zgodnie z wymaganiami Zamawiającego], użytkownicy tej sieci nie mogą mieć dostępu do żadnych zasobów lokalnych! I muszą być odizolowani od siebie nawzajem,
	+ sieci dostępnej dla personelu, zabezpieczonej z autentykacją na poziomie użytkownika active directory, sieć musi umożliwiać dostęp do systemu HIS oraz e-Usług, sieć musi zostać zabezpieczona w takim samym stopniu co sieć LAN,
	+ sieci administracyjnej – zabezpieczonej, ukrytej, dostępnej tylko dla ASI.
* skonfigurować (w ramach sieci otwartej) captive portal z regulaminem wymaganym do zaakceptowania przed uzyskaniem dostępu do sieci Internet.

Szczegóły miejsca instalacji poszczególnych punktów zawarte są w Załączniku nr 7 do SIWZ – Wykonawca zobowiązany jest dokonać analizy poprawności wytypowanych miejsc instalacji i w razie potrzeby zmodyfikować lokalizację zapewniając jak największe pokrycie terenu/budynku zasięgiem sieci WiFi.

Zakres 4 – Dostawa oprogramowania e-Usług

Wdrożenie portalu e-Usług.

Przez Portal należy rozumieć portal e-Usług Szpitala zawierający elementy statyczne jak i dynamiczne – tj. eUsługi.

Po aktualizacji Portal ma być zgodny z rekomendacjami wypracowanymi przez W3C i opisanymi na stronie <http://www.w3.org/WAI/guid-tech.html> w dokumencie WCAG 2.0. Portal będzie spełniał wymagania WCAG 2.0 na poziomie podstawowym.

Portal musi funkcjonować na następujących przeglądarkach internetowych: Firefox, Opera, Chrome, Edge.

Oprogramowanie, narzędzia i usługi wykonane lub użyte w trakcie tworzenia Portalu spełniać muszą wszystkie obowiązujące wymogi zawarte w prawie polskim oraz odpowiednich dyrektywach UE. Kodowanie znaków: UTF-8. Format strony www zgodny z HTML 4.01 lub XHTML 1.0.

Panel administratora powinien umożliwiać:

* zarządzanie użytkownikami (dodawanie, edytowanie, usuwanie, nadawanie uprawnień, ustalanie praw dostępu do poszczególnych podstron, blokowanie konta uniemożliwiające logowanie),
* automatyczne przesyłanie informacji o umieszczeniu nowego artykułu lub jego edycji do wybranego administratora,
* zarządzanie pozycjami w menu (dodawanie, usuwanie, ukrywanie, kopiowanie, edycja łącza, opcja „nie publikuj”/”ukryj”/ itp..),
* przeglądanie statystyk odwiedzin stron,
* prowadzenie biblioteki multimediów, do której można dodawać pliki w dowolnym formacie, które będą wykorzystywane na witrynie,
* przeglądanie dziennika bezpieczeństwa (automatyczny dziennik wszystkich logowań udanych i nieudanych wraz z czasem i numerem IP).

Portal zostanie umieszczony na serwerach Zamawiającego i musi być dostępny w sieci Internet najpóźniej w dniu zgłoszenia gotowości do odbioru końcowego**.**

Wykonawca dostarczy niezbędne licencje do prawidłowego funkcjonowania portalu jeśli takie są wymagane.

Wykonawca dołoży wszelkich starań, aby świadczone usługi były najwyższej jakości i bez zakłóceń oraz będzie podejmować działania zabezpieczające portal przed dostępem osób niepowołanych.

Wykonawca zobowiązany jest w okresie wdrożenia do wykonywania zmian i uzupełnień Portalu Zamawiającego, mających na celu rozwój oraz dostosowywanie do potrzeb Zamawiającego zgodnie z wymaganiami Zamawiającego w ramach obowiązujących przepisów prawa w terminach wzajemnie uzgodnionych.

Portal musi być w całości oparty na bazie danych - wszystkie treści zawarte w serwisie zapisane będą w bazie danych.

Wykonawca zobowiązany jest do nadto do:

a)przeprowadzenia z udziałem Zamawiającego testów Portalu,

b) przeprowadzania konsultacji w zakresie wprowadzania, edytowania i zarządzania treścią Portalu oraz przeszkolenie personelu w zakresie obsługi i wykorzystania funkcjonalności Portalu na warunkach określonych w SIWZ wraz z załącznikami, w szczególności w Szczegółowym Opisie Przedmiotu Zamówienia.

**1. Zmiany w grafice portalu**

Zostanie opracowana i wdrożona nowa, nowoczesna szata graficzna portalu, w celu:

* Nadania serwisowi profesjonalnego i nowoczesnego wyglądu, zgodnego z obecnymi standardami i trendami.
* Skrócenia czasu wczytywania strony.
* Zwiększenia czytelności strony i uproszczenia nawigacji po serwisie.

Nowa szata graficzna zostanie wdrożona zgodnie ze standardami konsorcjum W3C, co zapewni jej poprawne działanie na wszystkich platformach, w tym platformach mobilnych.

Nowa szata graficzna zostanie wdrożona w sposób, który wykorzysta możliwości nowoczesnych przeglądarek w celu zwiększenia User Expirience, jednocześnie zachowując kompatybilność ze starszymi przeglądarkami.

Wykonawca przedstawi propozycje grafiki do zatwierdzenia przez Zamawiającego – Zamawiający w ciągu max. 5 dni roboczych przekaże informację o zatwierdzeniu bądź odrzuceniu projektu.

**2. Wersja portalu do osób niedowidzących**

Oprócz nowej standardowej szaty graficznej zostanie przygotowana również jej uproszczona wersja o wysokim kontraście (np. czarne tło i żółta czcionka).

Kolorystyka oraz typografia w trybie dla osób słabowidzących będzie czytelna dla takich użytkowników.

Funkcjonalność portalu w tym trybie zostanie odpowiednio okrojona, tak, aby użytkownik mógł w pełni skupić się na treści.

Przejście ze standardowego trybu do trybu dla osób słabowidzących będzie odbywać się poprzez kliknięcie jednego, wyraźnego odnośnika.

Zgodność z wymaganiami standardu WCAG 2.0

**3. Zarządzanie treścią**

1. aktualizacja serwisu informacyjnego przez użytkowników bez umiejętności tworzenia stron WWW i znajomości wymaganych do tego standardów (HTML, XHTML, DHTML, CSS, itp.),

2. oddzielenie warstwy treści od warstwy wyglądu (prezentacji),

3. utrzymanie jednolitego wyglądu i struktury na podstronach,

4. funkcje CMS (systemu zarządzania treścią),

5. umożliwienie współdziałania wielu osób przy publikacji,

6. umożliwienie tworzenia otwartych publikacji, w których każdy czytelnik może wyrazić swoją opinię (fora wewnętrzne dla zarejestrowanych użytkowników/pacjentów i lekarzy),

7. dodatkowe funkcje, jak wyszukiwanie, ułatwienia w linkowaniu stron, automatyczne datowanie, formatowanie obrazków etc.

8. narzędzia wspomagające autorów i użytkowników w zarządzaniu treścią. Najważniejsze cechy systemu zarządzania zawartością:

• elastyczność systemu, łatwość rozbudowy i zmian w systemie,

• możliwość wykorzystania gotowych szablonów do przygotowania poszczególnych stron i dokumentów - wyeliminowanie konieczności powtarzania standardowych fragmentów kodu HTML oraz standardowych elementów serwisu,

• możliwość definiowania standardowej struktury i elementów strony WWW,

• możliwość zdefiniowania uprawnień osób oraz dla poszczególnych grup autorów, redaktorów, administratorów strony – możliwość rozdzielenia prac nad systemem na zespoły odpowiedzialne za poszczególne elementy: treść, grafikę, wyświetlanie, operacje na bazie danych,

Dostawa systemu e-Usług

1. Rozbudowa obecnej usługi E-rejestracji do poradni

Poziom: 5

Grupa docelowa: Pacjenci,

Przebieg usługi:

- pacjent po otrzymaniu skierowania od lekarza wypełnia formularz na stronie WWW szpitala służący do inicjacji procesu rejestracji do poradni – w formularzu podaje dane: datę skierowania, rodzaj skierowania, informację o pilności zabiegu i jaką formę kontaktu zwrotnego wybiera SMS lub e-mail,

- następuje rejestracja pacjenta do kolejki oczekujących, o czym pacjent zostaje powiadomiony używając wybranego przez pacjenta medium,

- pacjent w terminie 14 dni od inicjacji usługi dostarcza oryginał skierowania do rejestracji Poradni – jeśli nie, następuje skreślenie z listy oczekujących z powiadomieniem o tym fakcie pacjenta używając wybranego przez pacjenta medium; w obydwu przypadkach następuje zakończenie usługi.

2. Wstępna e-kwalifikacja pacjentów do 8 tygodniowego programu terapii uzależnień

Wstępna kwalifikacja osób chcących podjąć terapię uzależnień. Przejście usługi z wynikiem pozytywnym nie oznacza, że pacjent zostanie do programu przyjęty, gdyż po przybyciu zaproszonego pacjenta, w szpitalu odbywa się dodatkowa weryfikacja przez terapeutę i lekarza.

Poziom 5

Grupa docelowa: osoby chcące podjąć terapię uzależnień,

Przebieg usługi:

• - pacjent zgłasza chęć podjęcia terapii i kwalifikacji (w postaci rozmowy on-line przy użyciu komunikatora video) wypełniając formularz na stronie WWW, w którym jako formę kontaktu zwrotnego wybiera SMS lub e-mail,

• - terapeuta używając wybranego przez pacjenta medium wysyła możliwy termin przeprowadzenia wstępnej rozmowy kwalifikacyjnej oraz sposób jej przeprowadzenia (komunikator video),

• - pacjent używając wybranego wcześniej przez siebie medium potwierdza termin bądź wnosi o jego zmianę, co ponawia poprzedni krok,

• - po potwierdzeniu terminu przez pacjenta w wybranym czasie następuje przeprowadzenie wstępnej kwalifikacji on-line,

• - po przeprowadzeniu rozmowy on-line może pojawić się konieczność umówienia rozmowy uszczegóławiającej, co następuje tak samo, jak przy umawianiu wstępnej kwalifikacji on-line,

• - jeśli pacjent nie zostanie zakwalifikowany, przy użyciu wybranego przez pacjenta medium, pacjent dostaje powiadomienie o tym fakcie, a także informację, jakie warunki powinny być spełnione w celu kwalifikacji i następuje koniec usługi,

• - jeśli pacjent zostanie wstępnie zakwalifikowany, terapeuta używając wybranego przez pacjenta medium powiadamia go o tym fakcie, przekazując również informację o wpisaniu go do kolejki oczekujących, jak również informację o możliwości skorzystania z usługi „E-porada on-line”,

• - 2 tygodnie przed terminem przyjęcia przy użyciu wybranego przez pacjenta medium pacjent dostaje zaproszenie z informacją o wykazie przedmiotów i dokumentów wymaganych przy przyjęciu, jak również o konieczności potwierdzenia uczestnictwa w programie, po czym następuje zakończenie usługi,

• - w całym toku usługi pacjent ma możliwość rezygnacji z uczestnictwa w programie przy użyciu wybranego przez siebie wcześniej medium.

3. E-recepta

Bezpośrednia lub pośrednia transmisja recepty, wraz z informacjami ściśle z nią powiązanymi, pomiędzy lekarzem, farmaceutą, instytucją refundacyjną oraz władzami zdrowotnymi, przy użyciu mediów elektronicznych

Grupa docelowa: osoby będące w terapii uzależnień,

Przebieg usługi:

• podczas wizyty u lekarza dla pacjenta wypisywana jest e-recepta w systemie informatycznym – tj. tworzony jest elektroniczny zapis informacji na temat leku przepisanego pacjentowi, który obejmuje również sposób dawkowania tego leku,

• przygotowany dokument podpisywany jest przy pomocy podpisu kwalifikowanego oraz przesyłany za pośrednictwem Platformy P1 do farmaceuty,

• pacjent otrzymuje smsa, ze specjalnym kodem, który w połączeniu z dokumentem tożsamości, umożliwi realizację recepty w aptece,

• pacjent, który nie będzie posiadał telefonu lub nie będzie chciał skorzystać z funkcjonalności systemu, otrzyma wydrukowany kod, który przedstawi w wybranej przez siebie aptece,

• pacjent zgłasza się do dowolnie wybranej apteki po odbiór leków,

• informacja o refundacji leku oraz jej wielkości jest przesyłana do instytucji refundacyjnej,

• po dokonaniu refundacji następuje sfinalizowanie usługi.

4. E-zlecenie

Rozwiązanie to usprawni obieg informacji między lekarzem, pacjentem a instytucją refundacyjną. Dzięki funkcji e-Zlecenie na wyroby medyczne (np. na pieluchy dla osoby dorosłej) nie będzie potrzebna wizyta pacjenta w oddziale funduszu w celu potwierdzenia uprawnień. E-zlecenia będą wysyłane przez lekarza elektronicznie do NFZ, który dokona jego weryfikacji, a następnie prześle pacjentowi informację, np. SMS-em, o możliwości zrealizowania zlecenia.

Grupa docelowa: osoby będące w terapii uzależnień,

Przebieg usługi:

• podczas wizyty u lekarza dla pacjenta lub opiekuna wypisywane jest e-zlecenie w systemie informatycznym – tj. tworzony jest elektroniczny zapis informacji na temat danego wyrobu

• przygotowany dokument podpisywany jest przy pomocy podpisu kwalifikowanego oraz przesyłany za pośrednictwem Platformy P1 do instytucji refundacyjnej,

• instytucja refundacyjna dokonuje weryfikacji e-zlecenia oraz potwierdza posiadanie uprawnienia refundacyjnego zakupu wyrobu w postaci przesłania sms potwierdzenia możliwości zrealizowania zakupu wyrobu,

• pacjent otrzymuje smsa, ze specjalnym kodem, który w połączeniu z dokumentem tożsamości, umożliwi realizację wyrobu w aptece,

• pacjent zgłasza się do dowolnie wybranej apteki po odbiór wyrobu,

• informacja o realizacji zlecenia jest przesyłana do instytucji refundacyjnej,

• po dokonaniu refundacji następuje sfinalizowanie usługi,

• w przypadku odmowy potwierdzenia przez instytucję refundacyjną stosownych uprawnień usługa zostaje zakończona na tym etapie.

5. E-skierowanie

Rozwiązanie to usprawni obieg informacji między lekarzem, pacjentem a instytucją refundacyjną. Dzięki funkcji e-skierowanie niemożliwe będzie zapisanie się pacjenta do danego specjalisty w kilku różnych poradniach, a tym samym - zmniejszy kolejki. Pacjent nie będzie musiał dostarczać do przychodni oryginału papierowego skierowania; na wizytę będzie mógł się umówić telefonicznie przez podanie kodu dostępu oraz numeru dokumentu potwierdzającego tożsamość – zakres funkcjonalności usługi – e-rejestracja.

Grupa docelowa: osoby będące w terapii uzależnień,

Przebieg usługi:

• podczas wizyty u lekarza rodzinnego pacjent otrzymuje e-skierowanie w systemie informatycznym – tj. tworzony jest elektroniczny zapis informacji odnośnie wstępnego rozpoznania oraz skierowania do poradni specjalistycznej – lekarza specjalisty,

• przygotowany dokument podpisywany jest przy pomocy podpisu kwalifikowanego oraz przesyłany za pośrednictwem Platformy P1 do poradni specjalistycznej,

• pacjent otrzymuje smsa, ze specjalnym kodem, który w połączeniu z dokumentem tożsamości, umożliwi realizację rejestrację w poradni specjalistycznej,

• pacjent dokonuje rejestracji przy użyciu funkcjonalności usługi – e-rejestracja

• informacja o zrealizowaniu odbytej wizycie pacjenta jest przesyłana do instytucji refundacyjnej,

• pacjent, który nie będzie posiadał telefonu lub nie będzie chciał skorzystać z funkcjonalności systemu, otrzyma wydrukowany kod, który przedstawi we wskazanej przez lekarza poradni specjalistycznej.

6. Pakiet wiadomości SMS

W ramach wdrożenia e-Usług należy dostarczyć i skonfigurować pakiet wiadomości SMS do wykorzystania przez e-Usługi zainstalowane w Szpitalu. Pakiet musi współpracować z Systemem e-Usług bez dodatkowych modułów sprzętowych czy programowych lub należy bezpłatnie te moduły/urządzenia dostarczyć. Pakiet wiadomości SMS musi pozwalać na wysłanie min. 60 000 SMSów w ciągu min. 60 miesięcy od dnia uruchomienia e-Usług.

Zakres 5 – Konfiguracja i uruchomienie e-Usług

Wdrożenie portalu e-Usług.

Obowiązkiem Wykonawcy będzie przeniesienie treści obecnego serwisu Zamawiającego do tworzonego Portalu z zachowaniem jego dotychczasowej konstrukcji – strona ta ma być ogólnodostępna w archiwum nowej strony, bez możliwości jej modyfikacji. W ramach wdrożenia wymagane jest przeszkolenie 3 osób z wprowadzania danych do portalu/edytowania treści.

Integracja portalu e-Usług z HIS

W ramach integracji należy skonfigurować portal e-Usług do uruchomienia i współpracy z wdrażanymi w Projekcie e-Usługami. Prace należy wykonać zgodnie z zaleceniami producenta systemu HIS i producenta e-Usług.

Uwierzytelnianie dostępu do e-Usług

Dostarczony w ramach projektu System musi realizować dostęp za pomocą tych metod uwierzytelniana:

* + 1. Podpisu elektronicznego kwalifikowalnego – pacjenci przy komunikacji i składaniu wniosków elektronicznie, pracownicy - przekazywanie dokumentacji na zewnątrz oraz wydawanie dokumentacji w wersji elektronicznej. Wszelka dokumentacja przekazywana przez placówkę na zewnątrz musi być w wersji elektronicznej oznaczona kwalifikowanym podpisem elektronicznym. Dlatego wymaga się aby zarówno dyrekcja jak osoby kluczowe w danych jednostkach posiadały taki podpis. Osoba upoważniona/Ordynator w przypadku sporządzenia kopii dokumentacji pacjenta nawet w przypadku gdy lekarz prowadzący już nie pracuje w jednostce podpisuje i autoryzuje wystawiany dokument.
		2. Podpisu elektronicznego niekwalifikowanego – pracownicy podpisywanie dokumentacji wewnętrznej w ramach realizacji usługi **Elektroniczna Dokumentacja Medyczna z usługą e-Podpis.**
		System musi być przystosowany do stosowania podpisu cyfrowego i obsługi własnego centrum podpisu elektronicznego (niekwalifikowanego) (Wykonawca dostarczy i wdroży dla Zamawiającego centrum podpisu elektronicznego - niekwalifikowanego):
* uwierzytelnienie w Systemie z wykorzystaniem karty kryptograficznej wszystkich użytkowników którym zostały przydzielone takie uprawnienia,
* wskazanie osób mających prawa do podpisania danych typów dokumentów oraz wybrania z tej listy konkretnych osób podpisujących dany dokument,
* podpisywanie dokumentów tworzonych w Systemie podpisem cyfrowym z wykorzystaniem karty inteligentnej przez wszystkich użytkowników którym zostały przydzielone takie uprawnienia
	+ 1. Stosowanie profilu zaufanego ePUAP – dla pacjentów oraz personelu zgodnie z wymogami stawianymi przez platformę P1 oraz P2 oraz takich urzędów jak ZUS czy NFZ konieczne jest stosowanie podpisów za pomocą ePUAP-u.

|  |  |
| --- | --- |
| Lp. | **Minimalne wymagania - Podpis elektroniczny** |
|  | Wykonawca dostarczy centrum podpisu elektronicznego niekwalifikowanego i zainstaluje go na przeznaczonym do tego serwerze (centrum certyfikacji podpisu elektronicznego - niekwalifikowanego) |
|  | Konfiguracja uprawnień użytkowników mających otrzymać prawa posługiwania się certyfikatami. |
|  | Zarządzanie użytkownikami sytemu, w tym możliwość:* przydzielania im certyfikatów,
* nadawania uprawnień,
* manualnego nadawania haseł,
* automatycznego nadawania haseł,
* nadawania haseł tymczasowych.
 |
|  | Kompletna dokumentacja dla użytkownika zawierająca szczegółowe opisy wraz z ilustracjami poglądowymi procesu logowania i zarządzania hasłami.  |
|  | Kompletna dokumentacja dla administratora zawierająca przykładową konfigurację urzędów certyfikacji wraz z ilustracjami poglądowymi (ustawienia, import / eksport certyfikatów i list odwołań), ustawienia serwera LDAP oraz stacji roboczych. |
|  | Podpisywanie dokumentów XML. |
|  | Wykorzystanie certyfikatów kwalifikowanych i/lub niekwalifikowanych do składania podpisu elektronicznego. |
|  | Umożliwienie składania podpisu elektronicznego z wykorzystaniem kart chipowych |
|  | Możliwość złożenia wielu podpisów elektronicznych przy jednokrotnym podaniu numeru PIN do karty inteligentnej |
|  | Weryfikacja podpisu elektronicznego |
|  | Możliwość konfiguracji żądań podpisów dla każdego z dokumentów dostępnych w systemie:* definiowanie osoby lub funkcji pracownika podpisującego,
* definiowanie celu złożenia podpisu,
* definiowanie oczekiwanego miejsce złożenia podpisu,
* określenie terminu złożenia podpisu względem daty tworzenia dokumentu,
* określenie miejsca zasobu dyskowego, na którym będą składowane pliki.
 |
|  | Możliwość określenia osób mających prawa do podpisania danych typów dokumentów oraz wybrania z tej listy konkretnych osób podpisujących dany dokument. |
|  | Opisywanie dokumentów przez zbiór metadanych, zawierających m.in. dane pacjenta, dane osoby tworzącej dokument, jednostkę/komórkę organizacyjną, rodzaj dokumentu, datę utworzenia, datę podpisania, datę udostępnienia. |
|  | Możliwość przechowywania kolejnych wersji tych samych dokumentów. |
|  | Utrwalanie i zabezpieczanie dokumentów w Archiwum Dokumentów Elektronicznych  |
|  | Wczytywanie zewnętrznych dokumentów, umożliwienie złożenia podpisu elektronicznego pod nimi oraz przekazywanie ich do Archiwum Dokumentów Elektronicznych  |

Uruchomienie e-Usług

Wszystkie zainstalowane e-Usługi muszą zostać skonfigurowane zgodnie z ich przeznaczeniem i opisanym zakresem funkcjonalnym. W ramach uruchomienia e-Usług Wykonawca przeprowadzi szkolenia opisane w Zakresie 6 niniejszego OPZ.

Moduł integracji z P1, P2 [z EDM]

System musi pracować zgodnie z ogłoszonym i opublikowanym modelem wymiany danych przez CSIOZ. Musi zawierać opis komunikatów wymiany danych i zakres funkcjonalności zgodny z przyjętym modelem w platformie P1.

System w pełni musi spełniać Model Transportowy danych o Zdarzeniach Medycznych oraz Indeksie Elektronicznej Dokumentacji Medycznej gromadzonych w systemie P1. Musi zawierać również specyfikację zapytań o dane zdarzeń medycznych i indeksu tych danych.

System musi być zgodny z opisem hierarchii węzłów ISO OID, wykorzystywanej w komunikacji w ramach Platformy P1.

System musi pracować w oparciu o opublikowane rejestry udostępnione w ramach projektu P2. Dzięki zastosowaniu WEB Serwisów system będzie miał dostęp do wszelkich aktualizacji opublikowanych w ramach platformy P2. Dostęp do zakładanych rejestrów to:

* Rejestr Podmiotów Wykonujących Działalność Leczniczą – spowoduje brak konieczności prowadzania danych
* Rejestr Aptek – umożliwi poinformowanie pracownika o najbliższych dla niego działających placówkach
* Rejestr Hurtowni Farmaceutycznych – ułatwi pracę personelowi z działu zamówień publicznych.
* Rejestr Produktów Leczniczych – da możliwość aktualizacji wiedzy swojemu personelowi medycznemu w zakresie dostępnych obecnie produktów medycznych
* Rejestr Produktów Leczniczych – umożliwi weryfikacje czy badanie zostało wykonane zgodnie z obowiązującymi przepisami czy przez osobę uprawnioną
* Rejestr Systemów Kodowania – umożliwi dostęp personelowi do zbioru słowników medycznych. Ma eliminować nieporozumienia wynikające ze stosowania terminów medycznych przy wymianie informacji oraz postawionej diagnozie.

Aby wypełnić wszelkie interakcje danych w systemie HIS wymaganych do współpracy z platformami P1 oraz P2, w ramach modernizacji systemu poprawione zostaną funkcjonalności w następujących modułach:

* Generator formularzy,
* Archiwum dokumentacji (uruchomienie EDM i zapewnienie standardu HL7 CDA),
* Zlecenia medyczne (zapewnienie standardu HL7 CDA),
* Zakażania,
* Dokumentacja medyczna w Szpitalu (uruchomienie EDM i zapewnienie standardu HL7 CDA),
* Weryfikacja uprawnień pacjenta do usług,
* Poradnia, (Zmiana terminu wizyty i wizyty pierwszorazowe)
* Rozliczenia NFZ,
* Raporty JGP, kontrola JGP,
* Apteka Centralna,
* Apteczki Oddziałowe,
* Zlecenia Leków.

Funkcjonalność i obecny stan wdrożenia wyżej wymienionych modułów wymagały będą przeprowadzenia analizy/audytu przez Wykonawcę na środowisku Zamawiającego i wdrożenia lub rekonfiguracji systemu w taki sposób aby spełniały one wymagania Zamawiającego [zgodnie z przepisami prawa i wewnętrzną dokumentacją szpitala].

Inne integracje Systemu

W ramach integracji systemów, w celu realizacji pełnego zakresu e-Usług, należy wykonać integrację z systemem finansowo-księgowym w zakresie transferu danych rozliczeniowych za wykonane badania [np. rozchody leków z magazynów aptecznych, faktury wystawione do NFZ, koszty badań i konsultacji z oddziałów, itp.]. Dodatkowo, w celu zwiększenia bezpieczeństwa oraz zapewnienia rozliczalności danych przekazywanych do e-Usług, należy dokonać integracji systemu HIS z Active Directory.

Zakres 6 – Szkolenia

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu używania Systemu na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia.

Szkolenia z użytkowania i administracji Systemu usług eZdrowia dla użytkowników (min. 90 osób) oraz administratorów systemu (min. 3 osoby).

Szkolenia z obsługi systemu przez poszczególne grupy personelu w tym:

1. Lekarze: wystawianie e-dokumentów (e-recepty, e-zlecenia, e-skierowania), podpisywanie podpisem kwalifikowanym, zasady gromadzenia i przetwarzania dokumentacji w standardzie HL7 CDA.

2. Personel pomocniczy lekarzy: e-rejestracja, wstępna e-kwalifikacja pacjentów do 8 tygodniowego programu terapii uzależnień – rejestrowanie na wizyty oraz kwalifikacja pacjentów na terapię oraz funkcjonalności systemu.

3. Ogólne aspekty szkolenia dla personelu: bezpieczeństwo danych osobowych oraz użytkowania oprogramowania komputerów pod kątem ochrony danych osobowych, różnice między dokumentacją w formie papierowej i elektronicznej, jej zastosowanie i ograniczenia.

Szkolenia są niezbędne w celu zagwarantowania osiągnięcia zakładanych efektów w projekcie.

Szczegółowy zakres poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiający w ramach akceptacji harmonogramu i materiałów szkoleniowych.

Wykonawca na etapie uzgadniania materiałów szkoleniowych przekaże minimalne wymagania, jakie powinni spełniać oddelegowani przez Zamawiającego, uczestnicy szkolenia.

Do każdego modułu wspomagającego obsługę obszarów działalności szpitala, Zamawiający wskaże osoby, które Wykonawca przeszkoli.

Szkolenia będą realizowane w pomieszczeniach i na sprzęcie udostępnionym przez Zamawiającego.

Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych – dopuszcza prowadzenie szkoleń e-learningowych jedynie w ramach szkoleń uzupełniających.

Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 20 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych.

Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiającego w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.

Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu. Szkolenie musi obejmować co najmniej instalację, konfigurację, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.

Uzgodnieniu pomiędzy stornami podlegają:

* Minimalne wymagania dla uczestników szkoleń,
* Harmonogram szkoleń grupowych i indywidualnych,
* Materiały szkoleniowe dla szkoleń grupowych,
* Listy obecności ze szkoleń grupowych i indywidualnych,
* Protokoły odbioru zadania dot. szkoleń.

Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać pracownikom na rozpoczęcie pracy w systemie.

Zakres 7 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

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

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca 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.

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.

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

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył instrukcję dostępu do systemów i sieci Internet [LAN oraz WLAN] zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Dokumentacja musi być sporządzona w języku polskim.

Zakres 8 – Gwarancja i wsparcie

Świadczenie usługi gwarancji i wsparcia ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp. Zakres i warunki opisane w Załączniku nr 6 do Umowy.

Wykonawca zobowiązuje się do dostarczania wolnych od wad kolejnych wersji Systemu.

Wykonawca zobowiązuje się do aktualizacji dokumentacji Użytkownika i/lub Administratora.

Wykonawca zobowiązuję się do świadczenia konsultacji dla Administratorów w zakresie niezbędnych zmian w konfiguracji systemu.

Wykonawca zapewni usługę wsparcia użytkowników udostępniając:

* + usługę typu helpdesk, udostępnioną pod adresem e-mail, numerem telefonu
	+ portal typu helpdesk – dostępny on-line w trybie 356/7/24, gdzie będą publikowane m.in. statusy zgłoszeń oraz ich treść i historia korespondencji
	+ przez niniejszy portal będą mogły być dokonywane zgłoszenia Dysfunkcji

Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy systemu zgodnego z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Administratorów związane z bieżącą eksploatacją Systemu.

Wykonawca zapewni w godzinach pracy Zamawiającego w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów.

Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.

Wykonawca będzie świadczył na rzecz Zamawiającego usługi serwisu w zakresie przedmiotu zamówienia (umowy) w okresie 60 miesięcy (licząc od daty podpisania protokołu odbioru końcowego lub od daty zakończenia trwającego obecnie okresu gwarancji – w zależności co nastąpi później) zapewniając jednocześnie odpowiednie wsparcie merytoryczne.

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

* + z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: Dysfunkcji w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
	+ związanych z realizacją usługi wdrożenia Systemu;
	+ spowodowanych aktualizacjami Systemu.

Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów.

Zgłaszający, w przypadku wystąpienia dysfunkcji przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia Dysfunkcji. W Zgłoszeniu powinny być wypełnione wszystkie obligatoryjne pola formularza, a opis sytuacji prowadzącej do wystąpienia błędu lub awarii powinien umożliwiać jej odtworzenie przez zespół serwisowy Wykonawcy. Jeżeli odtworzenie błędu nie będzie możliwe w środowisku Wykonawcy, wówczas zdiagnozuje on błąd w środowisku Zamawiającego, a terminy usunięcia Dysfunkcji ulegają wydłużeniu o czas oczekiwania na dostęp do środowiska Zamawiającego.

Wykonawca zobowiązany jest do potwierdzenia w ciągu 4 godzin w czasie okna dostępności usługi serwisowej przyjęcie Zgłoszenia reklamacyjnego oraz jego klasyfikację. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.

Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie.

Zgłoszenia będą klasyfikowane zgodne ze słownikiem pojęć, zawartym w Załączniku nr 6 do Umowy, przez Zamawiającego w uzgodnieniu z Wykonawcą.

Wykonawca zobowiązany jest do usunięcia dysfunkcji w terminach wymienionych w pkt 7 procedury podejmowania prac serwisowych zawartej w Załączniku nr 6 do Umowy.

W każdym przypadku Zgłaszający i Wykonawca mogą uzgodnić inny czas dostarczenia rozwiązania niż określono w warunkach gwarancji. W takim przypadku niezbędne jest potwierdzenie ustalonego terminu w formie pisemnej, faksem lub e-mailem.

Terminy wymienione w Załączniku nr 6 do Umowy obowiązują również w przypadku dostarczonego sprzętu.

1. Od dnia podpisania Umowy [↑](#footnote-ref-2)
2. Od dnia zakończenia Zakresu poprzedzającego [↑](#footnote-ref-3)
3. Na całość rozwiązania od momentu podpisania ostatniego Protokołu Odbioru Końcowego Zakresów od 1 do 7. [↑](#footnote-ref-4)
4. Parametr ważny z uwagi na docelowe wykorzystanie serwera [↑](#footnote-ref-5)