Opis Przedmiotu Zamówienia

Załącznik nr 2 A

Spis treści

1 SPRZĘT I OPROGRAMOWANIE ... 3

1.1 Wymagania ogólne: ... 3
1.2 Serwer wirtualizacji (4 szt.) ... 4
1.3 Serwer bazodanowy (2 szt.) ... 6
1.4 Serwerowy System Operacyjny (1 sztuka – 16 core) ... 7
1.5 Konfiguracja i wdrożenie ... 9
1.5.1 Szafy, serwery, okablowanie ... 9
1.5.2 Wirtualizacja oraz Storage ... 9
1.5.3 Migracja istniejącego środowiska ... 14
1.6 Sieć ... 15
1.6.1 Przełącznik szkieletowy (2 szt.) ... 15
1.6.2 Przełącznik dostępowy TYP1 (2 szt.) ... 18
1.6.3 Przełącznik dostępowy TYP2 (4 szt.) ... 19
1.6.4 Urządzenie dostępowe sieci bezprzewodowej 802.11a/b/g/n/ac/ax (30 szt.) ... 20
1.6.5 Oprogramowanie do zarządzania infrastrukturą (1kpl.) ... 23
1.6.6 Firewall/UTM TYP1 (1kpl.) ... 27
1.6.7 Firewall/UTM TYP2 (4szt.) ... 32
1.6.8 Konfiguracja i wdrożenie ... 33
1.7 System Informacji Wewnętrznej ... 34
1.7.1 Oprogramowanie do zarządzania treścią (1kpl.) ... 35
1.7.2 Monitor w obudowie odpornej na uszkodzenia (2kpl.) ... 39
1.7.3 Instalacja i uruchomienie ... 39
1.8 System Backup ... 40
1.8.1 Oprogramowanie Backup (1kpl.) ... 40
1.8.2 Macierz do składowania kopii zapasowych (2szt.) ... 41
1.8.3 Instalacja i uruchomienie ... 42
1.9 Oprogramowanie do zarządzania zgłoszeniami (1 kpl.) ... 42
1.10 Zestaw komputerowy typu All-in-One z oprogramowaniem biurowym (90 kpl.) ... 48
1.11 Komputer przenośny z oprogramowaniem biurowym (15 kpl.) ... 56
1.12 System telefonii VoIP ... 63
1.12.1 Telefon stacjonarny SIP VoIP (100 szt.) ... 63
1.12.2 Centrala telefoniczna VoIP z funkcją Wideokonferencji (1 szt.) ... 64
1.12.3 Instalacja i uruchomienie ... 70
1.13 Urządzenie wielofunkcyjne laserowe mono (4 szt.) ... 70
1.14 Urządzenie wielofunkcyjne laserowe kolor (3 szt.) ... 71
1.15 Drukarka laserowa monochromatyczna (30 szt.) ... 71
1.16 Projektor Full-HD wraz z ekranem projekcyjnym (4 kpl.) ... 72
1.17 Zasilacz Awaryjny UPS do serwerowni (4 kpl.) ... 72

2 OPROGRAMOWANIE BAZODANOWE NA POTRZEBY HIS (2 LIC.) ... 73

3 WYKONYWANIE KOPII BEZPIECZEŃSTWA DANYCH W CHMURZE KRYPTOGRAFICZNEJ ... 75

3.1 Analiza architektury i opis rozwiązania, obejmuje: ... 75
3.2 Zasady świadczenia wsparcia oraz opieki serwisowej oprogramowania. ... 77
3.3 Dokumentacja. ... 77
3.4 Szkolenia ... 78

4 SYSTEM AUTOMATYCZNEJ DIGITALIZACJI DOKUMENTÓW NA POTRZEBY DOKUMENTACJI MEDYCZNEJ PROWADZONEJ W FORMIE ELEKTRONICZNEJ ZGODNIE Z NORMĄ PN-EN ISO 10781 (10 STANOWISK) ... 78

4.1 Ogólne warunki ... 78
4.2 Szczegółowy opis systemu ... 79
4.2.1 Licencje ... 79
4.2.2 Wdrożenie ... 79
4.3 Wymagania dotyczące serwisu i nadzoru autorskiego ... 80

4.4 Wymagania dotyczące sprzętu 81
4.5 Wymagania dotyczące gwarancji 81
4.6 Wymagania Niefunkcjonalne Systemu 82
4.7 Wymagania Funkcjonalne Systemu 83
5 SYSTEM REJESTRACJI CZASU PRACY (3 PUNKTY) 84

1 Sprzęt i oprogramowanie

1.1 Wymagania ogólne:

a) Gdziekolwiek w opisie przedmiotu zamówienia przywołane są normy lub nazwy własne lub znaki towarowe lub patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę Zamawiający dopuszcza rozwiązania równoważne.
b) Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2008 lub normą równoważną.
c) W momencie oferowana wszystkie elementy oferowanej architektury muszą być dostępne (dostarczane) przez producenta.
d) Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
e) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
f) Do każdego dostarczonego wraz z serwerem systemu operacyjnego muszą być załączone oryginalne dokumenty licencyjne uprawniające do używania systemu operacyjnego określonego dla każdego z serwerów
g) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.
h) Wszystkie serwery muszą posiadać Certyfikat CE produktu albo spełniać normy równoważne.
i) Oferowane serwery muszą być przygotowane do współpracy z systemami operacyjnymi takimi jak: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2019, LINUX Red Hat, Vmware, Microsoft Windows Server 2016, HyperV
j) Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10% , 50 Hz.
k) Sprzęt powinien być objęty gwarancją producenta sprzętu przez okres zgodny z wymaganiami zamieszczonymi w poniższych rozdziałach.
l) Wszystkie poniższe parametry należy traktować jako minimalne.
m) Wszelkie użyte nazwy własne producentów należy traktować informacyjnie i dopuszczona jest możliwość zastosowania technologii w inny sposób zapewniających poniższe funkcjonalności.
n) Wykonawca zobowiązany jest do dostarczenia przedmiotu zamówienia własnym transportem (lub transportem zorganizowanym we własnym zakresie i na własny koszt), rozładowania i wniesienia do wskazanego przez Zamawiającego miejsca, na własny koszt i ryzyko.
o) Wykonawca odpowiada za działania i zaniechania osób skierowanych do realizacji zadania jak za własne działania i zaniechania.
p) Harmonogram dostaw, instalacji, konfiguracji i wdrożeń zostanie szczegółowo ustalony z Zamawiającym. Wstępny harmonogram stanowi załącznik do projektu umowy.
q) W celu weryfikacji przed wyborem najkorzystniejszej oferty Zamawiający wezwie Wykonawcę do złożenia pełnej dokumentacji technicznej (w tym part numbery) dostarczanych rozwiązań sprzętowych i programowych. Dostarczona dokumentacja posłuży jako załącznik przy protokole odbioru dostawy i wdrożenia weryfikujący poprawność dostawy.
r) Wszystkie elementy dostawy muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie możliwość weryfikacji źródła pochodzenia elementów dostawy przed odbiorem i w razie braku potwierdzenia legalności źródła Zamawiający odmówi odbioru.

1.2 Serwer wirtualizacji (4 szt.)

Zaprojektowano użycie czterech serwerów jako serwerów produkcyjnych (aplikacyjny i bazodanowy), które z wykorzystaniem wirtualizatora będą uruchamiały maszyny wirtualne potrzebne do obsługi informatycznej Spółki. Serwery te będą pracowały z wykorzystaniem funkcji klastra.

Każdy z serwerów powinien mieć następującą konfigurację:

- Obudowa o wysokości maksymalnie 2U z zestawem umożliwiającym montaż w szafie rack 19”
- Dwa procesory min. 8 rdzeniowe
- Pamięć RAM min. 512GB typu Registered
- Płyta główna dedykowana do pracy w serwerach
- Karta sieciowa z 2 portami 25G zakończone złączem SFP28
- Dedykowane dyski do instalacji wirtualizatora
- Karta graficzna zintegrowana na płycie głównej
- Dwa zasilacze redundantne, typu Hot-Plug
- Wentylatory redundantne, typu Hot-Plug

Montaż i instalacja urządzeń w szafie serwerowej w miejscu wskazanym przez Zamawiającego.

Serwery należy podłączyć do Zasilaczy Awaryjnych UPS zgodnie z opisem. Ponadto serwery należy podłączyć do dostarczonych przełączników sieciowych.

Na serwerach należy skonfigurować środowisko wirtualne.

Cecha	Wymagania minimalne
Obudowa	Obudowa o wysokości maksymalnie 2U. Obudowa musi być przystosowana do montażu w standardowej szafie Rack 19” i zawierać komplet kabli połączeniowych niezbędnych do instalacji. Obudowa umożliwiająca instalację minimum 24 dysków Hot Plug 2.5” - w pełni wspierająca skonfigurowanie co najmniej 24 dysków dla jednostki przetwarzania. Obudowa umożliwiająca instalację minimum 12 dysków NVMe 2.5”. Zainstalowane min. 12 dysków SSD 2.5” o pojemności sumarycznej RAW min. 47TB – niedopuszczalne jest mieszanie dysków o różnej pojemności Zainstalowane min. 12 dysków HDD 2.5” o pojemności sumarycznej RAW min. 47TB – niedopuszczalne jest mieszanie dysków o różnej pojemności Zasilanie redundantne, jednofazowe o min. mocy 800W. Obudowa musi umożliwiać instalację redundantnych wentylatorów. Obudowa musi umożliwiać instalację min. 4 procesorów Obudowa musi umożliwiać instalację min. 6TB pamięci RAM DDR4 Obudowa musi pozwalać na instalację min. 6 portów USB (dostępnych na zewnątrz obudowy) z czego min. dwóch portów USB 3.0 (za pomocą oryginalnych modułów producenta, niedopuszczalne jest stosowanie przejściówek firm trzecich) Wymagane jest dostarczenie oryginalnej maskownicy producenta przykrywającej dyski (front obudowy) Obudowa musi pozwalać na instalację serwera HPE ProLiant XL190R Gen10 będącego w posiadaniu Zamawiającego.
JEDNOSTKA PRZETWARZANIA	
Płyta główna, chipset	Płyta główna z możliwością zainstalowania co najmniej dwóch procesorów. Chipset dedykowany przez producenta procesora do pracy w serwerach min. dwuprocesorowych. Konfiguracja umożliwiająca instalację maksymalnej ilości procesorów i pamięci, dostępnej dla zaoferowanej modelu jednostki przetwarzania, bez konieczności uzupełniania o jakiekolwiek elementy.
Procesory	Wszystkie gniazda procesorów obsadzone przez procesory ośmiordzerdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem. Każdy z procesorów osiągający w teście PassMark CPU Mark wynik min. 16500 punktów (http://www.cpubenchmark.net) według wyników testu z dnia 01.07.2020r lub później.
Pamięć RAM	Dla każdego procesora zainstalowane co najmniej 256GB pamięci RAM typu RDIMM o częstotliwości pracy 2666MT/s. w modułach co najmniej po 64GB. Płyta musi obsługiwać minimum 1.5TB pamięci RAM.

	Płyta główna umożliwiająca instalacje min. 8 kości pamięci dla każdego procesora. Możliwe zabezpieczenia pamięci: ECC, Memory Mirror lub równoważne.
Pamięć masowa	Zainstalowane min. dwa dyski M.2 SSD o pojemności minimum 240GB każdy (skonfigurowane w RAID 1) Zainstalowane min. cztery dyski M.2 NVMe o pojemności minimum 240GB każdy
Kontroler dysków	Co najmniej 1 kontroler obsługujący RAID 0, 1, 5, 10, 6 wyposażony w pamięć cache do odczytu i zapisu o pojemności minimum 2GB. Możliwość dokupienia licencji na szyfrowanie dysków.
Połączenia sieciowe	Minimum 4 porty 10/25GbE SFP28 (min. dwa porty powinny zostać obsadzone wkładkami SFP28 25Gb LR w pełni kompatybilnymi z dostarczanym serwerem). Karta/y sieciowe powinny być sygnowane przez producenta serwera i opisane w oficjalnych dokumentach producenta (DataSheet) 1 dedykowany port Ethernet RJ45 na potrzeby systemu zarządzania
Akcelerator graficzny	Możliwość instalacji co najmniej 2 kart GPU typu Nvidia Tesla
Złącza PCI-E	Minimum 3 złącza PCI-E 3.0 x16. Minimum 1 złącze PCI-E 3.0 x16 musi pozostać wolne przy wymaganej konfiguracji węzła (serwera) umożliwiające przyszłą rozbudowę o dodatkowe karty rozszerzające typu Fibre Channel, Infiniband, Ethernet.
Inne porty	Minimum 3 porty USB (na zewnątrz) w tym minimum 1 x USB 3.0, 1x VGA (zintegrowana karta graficzna oferująca minimalną rozdzielczość 1280x1024), 1x port szeregowy Wewnętrzny slot na kartę SD/MicroSD
Wspierane systemy operacyjne	Serwer musi znajdować się na liście zgodności systemów: SUSE Linux Enterprise Server (SLES) 11 SP4 i 12 SP2 Red Hat Enterprise Linux (RHEL) 6.9 i 7.3 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 VMware ESXi 6.5
Bezpieczeństwo	Możliwość wyposażenia serwera w zintegrowany z płytą główną moduł TPM.
ZARZĄDZANIE	
Zarządzanie	Niezależne od zainstalowanego na jednostce przetwarzania systemu operacyjnego, posiadające dedykowany port RJ-45 Gigabit Ethernet umożliwiające: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, SSH - obsługa RESTfull API - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer - integracja z Active Directory - możliwość obsługi przez dwóch administratorów jednocześnie - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
Zarządzanie	Zainstalowany moduł wyposażony w 2 zapewniające redundancję porty RJ-45 1Gb, umożliwiający zagregowane zarządzanie wszystkimi dostarczanymi jednostkami przetwarzania.
ZESTAW NIEZBĘDNY DO ZBUDOWANIA KLASTRA	
Zestaw	Zaoferowany zestaw musi zawierać wszystkie elementy niezbędne do zbudowania i uruchomienia klastra zgodnie z opisem funkcjonalnym.
GWARANCJA	
Gwarancja	5-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w następnym dniu roboczym. W czasie trwania gwarancji, w przypadku uszkodzenia dysku Wykonawca zobowiązany jest dostarczyć nowy dysk w ciągu 24 godzin od zgłoszenia uszkodzenia przez Zamawiającego.

	Wykonawca powinien umożliwić Zamawiającemu zgłaszanie uszkodzeń dysku/ów w trybie 24/7 za pomocą dedykowanego portalu bądź numeru telefonu. W okresie gwarancji Zamawiający ma prawo do bezpłatnego otrzymywania poprawek oraz aktualizacji oprogramowania dostarczonego wraz z serwerem. Procedura serwisowa nie może wymagać od Zamawiającego przeprowadzania testów sprzętu (np. sprawdzania sprzętu w podstawowej konfiguracji), całość procedur serwisowych musi zostać wykonana przez serwisanta.
INNE	
Inne	Serwer musi znajdować się na liście urządzeń wspieranych przez Oprogramowanie do Zarządzani infrastrukturą (pkt. 1.6.5) będące elementem niniejszego postępowania. Wykonawca musi zapewnić min. 5 dniowe szkolenie dla 1 administratora w certyfikowanym ośrodku szkoleniowym. Szkolenie musi obejmować System operacyjny oraz System wirtualizacji w zakresie min.: instalacja, administracja, konfiguracja wirtualizacji, konfiguracja maszyn wirtualnych, zarządzanie klastrem.

1.3 Serwer bazodanowy (2 szt.)

Cecha	Wymagania minimalne
Obudowa	1. do zabudowy w szafie serwerowej 19”, plus wszystkie elementy niezbędne do mocowania i wysuwania do celów serwisowych razem z ramieniem do zarzadzania kablami 2. maksymalna wysokość - 2U 3. mieszcząca co najmniej 8 dysków 2.5" hot-swap 4. wszystkie wyspecyfikowane elementy serwera muszą być w niej zamontowane, o ile nie określono inaczej, 5. wyprodukowana przez producenta płyty głównej 6. wymagane jest dostarczenie oryginalnej maskownicy producenta przykrywającej dyski (front obudowy)
Zasilacz	1. co najmniej 2 szt., nadmiarowe (redundantne) 2. 230V 50Hz, każdy o mocy co najmniej 500 W klasy „Platinum” 3. hot-plug
Chłodzenie	Nadmiarowe wentylatory typu hot-plug
Płyta główna	1. z chipsetem dedykowanym przez producenta procesora do pracy w serwerach co najmniej dwuprocesorowych 2. posiadająca co najmniej 4 interfejsy LAN 1Gb RJ45 RJ45 nie zajmujące slotów PCI-e 3. posiadająca zintegrowaną kartę graficzną z wyjściem VGA 4. posiadająca dodatkowy dedykowany interfejs do zarządzania i monitoringu 1GbE RJ45 5. posiadająca co najmniej 3 porty USB 3.0, w tym co najmniej 1 z przodu obudowy 6. posiadająca co najmniej jeden port SATA 3 7. pozwalająca na zainstalowanie co najmniej 3TB pamięci RAM 8. pozwalająca na zainstalowanie co najmniej 2 fizycznych procesorów 9. posiadająca złącza PCI - co najmniej 3x PCI-E 3.0 x8 , z możliwością rozbudowy do 6x PCI-e 3.0 x8 - minimum 2 złącza PCI-E muszą pozostać wolne przy wymaganej konfiguracji serwera 10. identyczna we wszystkich serwerach
Procesor	Zainstalowany jeden procesory minimum czterordzeniowy, x86 - 64 bity, osiągający w testach PassMark CPU Mark wynik nie gorszy niż 10500 punktów (z dnia 01.07.2020 lub później)
Pamięć RAM	1. co najmniej 128 GB w pełni buforowanej pamięci DDR4 ECC 2. moduły co najmniej po 16 GB 3. taktowanie co najmniej 2666 MHz
Kontroler dysków	1. co najmniej 1 szt. 2. instalowany w dedykowanym złączu lub zintegrowany 3. obsługujący co najmniej 8 dysków SAS/SATA o przepustowości 12 Gb/s 4. obsługujący RAID 0, 1, 5, 10, 50, 6 5. z co najmniej 2 GB pamięci cache do odczytu i zapisu 6. podtrzymanie bateryjne/kondensatorowe dla pamięci cache kontrolera 7. możliwość dokupienia licencji na szyfrowanie dysków 8. możliwość rozbudowy cache kontrolera do minimum 4GB przez wymianę lub zmianę pamięci kontrolera Dodatkowy kontroler HBA SAS 12Gb posiadający minimum 2 zewnętrzne porty SAS do podłączenia napędu taśmowego LTO

Dodatkowe kontrolery sieciowe	Kontroler posiadający co najmniej 2 interfejsy LAN 10/25Gb SFP28, nie zajmujący slotów PCI-e.
Dyski twarde	1. zainstalowane co najmniej 4 dyski 2,5” SSD, hot-plug, o pojemności co najmniej 480GB każdy 2. zainstalowane co najmniej 2 dyski 2,5” SSD, hot-plug, o pojemności co najmniej 240GB każdy
Zdalny interfejs zarządzający	Serwer musi być wyposażony w sprzętowe rozwiązanie zdalnego zarządzania, pochodzące od producenta serwera, niezależne od systemów operacyjnych, posiadające dedykowane złącze RJ-45. Rozwiązane musi mieć możliwość pracy zdalnej w serwerze (wirtualny KVM) z użyciem przeglądarki internetowej, licencja musi zawierać pełną możliwość zdalnego podłączenia napędów wirtualnych typu: FDD, CD/DVD, pamięć USB oraz wirtualnych folderów jak również przechwycenia konsoli graficznej.
Inne	Dodatkowo sprzęt: 1. musi być wspierany przez system Windows 2016 Server, Windows 2012 R2, Vmware, Linux 2. musi zawierać wszystkie licencje i akcesoria niezbędne do uruchomienia serwerów Serwer musi znajdować się na liście urządzeń wspieranych przez Oprogramowanie do Zarządzani infrastrukturą (pkt. 1.6.5) będące elementem niniejszego postępowania.
Dodatkowe wyposażenie	Dwa moduły SFP+ 10GBase-LR
Gwarancja	5-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w następnym dniu roboczym. Uszkodzone nośniki danych pozostają własnością Zamawiającego. W okresie gwarancji Zamawiający ma prawo do bezpłatnego otrzymywania poprawek oraz aktualizacji oprogramowania dostarczonego wraz z serwerem. Procedura serwisowa nie może wymagać od Zamawiającego przeprowadzania testów sprzętu (np. sprawdzania sprzętu w podstawowej konfiguracji), całość procedur serwisowych musi zostać wykonana przez serwisanta.

1.4 Serwerowy System Operacyjny (1 sztuka – 16 core)

Cecha	Wymagania minimalne
Licencja	Licencje na serwerowy system operacyjny muszą być przypisane do każdego z 16tu rdzeni procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego
Funkcje	• Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. • Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: ○ pozwalają na zmianę rozmiaru w czasie pracy systemu, ○ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, ○ umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, ○ umożliwiają zdefiniowanie list kontroli dostępu (ACL).

	• Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Dostępne dwa rodzaje graficznego interfejsu użytkownika: o Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, o Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. • Mechanizmy logowania w oparciu o: o Login i hasło, o Karty z certyfikatami (smartcard), o Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), • Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). • Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: O Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, O Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: ▪ Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ▪ Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, ▪ Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. ▪ Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. ▪ Zdalna dystrybucja oprogramowania na stacje robocze. ▪ Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej ▪ Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ▪ Dystrybucję certyfikatów poprzez http ▪ Konsolidację CA dla wielu lasów domeny, ▪ Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ▪ Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. ▪ Szyfrowanie plików i folderów. ▪ Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). ▪ Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

	▪ Serwis udostępniania stron WWW. ▪ Wsparcie dla protokołu IP w wersji 6 (IPv6), ▪ Wsparcie dla algorytmów Suite B (RFC 4869), ▪ Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, ▪ Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: o Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, o Obsługi ramek typu jumbo frames dla maszyn wirtualnych. o Obsługi 4-KB sektorów dysków o Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra o Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. o Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) • Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. • Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Inne	System musi zapewniać bezproblemową pracę min. 200 aktywnych użytkowników, jeżeli wymagane są tzw. licencje dostępowe należy je dostarczyć wraz z serwerowym systemem operacyjnym.

1.5 Konfiguracja i wdrożenie

1.5.1 Szafy, serwery, okablowanie

W szafach należy zainstalować dostarczane serwery (po jednym w każdej szafie).
Wszystkie urządzenia należy w odpowiedni sposób połączyć i okablować.
Okablowanie powinno zostać umieszczone w odpowiednich uchwytach do okablowania oraz w szczotkach kablowych.
Ilość akcesoriów musi być dostosowana do potrzeb.
Okablowanie musi zostać opisane/oznaczone po każdej stronie.
Każda końcówka kabla powinna zostać wyposażona w opis, który powinien zawierać nazwę urządzenia oraz port, do którego przewód jest podłączony po przeciwnej stronie. Wymaganie to dotyczy zarówno kabli służących do transmisji danych jak i do kabli zasilających.
Dostarczony Serwerowy System Operacyjny należy zainstalować na jednym z dostarczanych serwerów.
Licencję dla pozostałych serwerów dostarczy Zamawiający.

1.5.2 Wirtualizacja oraz Storage

Rozwiązanie musi udostępniać wspólny klaster przetwarzania danych i pamięci masowej o minimalnych parametrach:

System wirtualizacyjny	1. Wirtualizacja mocy obliczeniowej: Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym oraz musi spełniać poniższe warunki:

	o Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 512 logicznych wątków oraz do 12TB pamięci fizycznej RAM o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-8 wirtualnych kart sieciowych o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 2 porty szeregowe o Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2008/2008R2, Windows Server 2012/2012R2, Windows Server 2016, Windows 7, Windows 8.1, Windows 10, SLES 12, SLES 11, REHL 7, RHEL 6, RHEL 5, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux o Rozwiązanie musi umożliwiać przydzielenie pamięci RAM dla maszyn wirtualnych w sposób pozwalający na obsługę większej ilości pamięci niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji o Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych o Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, na maszynie wirtualnej o Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania o Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez bezpieczny szyfrowany kanał, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta głównego (root/Administrator) o Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania/eksportowania systemów operacyjnych wraz z ich konfiguracją i danymi o Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych wirtualnych instancji systemów operacyjnych bez przerywania ich pracy z możliwością zachowania stanu pamięci pracującej maszyny wirtualnej. o Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory lub Open LDAP o Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości pamięci operacyjnej i pojemności przydzielonej przestrzeni dyskowej o System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE o System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych o 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 4000 portów o 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 o Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN), zapewniające również separację warstwy trzeciej o Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi o Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek o Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych wirtualnych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie o Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z serwerów fizycznych na serwery w tym samym lub oddalonym ośrodku przetwarzania

	o Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi o Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury o Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych o Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania o Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to poprawki bezpieczeństwa, bez potrzeby wyłączania wirtualnych maszyn o Rozwiązanie musi posiadać co najmniej 2 niezależne. mechanizmy wzajemnej komunikacji między serwerami, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci o Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie o Oprogramowanie do wirtualizacji musi obsługiwać SAN o Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB o Rozwiązanie musi posiadać możliwość integracji zewnętrznych rozwiązań wykonywania kopii zapasowych o Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do wirtualizacji pamięci masowej (SDS) oraz wirtualzacji sieci (SDN). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami) o System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader o Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów o Licencja na oprogramowanie spełniające powyższe wymagania musi pochodzić z oficjalnego polskiego kanału sprzedaży i być fabrycznie nowa, nigdy nie zarejestrowana czy wykorzystywana. Licencje dostępne w modelu licencjonowania na procesor/rdzeń fizyczny. o Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej o Rozwiązanie powinno posiadać proaktywny/heurystyczny mechanizm, który migruje wirtualne maszyny po wykryciu wzrostu obciążenia lub potencjalnego problemu z serwerem fizycznym. o System/SDS musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich o Rozwiązanie musi umożliwiać szyfrowanie wirtualnych maszyn 2. Zarządzanie środowiskiem wirtualnym o Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej, jak i wirtualnej. o Konsola graficzna musi być dostępna za pomocą przeglądarek. o Każda instancja konsoli może zarządzać dowolną ilością serwerów fizycznych, na której zainstalowane jest oprogramowanie do wirtualizacji (brak ograniczeń licencyjnych). o Rozwiązanie musi zapewniać monitorowanie urządzeń w trybie „Real Time” 3. Wirtualizacja funkcji sieciowych – SDN o Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne o Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej o Rozwiązanie musi posiadać funkcję wirtualnego routera, zapewniającego komunikację środowiska maszyn wirtualnych z siecią fizyczną. o Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN o Oferowane rozwiązanie musi posiadać pełną wymaganą funkcjonalność zarówno funkcji bezpieczeństwa oraz funkcji sieciowych w ramach rozwiązań jednego producenta

	o Rozwiązania musi posiadać funkcję rozproszonego, stanowego firewall'a, umożliwiającego definiowania reguł dla protokołów, portów i adresów. o Każdy serwer fizyczny na którym wykorzystywane jest oprogramowanie do wirtualizacji funkcji sieciowych musi obsługiwać dowolną ilość serwerów wirtualnych (brak ograniczeń licencyjnych). 4. Wirtualizacja przestrzeni dyskowej – SDS o Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD o Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania" operacji odczytu / zapisu (Read/Write IO) po stronie serwerów fizycznych o Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności o Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania / dodatkowych maszyn wirtualnych. Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z zarządzaniem platformą wirtualizacyjną o Rozwiązanie musi zapewniać możliwość budowy wspólnej wysokowydajnej i wysoko dostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 16 serwerów fizycznych o Rozwiązanie musi zapewniać obsługiwanie wolumenów/dysków wirtualnych maszyn do rozmiaru min. 32TB o Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych, aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache'ujący, dysk pojemnościowy o Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania. o Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi szafami rack/chassis o Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną listę wspieranych lub rekomendowanych konfiguracji. o Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawce/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery) o Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej o Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych o Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych, o Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych. o Rozwiązanie musi posiadać listę wspieranych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 5 niezależnych producentów sprzętu serwerowego dostępnego na rynku Unii Europejskiej.

	o System musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością o Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej. o Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla min.: technologii deduplikacji oraz technologii implementującej zabezpieczenie danych poprzez pojedynczą i podwójną parzystość za pomocą oprogramowania. o Rozwiązanie musi zapewniać automatyczne rebalansowanie i przywracanie bezpieczeństwa danych bez konieczności stosowania dedykowanych nadmiarowych dysków typu HotSprare, a wyłącznie przy wykorzystaniu wolnego miejsca na dostępnych nośnikach. o Każdy serwer fizyczny na którym wykorzystywane jest oprogramowanie do wirtualizacji przestrzeni dyskowej musi obsługiwać dowolną ilość serwerów wirtualnych (brak ograniczeń na serwery czy pojemność w jakimkolwiek aspekcie licencyjnym). 5. Skalowanie całości platformy o Rozwiązanie musi udostępniać wspólny klaster mocy obliczeniowej i przestrzeni dyskowej, agregujący przetwarzanie danych, system rozproszonej pamięci masowej oraz serwerowy segment sieci. o Wirtualizacja mocy obliczeniowej musi pozwalać na połączenie pojedynczych node-ów serwerowych w klaster, umożliwiający bezprzerwowe przenoszenie maszyn pomiędzy serwerami fizycznymi czy natychmiastowe ich przywracanie w przypadku jakiejkolwiek awarii na pozostałych node-ach klastra. o Wirtualizacja zasobów dyskowych musi całkowicie eliminować złożoną dedykowaną sieć pamięci masowej. Rozproszona pamięć masowa musi być niezależna od producentów sprzętu i stanowić wysokodostępne rozproszone, samolecząc się rozwiązanie. o Każdy serwer musi zostać wyposażony w zestaw licencji umożliwiający wykorzystanie wszystkich funkcjonalności opisanych jako wirtualizacji mocy obliczeniowej, wirtualizacja funkcji sieciowych, wirtualizacja przestrzeni dyskowej.
Licencja	Jeżeli wymagana jest licencja na system wirtualizacyjny Wykonawca zobowiązany jest do dostarczenia odpowiedniej licencji pozwalająca na uruchomienie wszystkich opisanych wyżej funkcjonalności na dostarczanych serwerach. Licencja nie może być licencją typu Essentials tj. z ograniczeniem do maksymalnej ilości hostów.

Koncepcja zakłada migrację z rozwiązań niezagregowanych do pojedynczej skonsolidowanej opartej na oprogramowaniu pojedynczego producenta platformy, agregującej przetwarzanie danych - wirtualizacja serwerów, system rozproszonej pamięci masowej oraz serwerowy segment sieci. Wirtualizacja przetwarzania danych, konsoliduje obciążenia by lepiej wykorzystać moc obliczeniową i zapobiega marnowaniu zasobów (CPU, RAM), których nie mógłby wykorzystać pojedynczy serwer. Wirtualizacja pozwala połączyć pojedyncze node-y serwerowe w klaster, umożliwiający bezprzerwowe przenoszenie maszyn pomiędzy serwerami fizycznymi czy natychmiastowe ich przywracanie w przypadku jakiejkolwiek awarii na pozostałych node-ach klastra.

Rozproszona pamięć masowa całkowicie eliminuje złożoną dedykowaną sieć pamięci masowej oraz nie wymaga jakiegokolwiek własnościowego sprzętu o ograniczonej dostępności. Rozproszona pamięć masowa musi być niezależna od producentów sprzętu i wymagań jakiejkolwiek współdzielonej infrastruktury, musi mieć możliwość obsługi bezpośrednio widocznych dla niej indywidualnych urządzeń pamięci masowej. Musi być to wysokodostępne rozproszone, samolecząc się rozwiązanie. Zapewniać poziom bezpieczeństwa danych, gwarantujący pełne trzy kopie każdego fragmentu danych, na niezależnych urządzeniach fizycznych.

Każda kopia danych musi być replikowana synchronicznie, tak by w każdej chwili możliwe było natychmiastowe wykorzystanie którejkolwiek z kopii z pewnością, że jest ona identyczna z pozostałymi. Do rozmieszczania danych na poszczególnych dyskach nie może być wykorzystywany bezpośrednio żaden mechanizm typu RAID, dane w każdej zapisanej kopii powinny być dostępne natychmiast nawet w przypadku awarii, bez konieczności przeliczania sum kontrolnych itp. Rozwiązanie musi zapewniać automatyczne rebalansowanie i przywracanie bezpieczeństwa danych bez konieczności stosowania dedykowanych nadmiarowych dysków typu HotSpare, a wyłącznie przy wykorzystaniu wolnego miejsca na dostępnych nośnikach. Mechanizmy rozproszonej pamięci muszą dbać o to by najczęściej wykorzystywane dane były na najszybszych dostępnych nośnikach (NVMe PCIe, NVDIMM, SSD) oferując wydajność dedykowanych urządzeń przy jednoczesnej elastyczności pamięci współdzielonej.

System musi pozwalać na „rozciągnięcie" klastra na dwie odrębne szafy serwerowe, nawet w przypadku połączenia ich wyłącznie pojedynczym połączeniem sieciowym Ethernet, przy czym dla nominalnego trybu dystrybucji danych taki rozciągnięty klaster gwarantować musi ciągłość pracy nawet w przypadku awarii dowolnej połowy elementów klastra. Rozwiąza-

nie musi być oparte o co najmniej 2 niezależne autonomiczne node-y. Rozproszona pamięć masowa musi zapewniać możliwość uruchomienia wolumenów o mieszanym zabezpieczeniu danych, pozwalających na zdefiniowanie w ramach tego samego wolumenu pojemności obsługiwanej w ramach pełnej kopii danych oraz pojemności dla której wykorzystywane jest parzystość, przy czym migracja danych pomiędzy tymi dwiema pulami musi odbywać się bez fizycznego przenoszenia danych wyłącznie przy wykorzystaniu operacji na metadanych i dodania sum kontrolnych.

Rozwiązanie musi wspierać maszyny wirtualne, ich wysoką dostępność oraz kopie migawkowe.

Wszystkie opisane funkcjonalności muszą zostać w całości objęte dostarczanym licencjami i nie mogą mieć ograniczenia na pojemność w jakimkolwiek aspekcie licencyjnym. Rozwiązanie musi umożliwiać rozbudowę dostarczonej konfiguracji nominalnej o dodatkowe pojedyncze podzespoły, jak dodatkowe dyski.

System plików macierzy rozproszonej musi wspierać oferowane mechanizmy wirtualizacji i zapewniać akceleracją operacji na wirtualnych dyskach maszyn w zakresie tworzenia i scalania oraz scalania kopii migawkowych. Musi mieć on wbudowane mechanizmy realtime tiering-u, a także wspólny dla całego klastra mechanizm Storage QoS co najmniej w zakresie OPs/MBps Limits (maximums) oraz IOPs Guarantees (minimums), z możliwością przypisania polisy do pojedynczego wirtualnego dysku.

- Platforma musi zostać zainstalowana bezpośrednio na sprzęcie fizycznymi, udostępniać mechanizmy wirtualizacji i udostępniać klaster wysokodostępny.
- Muszą zostać wdrożone mechanizmy klonowania/eksportowania/kopii migawkowych systemów operacyjnych wraz z ich konfiguracją i danymi na platformie wirtualizacji.
- Instalacja musi obejmować mechanizm przydzielania i konfiguracji uprawnień z integracją z usługami katalogowymi Microsoft Active Directory.
- Wdrożenie musi obejmować uruchomienie wirtualnego przełącznika sieci wirtualnej i łączącego maszyny wirtualne i zapewniającego przyłączania do niego co najmniej dwóch fizycznych kart sieciowych wraz z obsługą wirtualnych sieci lokalne (VLAN).
- Połączenie wirtualnego przełącznika musi być zrealizowane poprzez agregację połączeń 25GbE.
- Muszą zostać uruchomione mechanizmy przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
- Muszą zostać uruchomione mechanizmy redundancji w przypadku awarii np. serwera fizycznego, przełączające na inne serwery infrastruktury.
- Muszą zostać uruchomione mechanizmy bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to poprawki bezpieczeństwa, bez potrzeby wyłączania wirtualnych maszyn.
- Wdrożony musi zostać mechanizm automatycznego równoważenia obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma.
- Uruchomiony musi zostać mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich.
- Musi zostać zaimplementowana centralna konsola graficzna do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
- Wdrożenie musi obejmować budowę wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych.
- Uruchomiony musi zostać mechanizm optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania".
- Rozwiązanie storage musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej.
- Rozwiązanie musi udostępniać wspólny klaster mocy obliczeniowej i przestrzeni dyskowej, agregujący przetwarzanie danych, system rozproszonej pamięci masowej oraz serwerowy segment sieci.

Klaster łącznie musi oferować co najmniej:

- 64 fizyczne rdzenie
- 2000GB pamięci RAM, zbudowanej w oparciu o moduły pamięci wykorzystujące symetrycznie wszystkie kanały pamięci procesora.
- 180TB przestrzeni użytkowej na dane na dyskach, zbudowanej w oparciu o co najmniej 24 dyski w każdym serwerze.

1.5.3 Migracja istniejącego środowiska

Zamawiający posiada 10 maszyn wirtualnych pracujących w środowisku wirtualnym Vmware ESX 5.5 na 3 serwerach fizycznych z licencją Vmware Essentials Plus KIT. Maszyny korzystają z systemów:
- Windows Server 2012 R2
- Debian
- FreeBSD
- Windows 7
- Windows Server 2012

- Ubuntu
- CentOS
- Windows Server 2016

Zamawiający wymaga wykonania migracji wszystkich maszyn wirtualnych do nowego środowiska. Wymagane jest skonfigurowanie dla każdej ze wskazanych przez Zamawiającego maszyn trybu wysokiej dostępności (automatyczne uruchamianie na działającym nodzie klastra).

1.6 Sieć

1.6.1 Przełącznik szkieletowy (2 szt.)

Każdy switch oprócz podstawowej funkcjonalności, musi prezentować dodatkowe, zaawansowane opcje. Do opcji tych zalicza się:

- zarządzanie jakością pakietów (QoS) - zarządzanie jakością pakietów, czyli QoS oznacza zdolność switche do różnego traktowania poszczególnych ramek. Mając taką funkcję, przełącznik może wykorzystywać ramki o wyższym priorytecie, używając do tego celu oznaczenia znajdującego się w ramkach Ethernet (IEEE 802.1p oraz 802.1Q).
- grupowanie portów - grupowanie (trunk) dwóch lub więcej portów przełącznika pozwala stworzyć jedną logiczną ścieżkę. Ta funkcja umożliwia zwiększenie przepustowości występującej między dwoma przełącznikami.
- VLAN (Virtual Local Area Network) - funkcja VLAN, która pozwala na odizolowanie logiczne grupy urządzeń w ramach współdzielonego medium. Jednocześnie, izolacja ruchu przez porty switche nie pozwala na analizę ruchu w sieci.
- monitoring portów - Funkcja port monitoring umożliwia monitorowanie ruchu na kilku portach przełącznika przez jeden wybrany port.
- redundancja,
- SNMP itp.
- w przypadku rozbudowanych sieci, składających się z wielu połączonych przełączników, niezbędne okażą się mechanizmy zapobiegania awariom (STP, RSTP,MC-LAG).

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	• Wysokość w szafie 19” – 1U o głębokości maksymalnie 55 cm • Maksymalny pobór mocy nie większy niż 600W • Minimalny zakres temperatur pracy od 0°C do 40°C • Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management • Port konsoli RS232 ze złączem DB9 lub RJ45 • Port konsoli USB • Port USB 2.0 (niezależny od portu konsoli USB)
Funkcjonalność	• Wydajność: minimum 4 Tbps (prędkość przełączania „wirespeed” dla każdego portu przełącznika) • Wydajność: minimum 2000 Mp/s • Przełączanie w warstwie 2 i 3 modelu OSI • Wielkość bufora pakietów (packet buffer): minimum 32MB • Modularny system operacyjny bazujący na jądrze Linux • Minimum 70GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash) podzielonej na minimum dwa niezależne nośniki (np. eUSB oraz CF). Nie dopuszcza się pamięci instalowanej na zewnątrz przełącznika (np. do zewnętrznego portu USB) • Oparty o jądro Linux Bootloader powinien znajdować się na niezależnym od właściwego systemu operacyjnego nośniku pamięci. • Oprócz uruchamiania systemu operacyjnego Bootloader musi pozwalać na: dostęp do logów, zrzutów pamięci (coredump) i konfiguracji, naprawę i formatowanie przestrzeni pamięci, wygrywanie i aktualizację systemu operacyjnego, czyszczenie konfiguracji, czyszczenie i zmianę haseł administratorskich, wybór wersji systemu operacyjnego • Minimum 16GB pamięci operacyjnej • Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów)

	• Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. • Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) • Funkcja łączenia przełączników w grupy co najmniej 2 urządzeń, w sposób ciągły synchronizujących ze sobą konfiguracje przy zachowaniu niezależnych płaszczyzn zarządzani (control plane). Przełączniki połączone w grupę muszą zapewnić co najmniej: realizację łączy agregowanych w ramach różnych przełączników będących w grupie, architekturę, w której oba przełączniki są aktywne dla funkcji L2 i L3, funkcje typu ISSU lub Live Upgrade. • Tablica adresów MAC o wielkości minimum 95000 pozycji • Obsługa ramek Jumbo o wielkości co najmniej 9kB • Obsługa Quality of Service • Obsługa mechanizmów, co najmniej: strict priority (SP) queuing, Deficit weighted round robin (DWRR) queuing oraz SP+DWRR • Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol • Obsługa sieci IEEE 802.1Q VLAN – 4094 jednoczesnych sieci VLAN • Obsługa IGMP v2/v3, IGMP Snooping, PIM SM • Routing IPv4 – statyczny i dynamiczny (min. OSPF, BGP) • Routing IPv6 – statyczny i dynamiczny (min. OSPFv3) • Obsługa ECMP (Equal Cost Multi Path) • Obsługa VRRP • Obsługa tunelowania GRE • Obsługa Virtual Routing and Forwarding (VRF) • Obsługa funkcji Multicast VLAN • Tablica routingu o pojemności co najmniej 120000 wpisów dla IPv4 oraz co najmniej 50000 wpisów dla IPv6 • Obsługa funkcji klienta DHCP • Obsługa DHCP Relay dla IPv4 i IPv6 • Obsługa list ACL (co najmniej 16000) na bazie informacji z warstw 2 i 3 modelu OSI. • Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia • Obsługa standardu 802.1p • Funkcja ograniczania ruchu typu multicast i broadcast • Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p • Funkcja kopiowania ruchu wejściowego i wyjściowego (port mirroring) lokalnego (w obrębie urządzenia) i zdalnego (na porty znajdujące się na innym urządzeniu) • Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS oraz TACACS+ • Zarządzanie poprzez port konsoli (CLI), SNMP 2c, SNMP 3, interfejs graficzny (WebGUI) znajdujący się bezpośrednio na urządzaniu oraz SSH v2 • Obsługa Syslog • Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) • Obsługa sFlow • Obsługa Network Time Protocol (NTP) • Obsługa Secure FTP (SFTP) oraz TFTP • Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty. • Obsługa skryptów w języku Python • Obsługa REST API • Obsługa RMON (minimum grupy 1, 2, 3 i 9) • Obsługa funkcji diagnostycznych ping i traceroute dla IPv4 i IPv6

	• Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego • Przechowywanie co najmniej dwóch wersji oprogramowania na przełączniku • Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). • Przełącznik musi posiadać mechanizm (automatycznego i ręcznego) tworzenia punktów szybkiego odtwarzania konfiguracji. Punkty szybkiego odtwarzania muszą zawierać aktualne zrzuty działającej konfiguracji oraz informacje dodatkowe (co najmniej: typ punktu, datę utworzenia, wersję oprogramowania, dane sprzętu, dane zapisującego punkt przywracania, opis). System musi umożliwiać ich kopiowanie i uruchamianie na innych urządzeniach tego samego typu. W urządzeniu musi być przechowywanych nie mniej niż 60 punktów przywracania konfiguracji. Przełącznik musi posiadać funkcję porównywania ze sobą (oraz prezentacji różnic) dwóch punktów odtwarzania konfiguracji oraz punktu odtwarzania konfiguracji z konfiguracją aktualnie działającą i konfiguracją zapisaną jako bieżąca. • Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
Wyposażenie	• Minimum 48 portów 1GbE/10GbE/25GbE SFP28 umieszczonych z przodu obudowy. Porty muszą wspierać co najmniej standardy: 25GBase-SR, 25GBaseLR, 25GBase-eSR, 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-T, 1000Base-T, 1000BaseSX, 1000BaseLX, kable DAC i AOC. • Minimum 8 portów 40/100GbE QSFP28 umieszczonych z przodu obudowy. Porty muszą wspierać co najmniej standardy: 100GBase-SR4, 100GBase-LR4, 40GBase-SR4, 40GBase-LR4, kable DAC i AOC • Wszystkie porty muszą być od siebie niezależne, nie dopuszcza się portów typu Combo • Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. • Minimum 4 wkładki światłowodowe 25GBase-LR SFP28 • Minimum 2 kable DAC 100Gb QSFP28 • Minimum 10 wkładek światłowodowych 10GBase-LR SFP+ Wszystkie akcesoria muszą być w pełni kompatybilne z dostarczanym przełącznikiem.
Gwarancja	Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu
Inne	• Producent musi posiadać w ofercie jednorodny system zarządzania pozwalający na konfigurację, zarządzanie i monitoring wszystkimi wyspecyfikowanymi urządzeniami sieciowymi. System zarządzania nie jest przedmiotem postępowania, ale musi być dostępny w chwili składania oferty. • Wszystkie przełączniki muszą być fabrycznie nowe.

1.6.2 Przełącznik dostępowy TYP1 (2 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	• Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 25cm.
Wyposażenie	• Co najmniej 48 porty w standardzie 10/100/1000BaseT • Minimum 4 porty 10Gigabitowe SFP+, niezależne od wymaganych portów 10/100/1000BaseT (obsadzone wkładkami 10GBase-LR w pełni kompatybilnymi z dostarczanymi przełącznikami). Wszystkie porty muszą być aktywne
Funkcjonalność	• Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN • Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) • Obsługa Secure FTP • Obsługa 802.3ad Link Aggregation Protocol (LACP) • Obsługa Simple Network Time Protocol (SNTP) v4 • Wielkość tablicy adresów MAC: minimum 16000 • Obsługa LLDP i LLDP-MED • Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting • Możliwość autoryzacji użytkowników zgodna z 802.1x • Możliwość autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, • Funkcja automatycznego provisioningu i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji • Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) • Obsługa list kontroli dostępu (ACL) • Obsługa ramek Jumbo o wielkości co najmniej 9220 bajtów • Obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP (802.3ad) • Obsługa IP SLA dla ruchu typu VoIP (co najmniej monitoring jakości połączeń głosowych przy pomocy testów jitter UDP) • Obsługa routingu statycznego (min 3k tras IPv4 i IPv6) • Obsługa routingu dynamicznego RIP i RIPng • Obsługa protokołu IEEE 802.1v • Obsługa ECMP • Obsługa protokołu TR-069 • Obsługa protokołów GVRP i MVR • Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
Gwarancja	Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego, w tym wsparcia telefonicznego w trybie 8x5.
Inne	• Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji producenta. • Wszystkie przełączniki muszą być fabrycznie nowe. • Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT • Pobór mocy nie większy niż 50W • Wydajność przełączania co najmniej 175 Gbps oraz przepustowość 110 Mpps dla pakietów 64 bajtowych • Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az • Bufor pakietów nie mniejszy niż 12MB • Minimum 4GB Flash • Minumim 1GB RAM • Opóźnienie dla portów 10G nie większe niż 1.6 µs

	• Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3 • Oprogramowanie do zarządzania infrastrukturą (będące częścią niniejszego postępowania) musi być wymienione w oficjalnej dokumentacji przełączników jako w pełni kompatybilne

1.6.3 Przełącznik dostępowy TYP2 (4 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	• Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 45cm.
Wyposażenie	• Co najmniej 48 porty w standardzie 10/100/1000BaseT z PoE+ (802.3at) • Minimum 4 porty 10Gigabitowe SFP+, niezależne od wymaganych portów 10/100/1000BaseT (obsadzone wkładkami 10GBase-LR w pełni kompatybilnymi z dostarczanymi przełącznikami). Wszystkie porty muszą być aktywne
Funkcjonalność	• Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN • Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) • Obsługa Secure FTP • Obsługa 802.3ad Link Aggregation Protocol (LACP) • Obsługa Simple Network Time Protocol (SNTP) v4 • Wielkość tablicy adresów MAC: minimum 16000 • Obsługa LLDP i LLDP-MED • Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting • Możliwość autoryzacji użytkowników zgodna z 802.1x • Możliwość autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, • Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) • Funkcja automatycznego provisioningu i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji • Obsługa list kontroli dostępu (ACL) • Obsługa ramek Jumbo o wielkości co najmniej 9220 bajtów • Obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP (802.3ad) • Obsługa IP SLA dla ruchu typu VoIP (co najmniej monitoring jakości połączeń głosowych przy pomocy testów jitter UDP) • Obsługa routingu statycznego (min 3k tras IPv4 i IPv6) • Obsługa routingu dynamicznego RIP i RIPng • Obsługa protokołu IEEE 802.1v • Obsługa protokołów GVRP i MVRP • Obsługa ECMP • Obsługa protokołu TR-069 • Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
Gwarancja	Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego, w tym wsparcia telefonicznego w trybie 8x5.
Inne	• Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji producenta. • Wszystkie przełączniki muszą być fabrycznie nowe. • Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT • Pobór mocy nie większy niż 100W (bez PoE)

	• Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W • Wydajność przełączania co najmniej 175 Gbps oraz przepustowość 110 Mpps dla pakietów 64 bajtowych • Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az • Bufor pakietów nie mniejszy niż 12MB • Minimum 4GB Flash • Minumim 1GB RAM • Opóźnienie dla portów 10G nie większe niż 1.6 µs • Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3 • Oprogramowanie do zarządzania infrastrukturą (będące częścią niniejszego postępowania) musi być wymienione w oficjalnej dokumentacji przełączników jako w pełni kompatybilne

1.6.4 Urządzenie dostępowe sieci bezprzewodowej 802.11a/b/g/n/ac/ax (30 szt.)

Dla potrzeb sieci bezprzewodowej na terenie placówki zaplanowano 30 sztuk centralnie zarządzanych punktów dostępowych, dedykowanych do zastosowań w szpitalach.
Zaprojektowany kontroler sieci bezprzewodowej (wbudowany w AccessPointy) to w pełni wyposażony, zintegrowany kontroler dostępu mobilnego, który spełnia wiele wymagań dotyczących mobilnych sieci bezprzewodowych, zabezpieczeń i zdalnego korzystania z sieci.
Urządzenia (AP) muszą zapewnić w przyszłości zainstalowanie dedykowanego kontrolera sieci bezprzewodowej pochodzącego od tego samego producenta co dostarczane AccessPointy.
Zastosowana w nim technologia adaptacyjnego zarządzania drogą radiową dostosowuje sposób interakcji klientów Wi-Fi i sprawdza, czy aplikacje do obsługi transmisji danych, głosu oraz wideo dysponują odpowiednimi zasobami w celu oferowania użytkownikom optymalnego komfortu korzystania z sieci bezprzewodowych.

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Funkcjonalność	1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax. 2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej 3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: • Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https • Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki • Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 4. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: • System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego • W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny • Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe • Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję • Tworzenie klastra do 130 urządzeń

	5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP 6. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa 7. W system musi być wbudowany serwer DHCP 8. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów 9. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach: • EAP-TLS • PEAP-MSCHAPv2 • PEAP-GTC • TTLS-MSCHAPv2 10. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP 11. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID 12. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN 13. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez: • Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania • Zewnętrzny portal WWW 14. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT 15. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne 16. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż: • Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe • Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu • Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma • Wykrywanie interferencji oraz miejsc bez pokrycia sygnału • Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz • Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g) • Wsparcie dla 802.11d oraz 802.11h • Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane 17. Minimalizacja interferencji związanych z sieciami 3G/4G LTE 18. Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej 19. Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 6dBm) 20. Obsługa roamingu klientów w warstwie 2 21. Obsługa monitoringu przez SNMP 22. Obsługa logowania na zewnętrznym serwerze SYSLOG 23. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci 24. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci 25. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie: • Widok diagnostyczny prezentujący problemy z sygnałem/prędkością • Wykorzystanie pasma

	• Ilość klientów korzystających z systemu/interferujących • Ilość ramek wejściowych/wyjściowych dla każdego radia • Ilość odrzuconych/błędnych ramek/s dla każdego radia • Szum tła dla każdego radia • Wyświetlanie logów systemowych 26. Punkt dostępowy musi posiadać co najmniej 2 wbudowane anteny pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 4.3 dBi dla 2,4GHz, 5.5 dBi dla 5 GHz 27. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax 28. Praca w trybie SU MIMO 2X2:2 dla 5GHz 29. Specyfikacja radia 802.11a/n/ac/ax: • Obsługiwana technologia OFDM oraz OFDMA • Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM • Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm • Prędkości transmisji: o 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a, o MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n o MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac o MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz) o MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz) • Obsługa HT – kanały 20/40MHz dla 802.11n • Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac • Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax • Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz • Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac • Wsparcie dla: o MRC (Maximal ratio combining) o CDD/CSD (Cyclic delay/shift diversity) o STBC (Space-time block coding) o LDPC (Low-density parity check) o Technologia TxBF 30. Specyfikacja radia 802.11b/g/n/ax: • Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA • Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM • Moc transmisji konfigurowalna przez administratora 31. Punkt dostępowy musi posiadać co najmniej: • 1 interfejs 100/1000BaseT o z funkcją auto-sensing link oraz MDI/MDX o z funkcją PoE/PoE+ o ze wsparciem dla standardu 802.3az Energy Efficient Ethernet (EEE) • interfejs konsoli RS-232 (RJ-45) lub USB • interfejs USB 2.0 (Typ-A, niezależny od portu konsoli) • przycisk przywracający konfigurację fabryczną • slot zabezpieczający Keningston
Gwarancja	Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

Inne	• Oferowane AccessPointy muszą pozwalać na stworzenie klastra z urządzeniami Aruba AP-207 będącymi w posiadaniu Zamawiającego • Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni • Parametry pracy urządzenia: o Temperatura otoczenia (zakres minimalny): 0-50 º C o Wilgotność (zakres minimalny): 5% - 92% o Obsługiwane standardy: • Ethernet IEEE 802.3 / IEEE 802.3u • Power-over-Ethernet IEEE 802.3af • Wireless IEEE 802.11a/b/g/n/ac/ax o Znak CE o EN 60601-1-1, EN60601-1-2 • Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE oraz przy pomocy lokalnego zasilacza DC (zasilacz nie musi być dołączony) • Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac • Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

1.6.5 Oprogramowanie do zarządzania infrastrukturą (1kpl.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Funkcjonalność	1. System musi być zbudowany w architekturze klient – serwer 2. System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułów dających dodatkową funkcjonalność, minimalnie: a. Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA b. Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetFlow (lub podobnych protokołów) oraz analizy zawartości pakietów SMTP, FTP, http c. Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS d. Zarządzanie dostępem zdalnym Ipsec/VPN e. Wbudowany serwer TACACS f. Funkcja monitorowania wydajności aplikacji 3. System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru Systemu 4. Licencja na System musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi różnych producentów 5. System musi posiadać funkcje umożliwiać automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet 6. Zarządzanie siecią bezprzewodową WLAN (licencja pozwalająca na obsługę co najmniej 50 punktów dostępowych) 7. Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz NetFlow (lub podobnych protokołów) z urządzeń sieciowych oraz obrazowanie wyników (licencja na obsługę w tym zakresie co najmniej 5 urządzeń jednocześnie) 8. System musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP i wyświetlania informacji co najmniej o: a. Średnim wykorzystaniu CPU i pamięci RAM b. Średnim czasie odpowiedzi urządzenia c. Obciążeniu interfejsów (dla ruchu wchodzącego i wychodzącego) d. Ilość błędnych lub odrzuconych pakietów na interfejsie 9. System musi posiadać funkcje konfiguracji urządzeń po protokole SNMP i SSH

	10. System musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backup'ów (ręcznie oraz automatycznie w określonych odstępach czasu) oraz grupowego implementowania konfiguracji na zarządzane urządzenia. System musi zachowywać historię tworzenia backup'ów (minimum 30 dni) wraz z informacją czy przebiegł on pomyślnie, a w przypadku, jeżeli nie, powinien także poinformować o przyczynie niepowodzenia 11. System musi pozwalać na tworzenie szablonów konfiguracji co najmniej w oparciu o cały plik konfiguracyjny, fragment konfiguracji, skrypt CLI, skrypt TCL. 12. System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń, w tym możliwość przechowywania kilku wersji oprogramowania dla jednego modelu urządzenia, możliwość importowania obrazu z komputera do Systemu (tzw. Offline), możliwość pobrania obrazu do Systemu bezpośrednio z Internetu (tzw. Online/LiveUpdate) 13. System musi pozwalać na globalne zarządzanie VLAN, tzn. na tworzenie, modyfikowanie oraz usuwanie VLAN jednocześnie ze wszystkich lub wybranych przełączników zarządzanych przez System. Musi istnieć także możliwość automatycznego generowania map logicznej topologii sieci obrazującej konkretny VLAN a zarządzanych urządzeniach. 14. System musi posiadać funkcję zarządzania listami kontroli dostępu (ACL), w tym: możliwość importowania ACL z urządzeń i tworzenie na ich podstawie szablonu, tworzenie ACL w systemie zarządzania, możliwość pojedynczej lub grupowej implementacji przechowywanych w systemie ACL na urządzeniach 15. System musi posiadać możliwość wyświetlania zbiorczej tablicy routingu zbudowanej w oparciu o tablice zarządzanych urządzeń 16. System musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. Dashboard (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy) 17. System musi generować alarmy na podstawie takich parametrów jak: wykorzystanie CPU, wykorzystanie RAM, temperatura urządzenia, obciążenie interfejsów fizycznych na wejściu i wyjściu, ilość odrzuconych pakietów; Muszą być dostępne co najmniej dwa poziomy alarmu dla pojedynczego parametru oraz muszą być one możliwe do zmiany. 18. System musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS'em wraz z możliwością konfiguracji konkretnego zakresu czasowego i dnia tygodnia, w którym wiadomości będą wysyłane. 19. System musi pozwalać na budowanie widoków przez administratora 20. System musi posiadać funkcje generowania raportów (co najmniej w formatach PDF, CSV, Excel, XLSX, Docx) w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta. Generowanie raportów musi się odbywać na życzenie (on demand) i w regularnych odstępach czasowych (scheduled, np. codziennie, raz w tygodniu, raz na kwartał itp.) 21. System musi posiadać narzędzia graficznej prezentacji topologii sieciowej wraz z dynamiczną prezentacją zmian stanu urządzeń oraz poziomem występujących na nich alarmów. Musi być też możliwość zmiany ikony reprezentującej urządzenie na topologii sieci wraz z możliwością wykorzystania różnych ikon dla różnych poziomów alarmów na urządzeniu. 22. System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji sprzętu używanego w sieci. 23. System musi posiadać funkcje lokalizowania użytkowników przewodowych po adresie IP lub MAC. Wynikiem musi być wskazanie konkretnego portu zarządzanego urządzenia sieciowego, do którego podłączony jest użytkownik 24. System musi posiadać funkcję powiązywania konkretnego interfejsu fizycznego zarządzanego urządzenia z adresem MAC urządzenia końcowego, które będzie miało dostęp do sieci tylko na tym interfejsie. Po wykryciu nieautoryzowanej próby połączenia musi być możliwość wygenerowania alarmu, wyłączenia interfejsu po określonym czasie od zaistnienia zdarzenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) oraz ponownego włączenia interfejsu po określonym czasie od wyłączenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) 25. System musi posiadać predefiniowaną bazę zakresów adresów MAC dla urządzeń sieciowych oraz biurowych wiodących producentów. Baza musi być zbudowana co najmniej dla takich producentów jak: Cisco, Epson, Toshiba, NEC,

	Nortel, Canon, Sony, Samsung, 3Com, Siemens, Nokia, Apple, Lexmark, Xerox, Avaya, D-Link, LG, Dell, Alcatel, Netgear, HPE, TP-Link, Ruckus oraz Huawei. Musi istnieć możliwość ręcznego dodania wpisu do tej bazy. 26. System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie 27. System musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym, w tym: a. Wykrywanie ataków między innymi takich jak: Duplicate ARP Address, ICMP Flood, TCP Port Scan, WinNuke, IP Spoofing, ICMP Redirect, Source Route, SYN Flood, UDP Port Scan, UDP Flood, Ping of Death, DHCP Server Detect b. Stworzenie topologii obrazującej logiczne połączenia między urządzeniami objętymi jednym lub kilkoma atakami sieciowymi, tzn. pokazuje urządzenie/urządzenia będące źródłem ataku i łączy je z urządzeniem/urządzeniami będącymi celem ataku. c. Stworzenie topologii obrazującej fizyczne połączenie między urządzeniami objętymi pojedynczym atakiem sieciowym, tzn. pokazuje całą ścieżkę fizyczną między źródłem, a celem ataku. 28. System musi posiadać funkcję Telnet/SSH oraz GUI proxy umożliwiającą zarządzanie CLI/Web przez przeglądarkę Internetową 29. System musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android 30. System musi posiadać funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox) 31. System musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail 32. System musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń. Dodatkowo musi być możliwość stworzenia kont jedynie z uprawnieniami do podglądu – bez możliwości dokonywania zmian w systemie ani na urządzenia. 33. System musi posiadać funkcję zarządzania VXLAN – tworzenie listy urządzeń wspierających VXLAN, tworzenie tuneli, tworzenie topologii sieci VXLAN, wyświetlanie informacji o statystykach ruchu w tunelach 34. System musi posiadać funkcje zarządzania siecią wirtualną poprzez integrację z VMware (minimum wersja 6.0) i Microsoft Hyper-V(minimum w wersji 2012). Między innymi musi pozwalać na: a. Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem VMware ESX z wykorzystaniem protokołu SOAP. b. Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Virtual Machine Manager z wykorzystaniem Windows PowerShell. c. Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Hyper-V z wykorzystaniem protokołu WMI. d. Zarządzanie siecią wirtualną, w tym serwerami VMware vCenter Server oraz Microsoft Virtual Machine Manager, wirtualnymi maszynami oraz wirtualnymi przełącznikami. e. Migrację wirtualnych maszyn pomiędzy fizycznymi serwerami. f. Przedstawienie wszystkich zasobów, szczegółowych informacji o nich oraz ich wzajemnych relacji w środowisku wirtualnym. Wymaga się, aby był wgląd minimum w: • Listę wszystkich fizycznych serwerów VMware ESX oraz Microsoft Hyper-V dostępnych w sieci. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: producent, model, nazwa serwera, adres IP, informacje na temat Managera sieci wirtualnej, ilość pamięci RAM (wraz z poziomem wykorzystania),

	CPU (wraz z poziomem wykorzystania) oraz informację czy dany serwer wspiera funkcję migracji maszyn wirtualnych. • Listę wirtualnych przełączników przyporządkowanych do konkretnych serwerów VMware ESX oraz Microsoft Hyper-V. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa przełącznika, ilość wirtualnych portów. • Listę wirtualnych maszyn przyporządkowanych do konkretnych przełączników wirtualnych. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa wirtualnej maszyny, adres IP, stan maszyny (Running, Stopped, Suspended). g. Zmianę stanu (minimum: Start VM, Stop VM, Suspend VM, Reset VM) i parametrów wirtualnej maszyny takich jak: zasoby CPU, ilość pamięci RAM, ilość przestrzeni dyskowej. h. Dodawanie, klonowanie i usuwanie wirtualnych masz. i. Kreowanie szablonów służących do tworzenia nowych wirtualnych maszyn, gdzie można zdefiniować parametry początkowe takie jak: nazwę VMware ESX/Microsoft Hyper-V, zasoby CPU, ilość pamięci RAM, przestrzeń dyskową, system operacyjny wirtualnej maszyny. j. Dodawanie wirtualnych przełączników wraz z możliwością wyboru konkretnych kart sieciowych fizycznego serwera, do których będzie połączony wirtualny przełącznik. Dodatkowo musi istnieć możliwość „load balancingu" pomiędzy kartami sieciowymi co najmniej w oparciu o: IP hash, MAC hash, port fizyczny ruchu przychodzącego. Musi być także możliwość ustawienia kart sieciowych w trybie Active-Standby. 35. System musi posiadać funkcje zarządzania co najmniej dla 1000 predefiniowanych modeli urządzeń. Oprócz tego musi być możliwość wgrania dowolnej bazy MIB dla urządzeń sieciowych nie obsługiwanych domyślnie przez System 36. System musi posiadać funkcję automatycznej aktualizacji przez Internet. 37. System musi posiadać funkcje implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów. 38. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled) 39. System musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy 40. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych
Kompatybilność	Na liście kompatybilności systemu zarządzania znajdować się muszą co najmniej: • przełączniki dostępowe TYP1, TYP 2 • przełączniki HP Procurve 2510 będące w posiadaniu Zamawiającego • Aruba AP-207 będące w posiadaniu Zamawiającego • HPE Proliant XL190r gen10 będące w posiadaniu Zamawiającego • HP Proliant ML350G6 będące w posiadaniu Zamawiającego • HP Proliant ML150G5 będące w posiadaniu Zamawiającego
Gwarancja	Minimum 60-cio miesięczna gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

1.6.6 Firewall/UTM TYP1 (1kpl.)

Zapora sieciowa typu Next Generation Firewall/UTM.
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
W ramach postępowania system powinien zostać dostarczony w postaci klastra HA (min. dwa urządzenia).

Parametry minimalne pojedynczego urządzenia:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Podstawowe funkcjonalności	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q
Wyposażenie	System realizujący funkcję Firewall powinien dysponować: - minimum 21 portami Ethernet 10/100/1000 Base-TX - minimum 8 portami SFP 10/100/1000 Base-X (z czego maksymalnie 4 mogą być współdzielone z portami 1G 10/100/1000 Base-TX) - minimum 2 porty SFP+ - dedykowane porty 1G do łączenia urządzeń w HA - minimum 2 porty 1G dedykowane dla łączy WAN - minimum 1 port konsolowy (RS-232 w postaci złącza USB lub RJ-45) -minimum dwa redundantne zasilacze
Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 55 tys. nowych połączeń na sekundę Przepustowość Firewall'a: nie mniej niż 19 Gbps. dla pakietów 1518 Bajtów oraz min. 17.5 Gbps dla pakietów 512 Bajtów Wydajność szyfrowania VPN IPSec: nie mniej niż 11.4 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1,55 Gbps. Wydajność skanowania ruchu z włączonymi funkcjami: Firewall, IPS, AC - minimum 780 Mbps. Wydajność skanowania ruchu z włączonymi funkcjami: Firewall, IPS, AC, Malware Protection - minimum 680 Mbps.

Logowanie i korelacja zdarzeń	System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze. System powinien mieć możliwość logowania do dedykowanego, centralnego systemu logowania producenta. System dedykowanego centralnego systemu logowania powinien posiadać parametry nie gorsze niż: <u>Wymagania Ogólne Centralnego Systemu Logowania</u> Centralny system logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Dostarczany system musi być w pełni kompatybilny z będącymi w posiadaniu Zamawiającego urządzeniami Fortinet Fortigate 30E. Rozwiązanie w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM. <u>Interfejsy, Dysk:</u> 1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB. <u>Parametry wydajnościowe:</u> a) System musi być w stanie przyjmować minimum 1 GB logów na dzień. b) Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. c) Możliwość zwiększenia ilość przyjmowanych logów do min. 1.5TB na dzień (przez zakup odpowiedniej licencji lub modułu) <u>Logowanie:</u> a) Podgląd logowanych zdarzeń w czasie rzeczywistym. b) Możliwość przeglądania logów historycznych z funkcją filtrowania. c) System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: • Listę najczęściej wykrywanych ataków. • Listę najbardziej aktywnych użytkowników. • Listę najczęściej wykorzystywanych aplikacji. • Listę najczęściej odwiedzanych stron www. • Listę krajów , do których nawiązywane są połączenia. • Listę najczęściej wykorzystywanych polityk Firewall. • Informacje o realizowanych połączeniach IPSec. d) Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. e) Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. f) System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. <u>Raportowanie</u> W zakresie raportowania system musi zapewniać: a) Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. b) Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. c) Funkcję definiowania własnych raportów. d) Możliwość spolszczenia raportów.

	e) Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. <u>Korelacja logów</u> W zakresie korelacji zdarzeń system musi zapewniać: a) Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. b) Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. c) Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. <u>Zarządzanie</u> a) System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. b) Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. c) System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. <u>Opisy do wymagań ogólnych</u> a) 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. Dostawa wyżej opisanego systemu centralnego logowania nie jest częścią niniejszego postępowania.
Kontrola Malware	System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.

Funkcje UTM/NGF	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection b) Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN d) Ochrona przed atakami - Intrusion Prevention System e) Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM f) Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP g) Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma h) Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) i) Możliwość analizy ruchu szyfrowanego protokołem SSL j) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
IPSec VPN	W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: a) Tworzenie połączeń w topologii Site-to-site oraz Client-to-site b) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności c) Praca w topologii Hub and Spoke oraz Mesh d) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF e) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
Klient VPN	W ramach funkcji IPSec VPN, SSL VPN – producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
Routing i NAT	Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Translacja adresów NAT adresu źródłowego i docelowego.
Oddzielne instancje	Możliwość budowy minimum 8 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
Firewall	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
Antyvirus	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
IPS	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
Application Control	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

Filtr treści WWW	Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
Filtr URL	Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
Obsługa użytkowników i integracja z zewnętrznymi bazami danych	System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych d) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub EAL4 dla funkcji Firewall • ICSA lub NSS Labs dla funkcji IPS • ICSA dla funkcji: SSL VPN, IPSec VPN
Zarządzanie	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Support i gwarancja	Serwisy i licencje: W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do bezpłatnego pobierania aktualizacji baz zabezpieczeń przez okres 60 miesięcy. Gwarancja na sprzęt min. 60miesięcy NBD
ISO	Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący urządzenie powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Oferent powinien przedłożyć: a) oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej b) oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej) c) certyfikat ISO 9001 podmiotu serwisującego.
Inne	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.

1.6.7 Firewall/UTM TYP2 (4szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wymagania podstawowe	1. Firewall/UTM posiadający min. 4 portów 10/100/1000Base-T RJ-45 2. 1 dedykowany porty WAN 10/100/1000Base-T RJ-45 3. Min. 1 port USB 4. Obudowa typu desktop 5. Możliwość instalacji w szafie 19” 6. Obsługa min. 600 tys. sesji (min. 28 tys. nowych sesji na sekundę) 7. Firewall o przepustowości min. 4.5Gbit/s dla pakietów 1518 byte 8. Wbudowana serwer VPN: IPSec oraz SSL - przepustowość dla IPSec VPN min. 4Gbit/s - przepustowość dla SSL VPN min. 400 Mbit/s 9. Wbudowany system antywirusowy 10. Wbudowany system IPS o przepustowości min. 950 Mbit/s 11. Wbudowany system Application Control o przepustowości min. 900Mbit/s 12. Wydajność przy włączonych równocześnie funkcjonalnościach Firewall, AppControl, IPS min.: 700Mbit/s 13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094 14. Opóźnienie nie większe niż 5µs 15. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) 16. Wbudowany DHCP Serwer i klient 17. Wbudowany kontroler WiFi nie wymagający dokupywania dodatkowej licencji 18. obsługa min. 5 AccessPointów
Obsługa Routingu IPv4	1. Routing dla protokołu IPv4 w sprzęcie 2. Obsługa RIP v1/v2 3. Obsługa OSPF
Obsługa IPv6	1. Routing dla protokołu IPv6 w sprzęcie 2. Telnet Server dla IPv6 3. SSH2 Server dla IPv6 4. Ping dla IPv6 5. Tracert dla IPv6
Bezpieczeństwo sieciowe	1. Obsługa redundancji routingu VRRP (RFC 2338)
Zarządzanie	1. Zarządzanie przez SNMP v1/v2/v3 2. Zarządzanie przez przeglądarkę WWW – protokół http i https 3. Możliwość wyświetlenia odświeżanych „na żywo”: sesji, użytkowników, obciążenia łącz, przepustowości per użytkownik/Adres IP 4. Możliwość tworzenie własnych formatek błędów/komunikatów wyświetlanych użytkownikom (np. przerwanie połączenia z powodu wirusa) 5. Możliwość włączenia wymagania logowania do sieci 6. Możliwość integracji z MS ActiveDirectory co najmniej w zakresie logowania do SSL VPN, logowania do sieci, identyfikowania użytkowników korzystających z sieci z wykorzystaniem kont użytkowników zawartych w AD 7. Możliwość ograniczenie przepustowości w oparciu o rodzaj aplikacji (urządzenie powinno posiadać listę aplikacji do wyboru) 8. Telnet Serwer dla IPv4 / IPv6 9. SSH2 Serwer dla IPv4 / IPv6 10. Ping dla IPv4 / IPv6 11. Traceroute dla IPv4 / IPv6 12. Obsługa zewnętrznego systemu logowania SYSLOG 13. Obsługa systemu synchronizacji czasu SNTP v4 (RFC 2030) 14. Możliwość instalacji min. 2 wersji oprogramowania 15. Możliwość przechowywania min. kilkunastu wersji konfiguracji na urządzeniu

	16. Obsługa Secure Shell (SSHv2) klient i serwer
Inne	1. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze. 2. System powinien mieć możliwość logowania do dedykowanego, centralnego systemu logowania producenta 3. System powinien mieć możliwość centralnego zarządzania przez dedykowane oprogramowanie producenta. Oprogramowanie musi wspierać UTM TYP1 oraz UTM TYP2 oraz będący w posiadaniu Zamawiającego UTM Fortigate 30E. Wszystkie wymienione urządzenia muszą być wymienione na liście kompatybilności producenta oprogramowania (dostawa oprogramowania nie jest wymagana w tym postępowaniu)
Gwarancja	1. Gwarancja na sprzęt min. 60 miesięcy

1.6.8 Konfiguracja i wdrożenie

Dostarczone urządzenia (Przełączniki Ethernet oraz Firewall TYP1) należy zainstalować w lokalizacji wskazanej przez Zamawiającego.

Do każdego z przełączników szkieletowych należy podłączyć dostarczone serwery. Połączenia należy wykonać za pomocą PatchCordów światłowodowych SM LC-LC nie dłuższych niż 2m. Każdy serwer musi zostać podłączony dwoma łączami 25G do przełącznika w sposób zapewniający bezawaryjną pracę w przypadku awarii jednego z przełączników szkieletowych.

Połączenie między przełącznikami szkieletowymi należy wykonać za pomocą portów QSFP28 100G.
Do tego celu należy wykorzystać kable DAC 100G.
Połączenie między przełącznikami dostępowymi a przełącznikami szkieletowymi należy wykonać za pomocą portów światłowodowych 10G w sposób zapewniający bezawaryjną pracę w przypadku awarii jednego z przełączników szkieletowych.

Na przełącznikach szkieletowych należy skonfigurować:
- Adresy IP do zarządzania
- Tryb HA (stack)
- VLANy
- połączenie z siecią Zamawiającego
- SpanningTree – musi zostać WYŁĄCZONE na wszystkich portach
- zachowanie urządzenia w przypadku awarii któregoś z przełączników szkieletowych – bezprzerwowe przełączanie

Na wszystkich **przełącznikach dostępowych (TYP 1, TYP 2)** należy skonfigurować autoryzację do sieci na wszystkich portach (poza uplinkami). Autoryzacja musi odbywać się po adresach MAC, których baza powinna pobierana być z serwera radius, którego instalacja leży po stronie Wykonawcy. Do bazy adresów MAC należy dodać wszystkie dostarczane urządzenia (komputery, drukarki, telefony IP)

Firewall TYP1:
Dostawca zobowiązany jest do wykonania migracji konfiguracji z istniejących u Zamawiającego urządzeń Fortinet Fortigate 30E.
W związku z specyfiką pracy Zamawiającego prace mogą być wykonywane tylko w weekendy w godzinach ustalonych z Zamawiającym co najmniej na dwa dni przed planowanymi pracami.
Dostawca rozwiązania w szczególności powinien:
- przenieść konfigurację tuneli VPN IPSec

- przenieść konfigurację interfejsów fizycznych, VLANów interfejsów IP
- przenieść konfigurację SSL VPN (wraz z ustawieniami webportali)
- przenieść konfiguracje kont użytkowników SSL VPN
- przenieść konfigurację administratorów urządzenia
- przenieść konfigurację polityk bezpieczeństwa (w tym profile AV, AC, IPS, DLP, Webfiltering)
- przenieść konfigurację routingu
- przenieść konfigurację DHCP
- przenieść konfigurację trybu HA

W przypadku braku możliwości przeniesienia konfiguracji 1:1 wykonawca ma obowiązek odpowiednio zmodyfikować konfigurację, aby osiągnięte funkcjonalności i zasady bezpieczeństwa były zbieżne z urządzeniem źródłowym.

Przełączenie pracy sieci na nowe urządzenia nastąpi po uzgodnieniu terminu z Zamawiającym.

Urządzenia Fortigate 30E będące w posiadaniu Zamawiającego należy przywrócić do ustawień fabrycznych a następnie skonfigurować obsługi połączeń IPSec VPN. Skonfigurować należy co najmniej:
- logowanie co centralnego systemu logowania
- interfejsy fizyczne, VLANy, interfejsy IP
- serwery DHCP
- profile bezpieczeństwa (AV, AC, IPS, DLP, Webfiltering)
- polityki bezpieczeństwa wraz z przyporządkowaniem do nich profili bezpieczeństwa
- tunel IPSec VPN z Firewallem TYP1 zainstalowanym w serwerowni przy ul. Koszykowej

Zamawiający dostarczy informacje niezbędne do konfiguracji (hasła, adres IP itp.)

Firewalle TYP2 należy zainstalować we wszystkich lokalizacjach Zamawiającego: ul. Dzielna, ul. Brzeska, Otwock, Zagórze – po jednym urządzeniu w każdej lokalizacji.
Urządzenia należy skonfigurować obsługi połączeń IPSec VPN. Skonfigurować należy co najmniej:
- logowanie co centralnego systemu logowania
- interfejsy fizyczne, VLANy, interfejsy IP
- serwery DHCP
- profile bezpieczeństwa (AV, AC, IPS, DLP, Webfiltering)
- polityki bezpieczeństwa wraz z przyporządkowaniem do nich profili bezpieczeństwa
- tunel IPSec VPN z Firewallem TYP1 zainstalowanym w serwerowni przy ul. Koszykowej

Urządzenia dostępowe do sieci bezprzewodowej należy zainstalować w miejscach wskazanych przez Zamawiającego. Odpowiednie okablowanie zostanie zapewnione przez Zamawiającego.
Urządzenia należy skonfigurować w sposób zapewniające bezawaryjną pracę (klaster HA).
Na wirtualnym kontrolerze należy skonfigurować przede wszystkim:
- Adres IP dla wszystkich AccessPointów
- hasło administratora
- SSID (min. 3 wskazane przez Zamawiającego)
- autoryzacja do SSID w tym dla gości umożliwiająca jednoznaczną identyfikację użytkownika przez wysyłanie hasła SMS – po stronie Wykonawcy jest zapewnienie odpowiedniej usługi bramki SMS na min. 60 miesięcy od daty instalacji
- konfiguracja IPS/IDS pozwalający na wykrywanie/eliminowanie obcych AccessPointów
- konfiguracja wewnętrznego firewalla w sposób pozwalający na korzystanie z usług min. DLNA, airplay, airprint

1.7 System Informacji Wewnętrznej

Zaplanowano wdrożenie systemu prezentującego informację dla Pacjentów. System powinienem w prosty i jednoznaczny sposób prezentować informacje na dużych wyświetlaczach (min. 75”) dla osób przebywający w poczekalni.

1.7.1 Oprogramowanie do zarządzania treścią (1kpl.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Funkcjonalności podstawowe	• Rozwiązanie umożliwia zarządzanie wyświetlanymi treściami multimedialnymi na połączonych w sieci wewnętrznej elektronicznych terminalach. • Rozwiązanie ma obsługiwać interakcję z użytkownikami poprzez panele dotykowe totemów. • Zarządzanie treściami multimedialnymi wyświetlanymi na totemach ma odbywać się za pomocą panelu administracyjnego dostępnego z poziomu każdego komputera działającego w sieci. • Zarządzanie musi posiadać możliwość przyznawania uprawnień administratorom do poszczególnych narzędzi panelu administracyjnego. • Zarządzanie treściami multimedialnymi musi odbywać się z dokładnością do pojedynczego totemu działającego w sieci rozwiązania. • W panelu administracyjnym system musi mieć możliwość zarządzania treściami wyświetlanymi na wygaszaczach ekranów totemów. • Ekran totemu z uruchomionym wygaszaczem musi wyświetlać jednocześnie szybkie przyciski akcji prowadzące do wybranych funkcji. • Ekran totemu musi mieć możliwość wyświetlania aktualnego czasu, daty, paska z informacjami z kanałów RSS. • Rozwiązanie musi pozwalać na zarządzanie kanałami RSS oraz innymi źródłami danych w taki sposób, aby możliwa była publikacja pochodzących z nich informacji na połączonych terminalach, a zwłaszcza: - możliwość podania adresu sieciowego źródła - możliwość wprowadzania danych umożliwiających indeksowanie i tworzenie spisów z dostarczonych danych - możliwość powiązania źródła danych z modułem wizualizującym, takim jak aktualna pogoda, zajętość sali. • System musi posiadać możliwość tworzenia i zarządzania komunikatami: podania daty komunikatu, edycji treści komunikatu, zaplanowania daty publikacji komunikatu, powiązania komunikatu z wybranym elementem, a zwłaszcza z lokalizacją lub osobą, powiązanie komunikatu z innym elementem i z możliwością umiejscowienia go na interaktywnym planie budynku i wykorzystanie funkcji nawigacji do wytyczenia trasy celu. • Na wygaszaczu ekranu musi mieć możliwość wyświetlanie treści ze źródeł zewnętrznych, a ekran musi mieć możliwość takiego podziału, że jednocześnie można na nim wyświetlać treści z różnych źródeł zewnętrznych. • Rozwiązanie ma umożliwiać podział ekranu wygaszacza tak by można było pokazywać równocześnie kilka różnych treści. • W panelu administracyjnym musi być edytor graficzny, który umożliwia projektowanie wygaszacza ekranu składającego się z tekstu, obrazów, zbiorów obrazów, slajdów kompozytowych, prezentacji oraz klipów wideo. • Rozwiązanie musi umożliwiać planowanie emisji treści na wygaszaczach totemów oraz przypisywać emisje do wybranych totemów. Musi być możliwe zmienianie kolejności emisji, ustalanie dat emisji i godzin emisji w ujęciach dziennym, tygodniowym, miesięcznym, czasu wyświetlania emisji oraz okresu wyświetlania, tworzenia grup emisji i wykonywanie działań na tych grupach tak samo jak na pojedynczych emisjach. • W panelu administracyjnym musi być moduł raportowania, który będzie prezentował agregowane dane o liczbie wyświetleń emisji, czasie emisji, wyświetlanych przez użytkowników ekranach, wyszukiwanych w rozwiązaniu informacji, wyznaczonych ścieżkach nawigacji. • W rozwiązaniu musi być możliwość kreowania komunikatów wyświetlanych użytkownikom na totemach. Komunikaty muszą mieć możliwość edytowania ich treści, wskazania dat na wyświetlanie się komunikatu, powiązania komunikatu z miejscem na interaktywnych mapach nawigacji w celu wytyczenia ścieżki nawigacji do określonego w komunikacie miejsca. • Rozwiązanie musi mieć zaimplementowaną funkcjonalność prezentowania interaktywnej struktury organizacyjnej placówki na totemach.

	• Interaktywna struktura organizacyjna musi mieć możliwość zarządzania nią z panelu administratora. • Rozwiązanie musi mieć możliwość publikowania informacji o konferencjach, zawierające min.: - agendę konferencji - możliwość powiązania konferencji z konkretnym miejscem na planie budynku • Sposób prezentowania interaktywnej struktury organizacyjnej ma być podobny do skorowidza. Użytkownik musi mieć możliwość odnalezienia określonej jednostki organizacyjnej, wyświetlenia okna modalnego z informacją na temat danej jednostki i wyznaczenie ścieżki nawigacji do jednostki organizacyjnej. • Rozwiązanie musi posiadać możliwość tworzenia interaktywnych prezentacji z użyciem edytora w panelu administracyjnym. • Edytor prezentacji interaktywnych musi zapewnić przynajmniej możliwość edycji treści slajdów, tła slajdów, położenia bloków informacyjnych na slajdach, możliwość podłączenia źródeł danych do bloków informacyjnych na slajdach, możliwość czasowej aktualizacji bloków informacyjnych z zewnętrznych źródeł danych, możliwość zdefiniowania źródła strumienia wideo dla bloku informacyjnego na slajdzie, możliwość grupowania slajdów w wizualnym edytorze prezentacji, tworzenia przejść za pomocą drzewka przejść między slajdami, możliwość umieszczania na slajdach interaktywnych przycisków akcji służących do przejść między powiązanymi slajdami oraz stanowiących odnośnik do elementów znajdujących się na interaktywnych mapach rozwiązania. • System musi posiadać możliwość dołączenia slajdów prezentacji interaktywnej do opisu pomieszczenia (rozszerzać sferę informacyjną dotyczącą pomieszczenia). • Rozwiązanie musi posiadać wyszukiwarkę ekranową umożliwiającą wprowadzenie dowolnego ciągu znaków użytkownikowi i wyświetlającą wyniki wyszukiwania spośród zindeksowanych przez wyszukiwarkę informacji o pomieszczeniach, pracownikach, z opisów w prezentacjach interaktywnych i w komunikatach. • Rozwiązanie musi mieć wbudowane skorowidze pracowników placówki oraz pomieszczeń. • Użytkownik musi mieć możliwość wyświetlenia w skorowidzu oraz w wynikach wyszukiwarki dodatkowych informacji na temat określonego obiektu oraz wyznaczenia ścieżki nawigacji, jeżeli dany obiekt posiada powiązanie z lokalizacją na interaktywnej mapie. • Rozwiązanie musi zapewnić możliwość integracji z Active Directory / LDAP dla celów autoryzacji i zarządzania uprawnieniami administratorów. • Zarządzanie uprawnieniami administratorów musi odbywać się z dokładnością do pojedynczych sekcji i narzędzi administracyjnych. • Elementem integralnym rozwiązania ma być aplikacja mobilna dla systemów Android oraz iOS, która będzie dawała dostęp do informacji umieszczanych na stronach rozwiązania, możliwość przeglądania interaktywnych map budynków, możliwość korzystania z interaktywnych funkcji map budynków, takich jak wyświetlanie informacji o pomieszczeniach i innych obiektach zlokalizowanych na mapach, a także wyznaczanie ścieżek nawigacji do miejsc docelowych obliczonych od wskazanych przez użytkownika lokalizacji, sprawdzenie aktualnej lokalizacji użytkownika przy użyciu wbudowanego skanera kodów QR, korzystanie z wyszukiwarki Rozwiązania oraz skorowidzów pomieszczeń i osób. • Oprogramowanie na totemach, aplikacja mobilna oraz panel administracyjny rozwiązania muszą posiadać obsługę w języku polskim. • Narzędzia do konfiguracji rozwiązania muszą dawać możliwość za pośrednictwem panelu administracyjnego edytowania umiejscowienia totemów, a także zarządzania wyświetlaniem poszczególnych modułów i treści z dokładnością do pojedynczego totemu.

	• W ramach panelu administracyjnego rozwiązania musi znaleźć się funkcja generatora kodów QR, która umożliwi generowanie kodów QR dla wskazanych na mapie interaktywnej lokalizacji. W ramach funkcjonalności rozwiązania wygenerowane kody QR mają być umieszczane w szablonie prezentującym kod oraz inne informacje o lokalizacji. Szablon musi umożliwiać wydruk tablicy z kodem QR w ustalonym formacie. • Rozwiązanie musi mieć możliwość odczytania kodów QR za pomocą czytników wbudowanych w totemach. Po odczytaniu kodu przy totemie rozwiązanie ma wygenerować bez dodatkowej akcji po stronie użytkownika ścieżkę nawigacji od aktualnej lokalizacji użytkownika do miejsca określonego w kodzie QR. Na ekranie z wygenerowaną ścieżką ma się znaleźć kod QR, który po odczytaniu za pomocą aplikacji mobilnej rozwiązania lub przy użyciu innego czytnika kodów QR ma wyświetlić na urządzeniu użytkownika mapy z zaznaczoną ścieżką nawigacji. • Rozwiązanie musi posiadać możliwość przyłączenia kolejnych totemów przy zachowaniu pełnej funkcjonalności bez konieczności wykonywania prac po stronie dostawcy. • Wymaga się, aby totemy rozwiązania działały poprawnie nawet w przypadku utraty połączenia z serwerem rozwiązania. • Rozwiązanie musi być w pełni gotowe do integracji z systemami zewnętrznymi, przynajmniej za pomocą: - kodów QR - interfejsów REST lub WEBservice
Funkcjonalności opcjonalne (Oprogramowanie powinno mieć możliwość rozbudowy o dodatkowe funkcje np. przez dokupienie dodatkowej licencji**)**	• Mieć wbudowaną funkcję nawigacji wewnątrzbudynkowej, która w oparciu o interaktywne mapy budynków umożliwi użytkownikom wyznaczanie ścieżek nawigacji do miejsc docelowych, takich jak pomieszczenia, miejsca, elementy ciągów komunikacyjnych, osoby oraz wszelkie inne obiekty z baz danych rozwiązania posiadających powiązanie z lokalizacją na interaktywnych mapach. • Rozwiązanie musi posiadać wbudowaną funkcjonalność tworzenia i wyświetlania interaktywnych planów budynków, pięter, pomieszczeń oraz przyległego do obiektu obszaru. • Moduł nawigacji musi mieć możliwość powiązania informacji z bazy danych z lokalizacją na interaktywnym planie budynku. • System musi mieć możliwość przypisania tagów do pomieszczeń widocznych w systemie. • Wszystkie opisy prezentowane w oknach szczegółów na temat obiektów umieszczonych na interaktywnych mapach muszą być edytowalne w panelu administracyjnym. Edytor musi umożliwiać, co najmniej edycję tekstu wyświetlanego przy opisie budynku, pomieszczeń, pięter, ciągów komunikacyjnych, punktów zainteresowań na mapie, informacji o osobach, informacji o usługach powiązanych z lokacją na mapie. Edytor opisów musi objąć takie informacje jak: nazwę, oznaczenie, położenie w budynku, powiązanie z ciągami komunikacyjnymi, umieszczenie zdjęć, a także możliwość rozszerzenia opisu o kolejne pola własne użytkownika. • Rozwiązanie musi posiadać wbudowany edytor schematów ścieżek nawigacji, który będzie umożliwiał budowanie i edycję za pomocą graficznego interfejsu powiązań między obiektami na interaktywnych mapach, wedle których będzie działał algorytm wyznaczania ścieżek nawigacji w rozwiązaniu. Edytor ma mieć możliwość wiązania węzłów schematu nawigacji z określonymi lokalizacjami na interaktywnych mapach, takimi jak pomieszczenia. • System musi posiadać możliwość czasowego zamknięcia niektórych elementów budynku. • Edytor schematu ścieżek nawigacji musi mieć możliwość łatwego umieszczania przez administratora znaczników na ciągach komunikacyjnych, informujących użytkowników o przeszkodach i ostrzeżeniach, których umieszczenie skutkuje jednocześnie dynamiczną zmianą w przeliczaniu ścieżki nawigacji w taki sposób, aby omijane były ciągi komunikacyjne w miejscach oznaczonych znacznikami. • System musi posiadać możliwość dodania ręcznego opisu pięter i legendy.

	• Funkcja nawigacji rozwiązania ma mieć wbudowany algorytm obliczający optymalną ścieżkę nawigacji każdorazowo podczas wyznaczania ścieżki przez użytkownika rozwiązania. Obliczenia mają być dokonywane w czasie rzeczywistym przy uwzględnieniu topologii budynków oraz warunków dodatkowych nadawanych w panelu administratora, takich jak znaczniki na schemacie nawigacji oraz wagi dla węzłów na schemacie nawigacji. Nie będą dopuszczone rozwiązania, które dokonują jedynie graficznej prezentacji przebiegu ścieżki bez udziału algorytmu obliczającego i nie uwzględniają zmiennych nadawanych dla procesu wyznaczania ścieżki nawigacji. • System musi posiadać możliwość czasowego przydzielenia pomieszczenia w zastępstwie innego. • Funkcja nawigacji musi umożliwiać tworzenie alternatywnych trybów nawigacji, które będą umożliwiały użytkownikom wybór trybu na przykład dla osób poruszających się na wózkach inwalidzkich. Administrator musi mieć możliwość przygotowania przy wykorzystaniu edytora schematów nawigacyjnych różnych trybów nawigacji uwzględniających warunki i ograniczenia poruszania się po budynkach placówki dla konkretnych scenariuszy. • System musi umożliwiać pacjentowi możliwość z poziomu wyskakującego okna ze szczegółami budynku do wnętrza obiektu z podziałem na piętra. • Rozwiązanie musi zapewniać widok pietra umożliwiający wybranie konkretnego pomieszczenia i uzyskanie na jego temat dodatkowego opisu i opcji umożliwiającej wybranie drogi do niego. • Edytor schematów nawigacji musi mieć opcję tymczasowego przydzielenia innej lokalizacji dla określonego celu, na przykład zmianę lokalizacji pracownika na zastępstwie. • Funkcja nawigacji musi dawać możliwość użytkownikom rozwiązania sprawdzenia swojej aktualnej pozycji na interaktywnej mapie zaimplementowanej w aplikacji mobilnej przy użyciu wbudowanego w aplikacji mobilnej skanera kodów QR i rozmieszczonych tablic z kodami QR identyfikującymi określone lokalizacje w budynku. W przypadku, gdy użytkownik wyznaczył wcześniej ścieżkę nawigacji do miejsca docelowego odczytanie jego aktualnej pozycji ma spowodować aktualizację ścieżki i wyznaczenie jej ponownie z aktualnej pozycji do wcześniej ustalonego miejsca docelowego. • Funkcja oznaczania swojej pozycji w budynku za pomocą kodów QR musi być dostępna w ramach aplikacji mobilnej Rozwiązania dla systemów Android oraz iOS, a także bez konieczności użycia dedykowanej aplikacji mobilnej rozwiązania dla systemów Android, iOS i Windows Phone. System musi posiadać możliwość wyznaczenia drogi do pomieszczenia po sczytaniu kodu QR wygenerowanego przez system lub zgodnie z wytycznymi systemu.
Gwarancja i wsparcie producenta	• Min. 5 lat z czasem reakcji NBD. Gwarancja powinna zapewniać dostęp do najnowszych wersji oprogramowania oraz pomocy technicznej producenta w trybie 8x5.

1.7.2 Monitor w obudowie odpornej na uszkodzenia (2kpl.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Matryca	● Typ matrycy – E-LED BLU ● Typ podświetlenia – LED ● Przekątna - min. 75” ● Format obrazu – 16:9 ● Rozdzielczość – min. UHD (3840x2160) ● Jasność – min. 500 cd/m^2 ● Kontrast – min. 4000:1 ● Kąt oglądalności – min. 178^o (L/P) ● Czas reakcji matrycy – max. 8ms
Złącza	● Wejścia Video: min. DP 1.2, DVI-I, 2 x HDMI 2.0 ● Wyjścia Video: min. 1 x HDMI 2.0 ● Wejścia Audio: 3,5mm Mini Jack, ● Wyjścia Audio: 3,5 mm Mini Jack ● Złącza sterujące: RS-232 (In/Out), RJ-45, 2 x USB
Wymiary i waga	● Wymiary max.: 168.5 x 96.1 x 5 cm ● Waga max.: 38,5 kg
Funkcjonalności	● Wbudowane w każdy monitor oprogramowanie oraz player umożliwia jące wyświetlanie treści oraz tworzenie harmonogramów wyświetlania bez konieczności stosowania dodatkowych urządzeń. ● Minimalna wielkość pamięci wewnętrznej dostępnej w każdym z moni torów – 4GB, minimalne wymagania co do wbudowanej platformy: Pro cesor min. Quad Core 1.6 GHz, pamięć RAM min. 2.5 GB LPDDDR-4, ● silnik wspierający odtwarzanie plików H263, H.264/AVC, MPEG-1/2/4, AVS+, HEVC, JPEG, PNG, VP8, VP9 Audio. ● Możliwość zarządzania zdalnego (przez RJ45 lub RS-232) pracą wszystk ich monitorów w ścianie video (włącz/wyłącz, wybór źródła, kontrola t emperatury, regulowanie głośności itp.) bez konieczności dokonywani a zakupu specjalnego oprogramowania przez użytkownika. ● Możliwość szybkiego sklonowania ustawień monitorów poprzez pamię ć USB w przypadku awarii sieci LAN. ● Elektronika urządzenia zabezpieczona przed działaniem warunków zew nętrznych ● Wbudowany moduł WiFi
Zasilanie	● Zużycie energii: max. 231 W/h, nie więcej niż 0.5W w trybie Stand By
Obudowa	● Monitor powinien posiadać obudowę zabezpieczającą wyświetlacza i f abryczną obudowę monitora przed uszkodzeniami w tym uderzanie cię żkimi przedmiotami, zachlapaniem różnego rodzaju substancjami (np. krwią) . Obudowa musi pozwalać na łatwe czyszczenie i powinna być odporna na działanie środków myjących (również zawierających spirytus) ● Mocowanie VESA
Akcesoria	● Wieszak ścienny pozwalający na montaż monitora na ścianie
Gwarancja	● Producenta, min. 3 lata

1.7.3 Instalacja i uruchomienie

Wykonawca zobowiązany jest do instalacji monitorów we wskazanych przez Zamawiającego miejscach. Odpowiednie okablowanie zostanie zapewnione przez Zamawiającego.
Monitory należy skonfigurować do współpracy z dostarczanym Systemem Zarządzania Treścią.
Wykonawca zobowiązany jest zainstalować oprogramowanie do Zarządzania Treścią w środowisku wirtualnym Zamawiającego. Oprogramowanie należy skonfigurować zgodnie z wytycznymi Zamawiającego (w tym wygląd wyświetlanych na monitorach treści).
Wykonawca przeprowadzi minimum 4-ro godzinne szkolenie z obsługi Systemy Informacji Wewnętrznej (monitorów i oprogramowania do zarządzania treścią).

1.8 System Backup

1.8.1 Oprogramowanie Backup (1kpl.)

Wymagane minimalne parametry techniczne
Licencje muszą umożliwiać backup maszyn wirtualnych na serwerach fizycznych o łącznej liczbie 8 procesorów fizycznych. Licencja przeznaczona dla wykorzystywanego przez Wykonawcę środowiska wirtualizacji. Licencja musi pozwalać na późniejszą rozbudowę do min. 16 procesorów. Wszystkie licencje powinny być dostarczone wraz z 5-letnim wsparciem, świadczonym przez producenta oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 8h na dobę.
• Oprogramowanie powinno współpracować z instrastrukturą VMware vSphere oraz Microsoft Hyper-V • Oprogramowanie powinno zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V • System i konsola zarządzająca oprogramowania musi wspierać instalację na systemach z rodziny Windows oraz Linux oraz musi wspierać procesory CPU klasy x86-64 oraz ARM
• Oprogramowanie powinno być licencjonowanie w modelu “per-CPU”. • Oprogramowanie powinno być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie powinno być “samowystarczalne”, odzyskiwanie musi pozwalać na dostęp do metadanych • Oprogramowanie powinno mieć mechanizmy deduplikacji i kompresji całego repozytorium backupu, w celu zmniejszenia wielkości archiwów • Oprogramowanie nie może wymagać żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej • Oprogramowanie powinno zapewniać mechanizmy informowania poprzez email • Oprogramowanie powinno mieć możliwość uruchamiania skryptów w ramach zadań • Oprogramowanie powinno mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie powinno mieć wbudowane mechanizmy szyfrowania
• Oprogramowanie powinno używać mechanizmów Change Block Tracking • Oprogramowanie powinno oferować podobne rozwiązanie jak CBT również dla platformy Hyper-V • Oprogramowanie powinno wspierać kopiowanie backupów na taśmy • Oprogramowanie powinno mieć możliwość kopiowania backupów zarówno w trybie manualnym jak i automatycznym (zgodnym z harmonogramem) • Oprogramowanie powinno mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie powinno mieć możliwość replikacji wirtualnych maszyn pomiędzy lokalizacjami (Funkcjonalność ta powinna być zapewniona dla vSphere i Hyper-V)
• Oprogramowanie powinno umożliwić uruchomienie maszyny wirtualnej bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, bez potrzeby kopiowania jej na storage produkcyjny. • Oprogramowanie powinno umożliwiać pełne odtworzenie wirtualnej maszyny • Oprogramowanie powinno wspierać odtwarzanie plików z następujących systemów plików: ext3, ext4, XFS, NTFS, FAT32 • Oprogramowanie powinno umożliwiać szybkie granularne odtwarzanie obiektów aplikacji takich jak Active Directory, Microsoft Exchange, Microsoft SQL, bez wymogu pełnego odtworzenia wirtualnej maszyny. • Oprogramowanie powinno używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows • Oprogramowanie powinno mieć możliwość tworzenia łańcucha zdarzeń procedur backup

1.8.2 Macierz do składowania kopii zapasowych (2szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokości maksymalnie 4U.
Procesor	Procesor klasy x86, min.4-rdzeniowy, taktowany zegarem co najmniej 3,2GHz lub równoważny, osiągający w teście PassMark CPU Mark min. 6000 Pkt według wyników testu z dnia 30.06.2020r.
Przestrzeń dyskowa	Min. 36 zatok na dyski Hot-Swap 3.5" w jednej obudowie Macierz musi udostępniać minimum 300 TB przestrzeni użytkowej z zabezpieczeniem na poziomie RAID6 zbudowanej w oparciu o minimum 28 dysków SATA/600, 5800RPM, 64MB Cache. Wymagane dyski muszą być zainstalowane w jednej obudowie.
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę do co najmniej 130 dysków 3.5 calowych (np. przez podłączenie dodatkowych półek)
Obsługa dysków	Macierz musi obsługiwać dyski SAS/SATA SSD i HDD. Macierz musi umożliwiać mieszanie napędów dyskowych SSD i HDD w obrębie pojedynczej półki dyskowej.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy JBOD, RAID 0, 1, 5, 6, 10, 50, 60
Pamięć	Min. 16 GB RAM (z możliwością rozbudowy do min. 64GB) Min. 240MB pamięci flash
Interfejsy sieciowe	Min. 3 porty 1G RJ45, min. 2 porty 10G SFP+
Zarządzanie	- Interfejs co najmniej w języku polskim - WEB (http/https) - SSH, Telnet - Możliwość zarządzania z chmury - dedykowana aplikacja dla Windows do wykrywania macierzy - dedykowana aplikacja dla systemów Android oraz iOS
Porty	Min. 2 porty USB 3.0, min. 2 porty eSATA
Zasilanie	Możliwość instalacji min. dwóch zasilaczy o mocy maks. 700W każdy. Zainstalowany min. 2 zasilacze
Ochrona danych	Szyfrowanie AES256, zdalna szyfrowana replikacja, kompresja danych, global Hot-Spare, wbudowany skaner antywirusowy, LUN Snapshot
Udostępniania plików	Udostępniania plików dla: Windows, Mac, Linux/UNIX - CIFS/SMB, AFP, FTP/FTPS (min, 8000 użytkowników, min. 8000 grup, min. 1000 udostępnionych folderów) - iSCSI (min. 200 LUN, min. 200 Target) - NFS - HTTP/HTTPS -WebDAV Wsparcie dla Windows ACL
Wbudowane usługi	Serwer FTP, Serwer DLNA, Serwer Kamer, AppleTimeMachine, WEB (WebDAV, HTTP/HTTPS), Serwer iTunes,
Usługi chmurowe	Wsparcie dla Amazon AWS, Google Drive, Dropbox
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.
Wymiary i waga	- maks. 930mm x 445mm x 180mm (DxSxG), - maks. 35Kg
Wyposażenie	- szyny do montażu w szafie Rack - min. 2 wkładki światłowodowe SFP+ 10GBase-LR w pełni kompatybilne z dostarczanym urządzeniem - min. 2 patchcordy LC-LC SingleMode o długości min. 3m.
Gwarancja	3-letnia gwarancja producenta NBD. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

1.8.3 Instalacja i uruchomienie

1.8.3.1 Macierze do składowania kopii zapasowych

W szafach RACK wskazanej przez Zamawiającego należy zainstalować dostarczone macierze.
Urządzenia należy w odpowiedni sposób połączyć i okablować.
Okablowanie powinno zostać umieszczone w odpowiednich uchwytach do okablowania oraz w szczotkach kablowych.
Ilość akcesoriów musi być dostosowana do potrzeb.
Okablowanie musi zostać opisane/oznaczone po każdej stronie. Każda końcówka kabla powinna zostać wyposażona w opis, który powinien zawierać nazwę urządzenia oraz port, do którego przewód jest podłączony po przeciwnej stronie.
Wymaganie to dotyczy zarówno kabli służących do transmisji danych jak i do kabli zasilających.
Dyski należy skonfigurować w RAID5.
Zainstalowany oprogramowanie należy skonfigurować zgodnie ze wskazaniami Zamawiającego.

1.8.3.2 Oprogramowanie Backup

Oprogramowanie do backup należy zainstalować w środowisku wirtualnym Zamawiającego.
Jeżeli oprogramowanie wymaga licencji na system Windows Server 2019, Zamawiający udostępni takową.

Oprogramowanie Backup należy zintegrować z posiadanym przez Zamawiającego środowiskiem wirtualnym.
Oprogramowanie należy skonfigurować, aby wykonywało Backup zgodny z harmonogramem tj.:
- kopia przyrostowa co 24 godzin
- kopia pełna co 7 dni

1.9 Oprogramowanie do zarządzania zgłoszeniami (1 kpl.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Ogólne wymagania funkcjonalne	• System powinien posiadać obligatoryjnie interfejs Użytkownika w języku polskim. • Podczas rejestracji zgłoszenia przez Konsultanta SD, wypełnienie formularza danymi podstawowymi jak „Odbiorca Usługi” (dalej: Odbiorca), formularz zostanie automatycznie uzupełniony o dane dodatkowe: - umowa SLA, której Odbiorca podlega - lokalizacja Odbiorcy - miejsce Odbiorcy w strukturze organizacyjnej - dane kontaktowe: telefon komórkowy, telefon stacjonarny, adres email, według zdefiniowanych relacji. • Podczas wyszukiwania informacji z repozytoriów danych: ▪ System wyświetli formularz, który umożliwi użytkownikowi wprowadzenie danych, które posłużą do automatycznej konstrukcji zapytania wysyłanego do bazy Systemu. ▪ Na przykład: po wpisaniu do pola „Status” wartości „Powiązane” na formularzu wyszukiwania Zgłoszeń i wybraniu opcji „Wyszukaj”, System zwróci listę wszystkich Zgłoszeń o statusie „Powiązane”. ▪ System będzie umożliwiał dokonywanie zmian dostępnego zakresu informacji (pól) możliwych do wykorzystania na formularzach podczas wyszukiwania informacji.

<table>
<tr><td></td><td>

Wpisanie w pole formularza początkowych znaków spowoduje skonstruowanie zapytania, w znaczeniu „zaczynające się od”.
Na przykład: po wpisaniu do pola „Nazwisko” wartości „A” na formularzu wyszukiwania Użytkowników i wybraniu opcji „Wyszukaj”, System zwróci listę wszystkich Użytkowników, których nazwiska zaczynają się od litery „A”.

System będzie umożliwiał dodawanie nowych pól do tabel dla repozytoriów danych o typach:

<table>
<tr><th>Typ danych</th><th>Opis</th></tr>
<tr><td>Tekstowe</td><td>Pole umożliwiające wprowadzanie i przechowywanie ciągu dowolnych znaków alfanumerycznych</td></tr>
<tr><td>Numeryczne</td><td>Pole umożliwiające wprowadzanie i przechowywanie całkowitych wartości liczbowych</td></tr>
<tr><td>Daty</td><td>Pole umożliwiające wprowadzanie i przechowywanie wartości określających daty i czasy</td></tr>
<tr><td>Wielo-wierszowe</td><td>Pole umożliwiające wprowadzanie i przechowywanie wielu wierszy ciągu dowolnych znaków alfanumerycznych</td></tr>
<tr><td>Logiczne</td><td>Pole umożliwiające wprowadzanie i przechowywanie wartości prawda / fałsz</td></tr>
</table>
</td></tr>
<tr><td>Help Desk</td><td>

System musi umożliwiać ręczną rejestrację zarówno prostych, szybkich do rozwiązania zgłoszeń jak i złożonych problemów opisujących rozległe awarie infrastruktury.
System musi umożliwiać rejestrację zgłoszenia przez użytkownika końcowego z wykorzystaniem interfejsu www (który powinien automatycznie generować zapis Incydentu) poprzez tzw. Panel Klienta.

System powinien generować zgłoszenia z sieci – automatyczne wysyłanie zgłoszeń do HelpDesk w przypadku wystąpienia awarii urządzeń w sieci komputerowej (możliwość).
System musi udostępniać elastyczny mechanizm notyfikacji pozwalający definiować reguły powiadomień przypisanych operatorów w zależności od parametrów zgłoszenia.
System musi uwzględniać pola obligatoryjne zgłoszenia: data i godzina Zgłoszenia, unikalny identyfikator Zgłoszenia (generowany automatycznie),
System powinien umożliwiać definiowanie pól wypełnianych automatycznie: priorytet Zgłoszenia, data rejestracji Zgłoszenia, data przekazania Zgłoszenia do odpowiedniej Grupy Wsparcia, data realizacji, data zamknięcia, kontrolę zadeklarowanych parametrów realizacji.

System musi mieć możliwość zdefiniowania wewnętrznych alarmów informujących o sytuacjach takich jak:
- zbliżający się termin rozwiązania;
- brak aktywności w kontekście wskazanych zgłoszeń.
System musi umożliwiać operatorom tworzenie parametryzowanych kolejek zgłoszeń oraz dawać dostęp do kolejek zdefiniowanych przez administratorów.
System powinien posiadać wewnętrzny mechanizm wysyłania wiadomości pomiędzy operatorami.
System musi umożliwiać zgłaszającemu śledzenie postępu prac nad jego zgłoszeniami poprzez interfejs WWW.

</td></tr>
</table>

	• System musi posiadać Bazę Wiedzy z możliwością indeksowania przy użyciu słów klucz, dwupoziomowa baza wiedzy z oddzielnym dostępem dla serwisantów i klientów, grupowanie rozwiązań wg tematów i podtematów. • Narzędzie powinno posiadać widok „moje zadania" do tworzenia zadań dla serwisantów, ułatwiających zespołowi realizację. • Komunikacja z użytkownikiem powinna odbywać się poprzez automatyczne przesyłanie odpowiedzi do użytkownika o przyjęciu zgłoszenia, jego zamknięciu lub innych zmianach procesu realizacji zgłoszenia. • System powinien zapewniać automatyczne przekazywanie spraw, tj. automatyczne przekazywanie zgłoszeń serwisantów, na podstawie ich typu. • System powinien zapewniać możliwość zmiany przypisanego do zgłoszenia Elementu Konfiguracji lub dodanie nowego Elementu Konfiguracji w czasie obsługi zgłoszenia. • System powinien zapewniać możliwość sprawnego zarządzania kalendarzem z uwzględnieniem dni świadczenia usługi dla każdej usługi zgodnie z deklarowanym czasami ich wsparcia, planowanych przerw w działaniu infrastruktury, harmonogram wszystkich Zmian, ukazaniu zależności i wzajemnego wpływu planowanych i realizowanych czynności, uławiającym koordynację wszelkich aktywności w ramach codziennej pracy pracowników HelpDesk.
Zarządzanie konfiguracją	• System musi umożliwiać przechowywanie informacji o nieograniczonej liczbie Elementów Konfiguracji w centralnym repozytorium. • Każdy z typów Elementów Konfiguracji musi mieć własną listę atrybutów opisujących dany element. Pola w rekordzie powinny być specyficzne dla danego typu Elementu Konfiguracji. • System musi umożliwiać śledzenie cyklu życia Elementów Konfiguracji od momentu zamówienia do wycofania z użycia. Dodatkowo musi istnieć dostęp do pełnej historii cyklu życia danego Elementu Konfiguracji (kiedy i kto zmieniał status Elementu Konfiguracji). • Baza CMDB musi posiadać typowe klasy odpowiadające typowym elementom konfiguracji występującym w infrastrukturze informatycznej. Do typowych elementów konfiguracji zaliczamy: serwer, notebook, komputer PC, monitor, switch, router, drukarka. • System powinien umożliwiać zasilanie repozytorium Elementów Konfiguracji ze źródeł zewnętrznych. • System powinien dawać możliwość powiązania Elementów Konfiguracji z Incydentami oraz Poziomami Usług. • Narzędzie powinno prezentować listę wszystkich zmian dotyczących Elementu Konfiguracji. • Dane o Elementach Konfiguracji muszą być dostępne dla Zgłoszeń, Incydentów, Problemów i Wniosków o Zmiany w trybie on-line. • System powinien umożliwiać propagowanie awarii Elementów Konfiguracji i ewentualnych przestojów związanych z tą awarią na powiązane z tym Elementem Konfiguracji inne Elementy. • System powinien umożliwić tworzenia relacji jeden-jeden, jeden-wielu, wiele-wielu na kilku poziomach pomiędzy Elementami Konfiguracji. Poprzez relację rozumiemy: ▪ Element Konfiguracji jest komponentem innego Elementu Konfiguracji; ▪ Element Konfiguracji wpływa na inny Element Konfiguracji; ▪ Element Konfiguracji należy do innego Elementu Konfiguracji; ▪ Element Konfiguracji zależy od innego Elementu Konfiguracji

Zarządzanie poziomem usług	• System musi umożliwiać stworzenie centralnego repozytorium umów SLA wraz z opisem metryk w nich zawartych. • System powinien umożliwić dodawanie, modyfikację i usuwanie umów: - umowa z odbiorcą usług IT (Umowa SLA); • System powinien wspierać priorytetyzację rozwiązywania problemów w celu zapewnienia realizacji poziomu parametrów zapisanych w umowach SLA. • Powinna istnieć możliwość uporządkowania kolejek czynności do realizacji na podstawie priorytetu SLA. • System powinien umożliwiać powiadamianie o naruszeniu zdefiniowanego poziomu usługi w momencie wystąpienia naruszenia. • Proponowane rozwiązanie powinno umożliwiać utrzymywanie centralnego katalogu umów SLA wraz z informacjami opisującymi parametry poszczególnych umów. • System musi monitorować poziom spełnienia warunków określonych w umowach SLA. • System powinien umożliwić tworzenie reguł umów SLA dla użytkowników, departamentów, priorytetów lub kategorii i kontrolę ich przestrzegania. • System musi umożliwiać tworzenie dowolnej liczby kalendarzy czasu pracy np.: - pn-pt od 8:00 do 17:00; - pn-so 8:00 – 20:00; - 24 x 7; - inne dowolne godziny pracy w tygodniu. • System musi umożliwiać tworzenie wyjątków w kalendarzach pracy w postaci definiowania świąt i dni wolnych od pracy samodzielnie przez Administratora Systemu. • System powinien umożliwić zdefiniowanie miernika na bazie dowolnych kryteriów, jakie ma spełniać monitorowany obiekt (w zakresie danych dostępnych dla tego obiektu). • System musi posiadać funkcjonalność prezentującą wybrane lub wszystkie parametry definiujące Usługę IT użytkownikom końcowym.
Raportowanie	• System musi udostępniać możliwość samodzielnego budowania raportów w oparciu o bieżące potrzeby Zamawiającego. • Narzędzie musi udostępniać graficzne narzędzie do projektowania raportów. • System musi posiadać możliwości definiowania prostych raportów ad-hoc przez użytkowników końcowych z możliwością ich zapisania do kolejnego użycia. Raportowanie ad-hoc powinno umożliwiać wybór danych tworzących kolumny raportu, kolumny do grupowania i sortowania. • System musi posiadać wbudowaną funkcjonalność graficznego prezentowania wybranych metryk. Uprawnieni użytkownicy powinni mieć możliwość definiowania własnych metryk. • Narzędzie musi mieć możliwość definiowania graficznej reprezentacji zestawu danych. • Narzędzie powinno umożliwiać definiowanie uprawnień do raportów.

Rodzaje raportów	● Funkcja HelpDesk: ▪ Liczba i historia zgłoszeń (całkowita, o danym statusie, podjęte przez poszczególnych pracowników, w podziale na medium, za pomocą którego dokonano zgłoszenie); ▪ Liczba i historia zgłoszeń rozwiązanych w zdefiniowanych w Umowach SLA, OLA, UC parametrach (z prezentacją poszczególnych progów kontrolnych, w zadanym okresie, rozwiązane, zamknięte, w podziale na osoby rozwiązujące zgłoszenie z prezentacją czasu rozwiązania, w podziale na osoby rejestrujące zgłoszenie z prezentacją czasu reakcji); ▪ Liczba i historia zgłoszeń o przekroczonych parametrach zdefiniowanych w Umowach SLA (z prezentacją poszczególnych progów kontrolnych, w zadanym okresie, rozwiązane, zamknięte, w podziale na osoby rozwiązujące zgłoszenie z prezentacją czasu rozwiązania, w podziale na osoby rejestrujące zgłoszenie z prezentacją czasu reakcji); ▪ Ilość zgłoszeń rozwiązanych przez pracowników HelpDesk z podziałem na kategorię zgłoszenia, osób rozwiązujących; ▪ Średni Czas Rozwiązania zgłoszeń w danym okresie w podziale na osoby rozwiązujące; ▪ Średni Czas Rozwiązania zgłoszeń w danym okresie liczony dla całego HelpDesku; ▪ Średni czas do Eskalacji Funkcjonalnej Incydentów (jeżeli nie możliwe jest rozwiązanie przez pracownika HelpDesk) liczony dla całego HelpDesku oraz w podziale na poszczególne osoby; ▪ Liczba reklamacji zgłoszonych przez Użytkowników. ● Zarządzanie Incydentami: ▪ Liczba Incydentów zgłoszonych w danym okresie czasu; ▪ Liczba Incydentów zamkniętych w danym okresie czasu; ▪ Liczba Incydentów rozwiązanych w zadeklarowanych czasach realizacji w podziale na poszczególnych pracowników IT; ▪ Liczba Incydentów przeterminowanych w podziale na poszczególnych pracowników IT; ▪ Liczba Incydentów rozwiązanych przez poszczególnych pracowników IT; ▪ Liczba reklamacji zgłoszonych przez Użytkowników dotyczących rozwiązania Incydentów; ▪ Liczba Incydentów zgłoszonych w danym okresie czasu w podziale na poszczególne Usługi IT; ▪ Liczba Incydentów zgłoszonych w danym okresie czasu w podziale na poszczególne Elementy Konfiguracji. ● Zarządzanie Konfiguracją: ▪ Liczba wolnych licencji na oprogramowanie; ▪ Lista Elementów Konfiguracji, które uległy zmianie w danym okresie czasu. ● Zarządzanie Poziomem Usług: ▪ Liczba zdefiniowanych Usług IT; ▪ Liczba dotrzymanych i niedotrzymanych parametrów świadczenia Usług IT

Wymagania ergonomiczne	System powinien: • umożliwiać poprawną obsługę rozdzielczości: 1024x768, 1280x800, 1280x1024, 1400x1050, 1600x1200, 1440x900, 1680x1050, 1920x1200; • zapewniać czytelność aplikacji: wszelkie przyciski, listy wyboru, opcje będą łatwo dostępne; • umożliwiać dynamiczne definiowanie widoków list wyszukiwanych rekordów i dynamiczne określanie "kolumn" wyświetlanych rekordów bez konieczności programowania, tworzenia i modyfikowania pól przez wyszkolonych administratorów Systemu po stronie Zamawiającego; • umożliwiać sortowanie listy rekordów, według wybranej kolumny po kliknięciu w nagłówek kolumny; • umożliwiać użytkownikom personalizowanie interfejsu, tzn. umożliwi zmianę miejsca wyświetlania komponentów interfejsu, np.: ekranu roboczego, obszaru nawigacyjnego, okna komunikatów, wykresów, itp. bez konieczności programowania; • zapewniać dopasowanie do potrzeb Zamawiającego tzn. system musi mieć możliwość dodawania i modyfikowania istniejących formularzy, możliwości dodawania i modyfikowania istniejących procesów; • umożliwiać użytkownikom korzystanie z wielu okien wybranych funkcjonalności równocześnie; • umożliwiać korzystanie ze schowka systemowego Windows metodą „kopiuj – wklej” (ang. copy – paste); • umożliwiać korzystanie z mechanizmu „przeciągnij i upuść” (ang. drag & drop) przy modyfikacji formularzy; • umożliwiać obsługę interfejsu zarówno za pomocą myszy jak i klawiatury
Bezpieczeństwo	• umożliwiać użytkownikom końcowym dostęp za pośrednictwem przeglądarki internetowej w tym bez potrzeby instalowania dodatkowego oprogramowania na stacji klienckiej; • umożliwiać korzystanie z pełnej funkcjonalności systemu za pośrednictwem przeglądarki internetowej; • wspierać przeglądarki internetowe: Firefox, Chrome, Opera; • zapewniać dwukierunkową integrację z usługami e-mail pracujących w oparciu o następujące protokoły: -SMTP -POP3 -MAPI
Integracja	System powinien umożliwić: • zintegrowanie z systemami Microsoft Active Directory • zintegrowanie z systemami Poczty elektronicznej (wysyłania, przyjmowania, pobierania adresów mailowych z książki adresowej systemu pocztowego)
Gwarancja i wsparcie	• Wsparcie Wykonawcy przez okres min. 60 miesięcy polegające na świadczeniu pomocy zdalnej w trybie 8x5 w ilości min. 1h tygodniowo. • Gwarancja powinno pozwolić na pobieranie nowych wersji oprogramowania przez okres min. 60 miesięcy

Wdrożenie i konfiguracja	Wykonawca powinien: • zainstalować system w środowisku wirtualnym Zamawiającego • skonfigurować integrację z MS ActiveDirectory Zamawiającego • skonfigurować integrację z serwerem pocztowym Zamawiającego • skonfigurować użytkowników oraz administratorów zgodnie z wytycznymi Zamawiającego • skonfigurować powiadomienia • skonfigurować sposób eskalacji zgłoszeń • skonfigurować kategorie zgłoszeń

1.10 Zestaw komputerowy typu All-in-One z oprogramowaniem biurowym (90 kpl.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Opis rozwiązania	Przedmiotem zamówienia jest komputer zintegrowany z monitorem i niewystający poza jego obrys. Zamawiający nie dopuszcza rozwiązań polegających na podczepieniu komputera w malej obudowie z pomocą uniwersalnych uchwytów do monitora lub jego podstawy. Zestaw powinien umożliwiać elastyczną rozbudowę w zakresie: - RAM, - CPU, - pamięci masowe (HDD lub SSD). W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. W przypadku rozwiązania składającego się z kilku komponentów należy podać nazwę producenta, typ, model, oraz numer katalogowy wszystkich elementów składowych rozwiązania.
Wyświetlacz i porty	Matryca matowa w technologii IPS z podświetleniem LED. Rozmiar matrycy min. 23,8”. Rozmiar pojedynczego piksela nie większy niż 0,275 mm. Minimalna rozdzielczość 1920x1080 pikseli. Kąty widzenia pion/poziom co najmniej 178/178 stopni. Czas reakcji matrycy min. 6 ms. Ergonomiczna regulacja podstawy w zakresie: - pochylenie przód/tył min. od -5 do +30 stopni od pionu, - wysokości min. 110 mm, - obrotu na boki (swivel) +/- 45 stopni. Obudowa musi posiadać złącze VESA w standardzie 100 mm. Demontaż podstawy musi odbywać się beznarzędziowo. Złącza min.: - DisplayPort, - HDMI, - wyjście Audio, - 3x USB 3.1 Gen. 1. (w tym min. 1x USB 3.1 typ C) - 1x wejście obrazu cyfrowego (HDMI-in lub DisplayPort-in) pozwalające ustawić komputer w tryb pracy monitora LCD. Wymagana liczba i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.

Wydajność systemu	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych, osiągający w teście PerformanceTest firmy PassMark Software wynik co najmniej 9200 punktów w kategorii CPU Mark (z dnia 01.07.2020 lub później). Zamawiający może zażądać dostarczenia dowodu spełniania ww. warunków w postaci wydruku ze strony https://www.cpubenchmark.net lub raportu z przeprowadzonego testu na konfiguracji nie mocniejszej niż oferowana w niniejszym postępowaniu. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Chipset	Dostosowany do zaoferowanego procesora.
Pamięć operacyjna	32 GB RAM w technologii DDR4 o taktowaniu min. 2600MHz. 2 sloty SoDIMM wspierające pracę pamięci w trybie dual-channel.
Parametry pamięci masowej	SSD o pojemności min. 256 GB w technologii PCIe NVMe. Możliwość instalacji dysków M.2 w formatach 2242 i 2280. Możliwość rozbudowy o dodatkowy dysk SATA 2,5 cala.
Karta graficzna	Zintegrowana z CPU, wykorzystująca pamięć RAM dynamicznie przydzielaną na potrzeby operacji graficznych.
Wyposażenie multimedialne	1. Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. 2. Wbudowane głośniki stereo min 2x 2 W. 3. Wbudowana kamera internetowa o rozdzielczości min.1080p z sygnalizacją LED. 4. Kamera wyposażona w mechanizm umożliwiający fizyczne zasłonięcie obiektywu. 5. Wbudowane dwa mikrofony. 6. Możliwość elastycznego podłączenia dodatkowych zewnętrznych wyświetlaczy za pomocą wbudowanych portów HDMI i DisplayPort.
Połączenia i karty sieciowe	1. Port sieci LAN 10/100/1000 Ethernet RJ-45 zintegrowany z płytą główną obsługujący technologię WoL, PXE. 2. Wbudowe WiFi w standardzie 802.11AC z2x2. 3. Bluetooth 5.0
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.

	13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN

	e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Dodatkowe oprogramowanie	Oprogramowanie producenta komputera: - umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. - Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. - Musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym, kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. - Musi zapewniać możliwość ustawienia automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z SSD/HDD lub innych podłączonych urządzeń zewnętrznych informacji o: - modelu komputera, - numerze konfiguracji, - numerze seryjnym, - identyfikatorze inwentarzowym (Asset Tag), - adresie MAC karty sieciowej, - wersji BIOS-u wraz z datą jego produkcji, - zainstalowanym procesorze, jego taktowaniu i liczbie rdzeni, - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze, - dyskach podłączonych do portów SATA/M.2 (model dysku twardego). Możliwość z poziomu BIOS: - wyłączenia/włączenia portów USB, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: a) użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer, ale nie może kopiować danych z komputera na urządzenie pamięci masowej podłączone do portu USB, b) użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenie pamięci masowej. - ustawienia hasła: administratora, Power-On, HDD/SSD, - blokady aktualizacji BIOS bez podania hasła administratora, - wglądu w system zbierania logów (min. informacja o aktualizacji BIOS, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - komunikowania zmiany konfiguracji sprzętowej komputera, - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania sekwencji bootowania dla trzech scenariuszy uruchomiania komputera: podstawowej, sieciowej (WOL), po awarii, - załadowania optymalnych ustawień BIOS - obsługa BIOS za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.

Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • test pamięci RAM, • test dysku twardego, • test monitora, • test magistrali PCI-e, • test portów USB, • test płyty głównej, • test procesora. Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: producent, model, • BIOS: wersja oraz data wydania, • Procesor: nazwa, taktowanie, • RAM: ilość zainstalowanej pamięci, producent oraz numer seryjny poszczególnych kości pamięci, • Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy. System diagnostyczny działający nawet w przypadku uszkodzenia dysku z systemem operacyjnym komputera.
Zabezpieczenia i zarządzanie	Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona). TPM sprzętowy w wersji 2.0. Czujnik otwarcia obudowy komputera sygnalizujący nieautoryzowany dostęp do takich komponentów jak HDD, RAM, CPU. Wbudowana w płytę główną technologia monitorowania i zarządzania komputerem na poziomie sprzętowym (out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: a) monitorowanie konfiguracji komputera na poziomie komponentowym, b) zdalną konfigurację ustawień BIOS (BIOS Setup), c) możliwość zdalnego zarządzania stanem zasilania komputera: włączenie/wyłączenie/reset/poprawne zamknięcie systemu operacyjnego, d) zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego nośnika FDD/ CD ROM/DVD/Boot USB lub pliku obrazu bootującego takiego nośnika z serwera zarządzającego e) zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości minimum 2560x1600. f) technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.2 (http://www.dmtf.org/standards/mgmt/dash/)
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesora w BIOS.
Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty) - Deklaracja zgodności CE (załączyć do oferty) - TUV Eye Comfort (dokument producenta potwierdzający spełnienie kryterium)

	Głośność jednostki mierzona z pozycji operatora w trybie IDLE maksymalnie 25 dB. Należy dołączyć certyfikat akredytowanej jednostki potwierdzający głośność oferowanego urządzania. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Wymagania dodatkowe	Waga urządzenia maks. 7,5 kg. Suma wymiarów proponowanego rozwiązania bez podstawy nie większa niż 985 mm. Zasilacz o mocy maksymalnej co najmniej 90W o sprawności min. 88%. Dopuszcza się zastosowanie zasilacza zewnętrznego. Klawiatura USB w układzie polskim programisty rozszerzona o możliwość włączenia komputera za pomocą dedykowanego przycisku lub skrótu klawiszowego. Mysz optyczna USB z klawiszami oraz rolką (scroll).
Gwarancja	Minimum 60 miesięcy. Serwis świadczony w miejscu instalacji sprzętu. Gwarancja musi obejmować pozostawienie dysków w przypadku konieczności wykonania dodatkowej diagnostyki poza placówką zamawiającego. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Informacje dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy dostarczą do siedziby Zamawiającego, próbkę oferowanego sprzętu. W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią OPZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek
Wyposażenie dodatkowe	Oprogramowanie Antywirusowe w pełni kompatybilne z ESET Security Management Center (będącym w posiadaniu zamawiającego) umożliwiającym centralne zarządzanie oprogramowaniem AV zainstalowanym na stacjach roboczych. Licencja na oprogramowanie musi zapewniać ochronę stacji roboczych, urządzeń mobilnych, serwerów plików, serwerów pocztowych. Licencja musi zapewniać aktualizacje oraz support w okresie 60 miesięcy od daty dostawy. Zasilacz awaryjny UPS: - min. 500VA/ min. 300W - technologia Line Interactive - min. 3 gniazda wyjściowe C13 - min. 1 gniazdo wejściowe C14 - czas podtrzymywania przy obciążeniu 50% minimum 6.5 minuty - typowy czas przełączenia nie większy niż 6.1ms - przewód min. 1.8m - gwarancja przewidująca naprawę lub wymianę na okres min. 24 miesiące - informacja wizualna o stanie baterii – LED - informacją dźwiękowa o przeciążaniu, wyczerpaniu baterii, pracy z UPS i sieci miejskiej - funkcja okresowego autotestu akumulatora - waga: nie więcej niż 5.3kg - wysokość max. 190mm

	Przewód typu Patchcord kat. 5e zakończone wtykiem RJ-45 – 1 sztuka o długości min. 3m
Oprogramowanie biurowe	Preinstalowane oprogramowanie z licencją (nieograniczoną czasowo) pakietu biurowego spełniające następujące wymagania techniczne: 1. Wymagania odnośnie interfejsu użytkownika: a) pełna polska wersja językowa interfejsu użytkownika, b) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; 2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012, poz. 526); 3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji; 4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); 5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim; 6. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a) edytor tekstów, b) arkusz kalkulacyjny, c) narzędzie do przygotowywania i prowadzenia prezentacji, d) narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), e) narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR; 7. Edytor tekstów musi umożliwiać: a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b) wstawianie oraz formatowanie tabel, c) wstawianie oraz formatowanie obiektów graficznych, d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, f) automatyczne tworzenie spisów treści, g) formatowanie nagłówków i stopek stron, h) śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, j) określenie układu strony (pionowa/pozioma), k) wydruk dokumentów, l) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, m) pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, o) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,

	p) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa; 8. Arkusz kalkulacyjny musi umożliwiać: a) tworzenie raportów tabelarycznych, b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), e) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, g) wyszukiwanie i zamianę danych, h) wykonywanie analiz danych przy użyciu formatowania warunkowego, i) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k) formatowanie czasu, daty i wartości finansowych z polskim formatem, l) zapis wielu arkuszy kalkulacyjnych w jednym pliku, m) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; 9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a) przygotowywanie prezentacji multimedialnych, b) prezentowanie przy użyciu projektora multimedialnego, c) drukowanie w formacie umożliwiającym robienie notatek, d) zapisanie jako prezentacja tylko do odczytu, e) nagrywanie narracji i dołączanie jej do prezentacji, f) opatrywanie slajdów notatkami dla prezentera, g) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, h) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, i) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, możliwość tworzenia animacji obiektów i całych slajdów, j) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, k) pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013; 10. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, e) automatyczne grupowanie poczty o tym samym tytule,

	f) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, g) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, h) mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, i) zarządzanie kalendarzem, j) udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, k) przeglądanie kalendarza innych użytkowników, l) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, m) zarządzanie listą zadań, n) zlecanie zadań innym użytkownikom, o) zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom, p) przeglądanie listy kontaktów innych użytkowników, q) możliwość przesyłania kontaktów innym użytkowników.
Inne	Urządzenia muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta. Urządzenia muszą być dedykowane dla zadania Zamawiającego, nie mogą pochodzić z innych realizacji.

1.11 Komputer przenośny z oprogramowaniem biurowym (15 kpl.)

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji u producenta komputera.
Ekran	Matryca TFT, 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: - FHD 1920x1080, 250nits
Obudowa	Matowa obudowa komputera wyposażona w metalowe zawiasy spełniająca certyfikację MIL-STD-810G. Należy dostarczyć kartę katalogową potwierdzającą zgodność z testami MIL-STD-810G lub dostarczyć oświadczenie producenta komputera.
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w min. dwa złącza dla dysków z czego min. jedno M.2 z obsługą dysków PCIe NVMe. Płyta główna umożliwiająca konfiguracje wielodyskową.
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, na poziomie wydajności 7800 punktów na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/ (min. z dnia 01.07.2020 lub później). Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna	Min. 16 GB z możliwością rozbudowy do 32 GB, rodzaj pamięci DDR4, 2400MHz. Komputer wyposażony w minimum dwa banki pamięci umożliwiające pracę w trybie dual-channel.
Dyski	Wyposażony w dysk półprzewodnikowy (SSD) o pojemności min. 256 GB, pracujący przy wykorzytaniu interfejsu PCIe NVMe. Dysk powinine zawierajać partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
Zabezpieczenie dysku twardego	Komputer wyposażony w systemem automatycznego parkowania głowicy w przypadku zastosowania dysku talerzowego.
Karta graficzna	Karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 1400 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/ z dnia 01.07.2020 lub później)

Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min. 2x 2W, wbudowane dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, kamera HD 720p pracująca przy niskim oświetleniu.
Karta sieciowa	10/100/1000 – RJ 45 wspierająca technologia PXE i WoL.
Porty/złącza	Min. 1xUSB-C, 3xUSB-A z czego min. dwa w standardzie 3.1, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI ver. 1.4, RJ-45, czytnik kart multimedialnych min. microSD. Min. 1 z portów w trybie Power On/Always On.
Stacja dokująca	Możliwość podłączenia stacji dokującej producenta komputera za pomocą dedykowanego złącza dokowania lub złącza USB-C umożliwiające min. transmisję wideo, danych oraz ładowanie komputera w tym samym czasie.
Klawiatura	Klawiatura odporna na zalanie, układ US, z wbudowanym joystikiem do obsługi wskaźnika myszy z dedykowanymi 3 klawiszami. Klawiatura z wydzielonym blokiem numerycznym.
WiFi	Wbudowana karta sieciowa, pracująca w standardzie AC 2x2
Czytnik linii papilarnych	Wbudowany dotykowy czytnik linii papilarnych.
Bluetooth	Wbudowany moduł Bluetooth min. 4.2
Bateria	Bateria - 3 ogniwa, pozwalająca na nieprzerwaną pracę urządzenia do 600 minut. Czas pracy na baterii potwierdzony w teście MobileMark® 2014 (MobileMark 2014 Battery Life) – należy dostarczyć wyniki w formatach FDR (Full Disclosure Report) i PDF programu MobileMark® 2014. Jako równoważne dopuszcza się kartę katalogową producenta komputera potwierdzającą czas pracy na zasilaniu bateryjnym.
Zasilacz	Zasilacz zewnętrzny o mocy maks. 65W
System Diagnostyczny	Wizualny system diagnostyczny producenta dzialający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • Wykonanie testu CPU • wykonanie testu pamięci RAM • test dysku twardego • test matrycy LCD • test magistrali PCI-e • test portów USB Wizualna lub akustyczna sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • Notebook: Producent, PN, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie, obsługiwane instrukcje, ilości pamięci L1, L2, L3 • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, prędkość obrotowa, temperatura pracy • LCD: producent, model, rozmiar, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS wraz z datą, - nr seryjnym komputera - PN producenta sprzętu pozwalający na identyfikację jednostki - ilości pamięci RAM - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - unikalnych nr inwentarzowych tzw. Asset Tag'ów

	- nr seryjnym płyty głównej komputera Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość Wyłączania/Włączania technologii antykradzieżowej - Możliwość ustawienia hasła dla twardego dysku - Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - Możliwość ustawienia minimalnech wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. - Mozliwość włączania/wyłaczania wirutalizacji z poziomu BIOSU - Możliwość ustawienia kolejności bootowania - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, zintegrowanej karty WIFI i BT, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, czytnika kart multimedialnych
Bezpieczeństwo	-złącze Kensington Lock, wsparcie dla ochrony antykradzieżowej
Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty) – ENERGY STAR - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Waga/Wymiary	Waga urządzenia z baterią podstawową max 2.2kg, grubość urządzenia nie większa niż 20mm.
Szyfrowanie	Komputer wyposażony w moduł dTPM 2.0
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).

	11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).

	29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Gwarancja	5 lat świadczona w miejscu użytkowania sprzętu (on-site) W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego. Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego oraz oferowanego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy ostarczą do siedziby Zamawiającego, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą

	zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek
Wyposażenie dodatkowe	Oprogramowanie Antywirusowe w pełni kompatybilne z ESET Security Management Center (będącym w posiadaniu zamawiającego) umożliwiającym centralne zarządzanie oprogramowaniem AV zainstalowanym na stacjach roboczych. Licencja na oprogramowanie musi zapewniać ochronę stacji roboczych, urządzeń mobilnych, serwerów plików, serwerów pocztowych. Licencja musi zapewniać aktualizacje oraz support w okresie 36 miesięcy od daty dostawy. Przewód typu Patchcord kat. 5e zakończone wtykiem RJ-45 – 1 sztuka o długości min. 3m
Oprogramowanie biurowe	Preinstalowane oprogramowanie z licencją (nieograniczoną czasowo) pakietu biurowego spełniające następujące wymagania techniczne: 11. Wymagania odnośnie interfejsu użytkownika: c) pełna polska wersja językowa interfejsu użytkownika, d) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; 12. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: c) posiada kompletny i publicznie dostępny opis formatu, d) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012, poz. 526); 13. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji; 14. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); 15. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim; 16. Pakiet zintegrowanych aplikacji biurowych musi zawierać: f) edytor tekstów, g) arkusz kalkulacyjny, h) narzędzie do przygotowywania i prowadzenia prezentacji, i) narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), j) narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR; 17. Edytor tekstów musi umożliwiać: q) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, r) wstawianie oraz formatowanie tabel, s) wstawianie oraz formatowanie obiektów graficznych, t) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), u) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, v) automatyczne tworzenie spisów treści,

	w) formatowanie nagłówków i stopek stron, x) śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, y) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, z) określenie układu strony (pionowa/pozioma), aa) wydruk dokumentów, bb) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, cc) pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, dd) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, ee) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, ff) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa; 18. Arkusz kalkulacyjny musi umożliwiać: o) tworzenie raportów tabelarycznych, p) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, q) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, r) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), s) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, t) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, u) wyszukiwanie i zamianę danych, v) wykonywanie analiz danych przy użyciu formatowania warunkowego, w) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, x) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, y) formatowanie czasu, daty i wartości finansowych z polskim formatem, z) zapis wielu arkuszy kalkulacyjnych w jednym pliku, aa) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, bb) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; 19. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: l) przygotowywanie prezentacji multimedialnych, m) prezentowanie przy użyciu projektora multimedialnego, n) drukowanie w formacie umożliwiającym robienie notatek, o) zapisanie jako prezentacja tylko do odczytu, p) nagrywanie narracji i dołączanie jej do prezentacji, q) opatrywanie slajdów notatkami dla prezentera, r) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, s) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,

	t) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, możliwość tworzenia animacji obiektów i całych slajdów, u) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, v) pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013; 20. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: r) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, s) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, t) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, u) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, v) automatyczne grupowanie poczty o tym samym tytule, w) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, x) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, y) mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, z) zarządzanie kalendarzem, aa) udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, bb) przeglądanie kalendarza innych użytkowników, cc) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, dd) zarządzanie listą zadań, ee) zlecanie zadań innym użytkownikom, ff) zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom, gg) przeglądanie listy kontaktów innych użytkowników, hh) możliwość przesyłania kontaktów innym użytkowników.
Inne	Urządzenia muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta. Urządzenia muszą być dedykowane dla zadania Zamawiającego, nie mogą pochodzić z innych realizacji.

1.12 System telefonii VoIP

1.12.1 Telefon stacjonarny SIP VoIP (100 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Informacje ogólne	Telefon VoIP wspierający 2 linie SIP z możliwością stworzenia 3-cio stronnej konferencji
Wyświetlacz i przyciski	Ekran o wielkości min. 2,9” o rozdzielczości min. 132x45 min. 2 przyciski dla linii SIP wraz z informacją o stanie linii (min. Dwukolorowa) min. 3 dodatkowych programowalnych przycisków kontekstowych
Złącza i transmisja danych	min. dwa porty Ethernet RJ-45 10/100Mbit/s
Kodeki	Min. G.729 A/B, DTMF G.711µ/a, G.722, G.723, G.726-32, iLBC
Inne	Możliwość montażu na ścianie Obsługa VLANów 802.1Q
Gwarancja	Min. 24 miesiące

1.12.2 Centrala telefoniczna VoIP z funkcją Wideokonferencji (1 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wymagania ogólne	Wirtualna centrala telefoniczna w postaci maszyny wirtualnej pracującej w środowisku Vmware i MS HyperV
Komunikacja zunifikowana	Funkcjonalność systemu zunifikowanej komunikacji w zakresie obsługi połączeń i terminali w zakresie telefonii oraz wideo musi obejmować: 1. Zestawienie co najmniej 96 połączenia jednocześnie 2. Zestawianie połączeń w oparciu o zdefiniowany plan numeracji 3. Możliwość odrzucania połączeń 4. Możliwość warunkowego przekazania połączenia, gdy abonent rozmawia albo nie odbiera połączenia, albo też bezwarunkowo wszystkich połączeń z rozróżnieniem stanu dostępności 5. Parkowanie połączeń oraz funkcje CallPickup 6. Obsługa połączeń na bazie numeracji skróconej, numerów E.164 oraz identyfikatorów SIP URI. 7. Obsługa połączeń oczekujących 8. Identyfikacja połączeń przychodzących 9. Dostęp do książki telefonicznej bezpośrednio z ekranu terminala 10. Obsługa klawiszy szybkiego wybierania numerów 11. Podgląd stanu innych linii/numerów 12. Przekazywanie (transfer) połączeń 13. Oddzwanianie (Callback) 14. Funkcje grup huntingowych z kolejkowaniem połączeń oraz odtwarzaniem dla połączeń oczekujących zapowiedzi powitalnej i zapowiedzi w trakcie oczekiwania. 15. Realizacja audiokonferencji aranżowanych w trybach ad-hoc (rozumianym, jako: wydzwanianie przez organizatora konferencji kolejno do osób, które mają uczestniczyć w konferencji i kolejne dołączanie ich do niej) i planowym (rozumianym, jako: samodzielne wdzwonienie się osób, które mają uczestniczyć w konferencji na podany wcześniej numer), z możliwością udziału w nich łącznie nie mniej niż *50* stron konferencji w jednej lub wielu konferencjach. 16. Możliwość realizacji wideokonferencji z możliwością dołączenia do niej uczestników „tylko audio” za pomocą linii telefonicznych, 17. Funkcjonalność sekretarsko-dyrektorską, w tym monitorowanie linii dyrektora przez sekretariat, ograniczanie połączeń do dyrektora, możliwość włączenia przez dyrektora statusu „nie przeszkadzać” oraz funkcję interkom 18. Logowanie abonenta na telefonie IP, z zachowaniem profilu zalogowanego abonenta (numery linii, uprawnienia abonenckie, ustawienia obsługi połączeń) 19. wbudowana funkcjonalność „Live Chat” umożliwiająca kontakt pomiędzy użytkownikami systemu, a odwiedzającymi firmową stronę internetową za pomocą chatu, połączenia głosowego lub wideo oraz przekazanie takiego połączenia do innego użytkownika - System powinien wspierać protokoły standardowe SIP oraz XMPP - System powinien wspierać funkcję „group chat” (czat z wieloma osobami jednocześnie)
Zarządzanie połączeniami	- Funkcjonalność w zakresie zarządzania połączeniami musi obejmować: 1. Ograniczanie możliwości połączeń (restrykcje), w tym z wymaganiem podania kodu dostępu.

	2.	Możliwość generowania raportów połączeń Call Detail Recorts (CDR), zawierających, co najmniej informacje statystyczne o numerach abonentów wywołującego i wywoływanego, o czasie rozpoczęcia i zakończenia połączenia – dla celów późniejszego tworzenia zestawień wykorzystania systemu telekomunikacyjnego przez jego użytkowników. Możliwość automatycznego wysyłania CDR to zewnętrznych systemów analizujących.
	3.	Możliwość zdefiniowania pojedynczego numeru biznesowego na stacjonarnym terminalu użytkownika, którego wywołanie przez połączenie przychodzące z wnętrza systemu lub z zewnątrz (z sieci PSTN) spowoduje automatyczne jednoczesne propagowanie tego połączenia na inne zdefiniowane przez użytkowane numery urządzeń mobilnych (nie mniej niż cztery). Po odebraniu takiego połączenia na którymkolwiek z nich musi być możliwe przenoszenie połączenia pomiędzy urządzeniem mobilnym a terminalem użytkownika bez konieczności przerywania połączenia
	4.	Logiczne przypisanie do wielu terminali jednego i tego samego numeru (p.. do terminala stacjonarnego i terminala bezprzewodowego)
	5.	Narzędzia do centralnej konfiguracji i zarządzania systemem dla administratora, dostępne poprzez przeglądarkę www.
	6.	Narzędzia zarządzania dla użytkowników końcowych dostępne przez przeglądarkę internetową, dające im możliwość konfiguracji podstawowych parametrów ich terminala, zrealizowane w języku polskim
	7.	wybór sposobu kompresji głosu i wideo dla połączeni– - obsługa, co najmniej standardów: a) G.711, G.729 – dla zachowania zgodności systemu telekomunikacyjnego ze starszymi typami telefonów IP oraz zapewnienia możliwości współpracy z systemami telekomunikacyjnymi innych producentów b) G.722, OPUS – dla zapewnienia połączeń głosowych o podwyższonej jakości dźwięku c) iLBC – dla zapewnienia możliwości wykorzystywania terminali IP objętych systemem telekomunikacyjnym w lokalizacjach objętych łączami o słabych lub niegwarantowanych parametrach jakościowych QoS (np. połączenia VPN),
	8.	automatyczne wybieranie drogi (Auto Route Selection)
	9.	możliwość routingu połączeń na bazie czasu i daty, obsługa routingu telefonii na bazie klasycznej numeracji telefonicznej oraz routingu na bazie SIP URI.
	10.	narzędzia dynamicznego uaktualniania oprogramowania systemowego terminali
	11.	obsługę standardowych protokołów komunikacyjnych SI– - w zakresie komunikacji z terminalami IP i bramami głosowymi oraz trunkami IP/SIP do innych systemów telekomunikacyjnych, a także dla zapewniania przenoszenia informacji o dostępności użytkowników systemu
	12.	możliwość realizacji usługi wideotelefonii z wykorzystaniem terminali wideotelefonicznych
	13.	możliwość realizacji usługi wideotelefonii z wykorzystaniem aplikacji webowej
	14.	możliwość zabezpieczania sygnalizacji za pomocą standardowego protokołu TLS

	15. możliwość zestawiania połączeń szyfrowanych w oparciu o standardowy protokół sRTP zarówno pomiędzy terminalami IP, jak też i do bram głosowych 16. system sterowania połączeniami powinien realizować funkcje kontroli wykorzystania pasma w sieci poprzez mechanizm Call Admission Control. - System musi realizować funkcję zdalnego zarządzania połączeniami telefonicznymi realizowanymi z terminala abonenta poprzez funkcję CTI na bazie komunikatora abonenta. Funkcja sterowania telefonem musi być dostępna co najmniej dla abonentów wyposażonych w telefon IP, kompatybilny do sterowania poprzez CTI. - Informacja o dostępności powinna uwzględniać kilka źródeł informacji: 1. zajętość abonenta w czasie rozmowy telefonicznej, 2. zajętość wynikająca z zaplanowanego spotkania w kalendarzu, 3. zajętość zdefiniowaną samodzielnie przez użytkownika poprzez ustawienie statusu obecności w komunikatorze użytkownika. 4. możliwość realizacji funkcji logowania / wylogowania agentów kolejek na podstawie informacji przesyłanych z zewnętrznego systemu rejestracji czasu pracy po odczycie karty dostępu
Efektywność i bezpieczeństwo komunikacji	System musi realizować następujące funkcje zapewniające efektywność i bezpieczeństwo komunikacji: 1. połączenia głosowe wysokiej jakości z wykorzystaniem kodeków szerokopasmowych, w tym OPUS 2. połączenia wideo, w tym połączenia wielostronne dla minimum 9 uczestników, bez potrzeby dokupywania osobnej licencji oraz sprzętu wideo. 3. informowanie o aktualnym stanie dostępności innych użytkowników systemu (dostępny/niedostępny/proszę-nie-przeszkadzać/przerwa/urlop), 4. interfejs użytkownika umożliwiający łatwy dostęp do informacji o nieodebranych/odebranych/wykonanych połączeniach, do poczty głosowej, a także tworzenie własnych książek adresowych 5. możliwość szyfrowania połączeń 6. dedykowanie rozwiązanie SBC tego samego producenta umożliwiające zestawienie bezpiecznego tunelu VPN pomiędzy siecią LAN a instancją zainstalowaną w innej lokalizacji geograficznej przy zachowaniu pełnej funkcjonalności systemu w tym w szczególności zdalnej konfiguracji i monitoringu terminali końcowych oraz przekazywania prezencji użytkowników
Zarządzanie systemem	- System musi realizować następujące funkcje zapewniające efektywne zarządzanie i utrzymanie systemu telekomunikacyjnego: 1. zdalne zarządzanie całym systemem przez interfejs www (http oraz https) 2. dokonywanie zmian typu instalacja nowych terminali, zmiana ich parametrów, przenoszenie ich na nowe miejsca pracy 3. wykorzystanie mini-przełącznika sieciowego wbudowanego w terminal do podłączenia komputerów do sieci LAN (współdzielenie łącza przez komputer i terminal) celem obniżenia kosztów budowy struktury sieci LAN oraz redukcji złożoności sieci LAN, z możliwością konfiguracji innych VLANów dla głosu i danych 4. zintegrowany system zdalnego monitoringu i zarządzania centralą dostarczany przez producenta i umożliwiający zdalne aktualizacje

	systemu, monitoring poszczególnych usług serwera telekomunikacyjnego oraz prace interwencyjne jap.np. ręczny restart usług serwera 5. nielimitowana liczba użytkowników wewnętrznych - Musi posiadać funkcje w zakresie zarządzania: 1. Język skryptowy na potrzeby konfiguracji, 2. Strumieniowanie rekordów CDR na potrzeby audytu, 3. Logi podsystemów na potrzeby diagnostyki, 4. SNMP, 5. Funkcje archiwizacji i odtwarzania konfiguracji systemu
Zarządzanie użytkownikami	1. Mobilność i dostępność użytkowników przez umożliwienie im logowania się do systemu z dowolnego terminalu ze zdefiniowanej puli 2. Możliwość dostępu z poziomu terminalu do informacji pochodzących z różnorodnych aplikacji merytorycznych 3. Możliwość zdefiniowania dla użytkownika pojedynczego numeru urzędowego, obejmującego osobisty terminal użytkownika w systemie oraz jego inne urządzenie komunikacyjp. (np. telefon komórkowy) 4. Obsługa terminali bezprzewodowych stacjonarnych i mobilnych, 5. zintegrowany, nie wymagający dodatkowych licencji komunikator UC z możliwością przesyłania plików między użytkownikami systemu - System powinien umożliwiać agregację informacji o dostępności użytkownika korzystającego z różnych terminali i udostępniać ją dla komunikatorów programowych oraz innych aplikacji wykorzystujących taką informację. - Wymagana realizacja funkcji informacji o dostępności abonentów w klastrze na każdym z serwerów sprzętowych systemu w celu podniesienia niezawodności. - System powinien zapewniać przechowywanie indywidualnych list kontaktowych dla danego użytkownika.
Kolejkowanie	- W ramach kolejkowania połączeń system powinien mieć możliwość obsługi wielu kanałów komunikacji, co najmniej: telefonię (głos), chat i połączenia wideo. Musi mieć możliwość rozbudowy o obsługę kampanii wychodzących (outbound) . - System musi realizować funkcje kolejkowania Contact Center dla połączeń głosowych oraz dla połączeń wideo. - W ramach funkcji kolejkowania osoby delegowane do obsługi kolejek ACD muszą posiadać webową aplikację na PC dedykowaną do obsługi połączeń oraz edycji stanu gotowości (gotowy/nie gotowy/wylogowany) do przyjmowania kolejnych połączeń. - Osoby delegowane do obsługi muszą mieć możliwość wykorzystania telefonu IP do obsługi połączeń oraz edycji stanu gotowości (gotowy/nie gotowy/wylogowany) do przyjmowania kolejnych połączeń. - System powinien realizować funkcje nadzorcze w zakresie podglądu stanu kolejek ACD i poszczególnych stanowisk. - System powinien realizować funkcje nadzorcze w zakresie generowania raportów historycznych oraz bieżących z pracy systemu oraz pracy poszczególnych agentów. - Funkcje Contact Center powinny być realizowane przez aplikację opartą o protokół IP oraz zintegrowany z systemem sterowania oraz bramami głosowymi systemu telefonii. Nie dopuszcza się stosowania systemów hybrydowych, gdzie serwer ACD jest wyposażony w oddzielne interfejsy TDM.

	- Możliwość rozbudowy systemu kolejkowania o możliwość kierowania połączeń na bazie umiejętności (skill based routing), co najmniej 5 poziomów umiejętności osób. - System powinien mieć możliwość obsługi funkcji nadzorczej monitorującej stanowiska (Supervisor) w formie dedykowanej aplikacji webowej do kontroli, jakości i monitorowania kolejek
IVR	- Funkcje zapowiedzi słownych IVR w ramach centralnego systemu zapowiedzi bez ograniczeń w ilości zagnieżdżeń. - Terminowanie połączeń telefonicznych i ich automatyczną obsługę przez system zapowiedzi IVR (Interactive Voice Responder), definiowaną przez skrypty budowane przez graficzne narzędzie. Obsługa skryptu musi umożliwiać: 1. odgrywanie zapowiedzi głosowych (pliki .wav) 2. odczyt i interpretację sygnałów DTMF 3. możliwość sięgania do danych w źrónp.h HTTP/XML i bazach danych 4. przy obsłudze kolejkowania połączeń odczytywanie danych systemowych takich jak liczba osób oczekujących w kolejkach 5. przy obsłudze kolejkowania połączeń możliwość przesyłania danych do programu, którym dysponuje agent systemu na swoim komputerze PC 6. kolejkowanie połączenia do wybranej kolejki z przypisaną do nich grupą agentów 7. zarezerwowanie zdefiniowanego czasu dla zamknięcia połączenia, do celów sporządzenia notatki oraz wpisania danych do innych aplikacji, 8. przy obsłudze kolejkowania możliwość konfiguracji dla każdego agenta indywidualnych dzwonków dla każdej kolejki na ich terminalach IP. 9. Kierowanie połączeń przychodzących na podstawie numeru dzwp.iącego (np. wykrywanie strefy numeracyjnej) lub podanego w IVR identyfikatora - Możliwość rozbudowy o funkcję pobierania i zapisu informacji do zewnętrznych baz danych w ramach funkcji skryptu IVR. - Możliwość generowania dynamicznych zapowiedzi z wykorzystaniem zamiany tekstu na mowę (TTS) na podstawie informacji wprowadzonych przez dzwoniącego w IVR oraz danych z systemów zewnętrznych
Konferencje	- Musi umożliwiać obsługę wielu równoczesnych konferencji współdzielonych, tzn. bez przypisanego gospodarza spotkania. Wymagana obsługa co najmniej 50 jednoczesnych konferencji współdzielonych bez limitu wielkości konferencji. - System wideokonferencji musi pozwalać na: 1. Uczestniczenie w wideokonferencji bez potrzeby instalacji dodatkowego oprogramowania (jedynie przy użyciu przeglądarki internetowej) 2. rozproszenie geograficzne w co najmniej dwóch lokalizacjach przy założeniu spełnienia wymagań technicznych na łącza między nimi. 3. dopasowanie widoku ekranu powitalnego kp.ferencji, np. dodanie graficznego logo organizacji. 4. Przeprowadzanie konferencji w trybach: a) Jeden do jednego b) Wielu do wielu c) Jeden do wielu (wideoszkolenia)

	5. Automatyczne publikowanie informacji o wideoszkoleniach na stronie internetowej - Musi posiadać funkcjonalność nagrywania spotkań wideo wg poniższych wskazań: 1. Musi umożliwiać nagrywanie, co najmniej 10 jednoczesnych spotkań wideo. 2. Nagrywanie spotkań musi być realizowane, w jakości co najmniej 1080p30. - Musi umożliwiać nagrywanie połączeń audio wg poniższych wskazań: 1. Konfiguracja nagrywania dla każdego abonenta osobno 2. Możliwość nagrywania tylko połączeń zewnętrznych lub wszystkich 3. możliwość zablokowania wyłączenia nagrywania przez abonentów
Bezpieczeństwo	- Musi wspierać mechanizmy w zakresie bezpieczeństwa: 1. Szyfrowanie połączeń Secure Real-Time Transport Protocol z wykorzystaniem AES, 2. Szyfrowanie połączeń sygnalizacyjnych z wykorzystaniem TLS/SSL, 3. Szyfrowanie komunikacji z aplikacjami mobilnymi 4. Obsługa kodów bezpieczeństwa/PIN dla połączeń do spotkań, 5. Informacja o udziale uczestników audio w konferencji wideo na ekranie połączenia
Obsługa FAXów	- Wbudowany serwer fax2mail - Możliwość rozbudowy systemu o funkcjonalności: 1. Email2FAX 2. SMS2Chat 3. Chat2SMS
Aplikacja mobilna	- System powinien mieć możliwość współpracy z aplikacją programowego Komunikatora na urządzenia mobilne, (co najmniej urządzeń na bazie Android i urządzeń typu iPad oraz iPhone) o funkcjonalności obejmującej: 1. informację o dostępności 2. obsługę komunikacji tekstowej (ang. IM, „chat") oraz czat grupowy 3. obsługę połączeń głosowych 4. możliwość podglądu zawartości skrzynki poczty głosowej oraz możliwość odsłuchania wiadomości ze skrzynki poczty głosowej - Producent oprogramowania centrali powinien udostępniać dedykowaną aplikację mobilną co najmniej dla systemów Android oraz urządzeń iPad oraz iPhone
Inne funkcje	- Terminale systemu muszą mieć możliwość dowolnego przenoszenia w obszap.e sieci IP (np. przełączania do innych portów LAN) bez konieczności zmiany jakichkolwiek ustawień w systemie. Odłączenie i ponowne podłączenie terminala nie mogą powodować utraty bądź zmiany jego ustawień. System powinien mieć możliwość: • realizacji funkcjonalności poczty głosowej z możliwością tworzenia skrzynek poczty głosowej dla użytkowników. • realizacji funkcjonalność tworzenia i obsługi indywidualnych zapowiedzi poczty głosowej przed przekierowaniem połączenia do skrzynki. • realizacji funkcjonalność tworzenia i obsługi indywidualnych zapowiedzi abonenckich przed zestawieniem połączenia przychodzącego do abonenta posiadającego pocztę głosową. • realizacji funkcjonalności zapewniającej dostęp dla każdego abonenta posiadającego pocztę głosową do aplikacji webowej, z której abonent może nagrać

	swoje powitanie oraz zmieniać ustawienia kierowania połączeń na pocztę głosową. • tworzenia grup rozgłoszeniowych poza siecią lokalną (unicast paging) System powinien mieć funkcje: • poczty głosowej powinny zapewnić integrację z pocztą elektroniczną w celu unifikacji wiadomości, co najmniej jako przesyłanie na konto email abonenta informacji pozostawionych na poczcie głosowej w formie emaila z załącznikiem oraz transkrypcję nagrania do treści wiadomości email. • emitowania muzyki podczas zawieszenia obsługiwanego połączenia telefonicznego (ang. Music on Hold). Wymagana jest realizacja emitowania muzyki w sieci IP w trybie rozsiewczym (multicast) oraz w postaci indywidualnych, oddzielnych sesji (unicast). • współpracy z systemami rozgłoszeniowymi bez limitu końcówek (multicast paging)
Wsparcie i gwarancja	- System musi być dostarczony z licencjami pozwalającymi na bezpłatne aktualizacje i wsparcie producenta przez 5 lat od daty uruchomienia

1.12.3 Instalacja i uruchomienie

Zamawiający posiada 200 numerów telefonicznych. W chwili obecnej obsługa telefonii VoIP świadczona jest przez zewnętrznego operatora telefonicznego (Netia).

Zamawiający wymaga skonfigurowanie nowej centrali, tj.:
- skonfigurowania numeracji
- skonfigurowania wybierania skróconego
- skonfigurowania kont SIP
- skonfigurowania DialPlanów
- skonfigurowania SIP Trunk do operatora
- skonfigurowania zapowiedzi (w tym przygotowania odpowiednich zapowiedzi zgodnie z wytycznymi Zamawiającego)
- skonfigurowania wielopoziomowego IVR
- skonfigurowania prezentacji numeru
- skonfigurowania grup dzwonienia
- skonfigurowania provisioningu dla telefonów

Ponadto Zamawiający wymaga rozmieszczenia oraz podłączenia wszystkich dostarczanych telefonów. Telefony należy skonfigurować do pracy z centralą. Dla telefonów należy wydzielić osobną podsieć (VLAN) z automatycznym przydzielaniem adresów IP oraz skonfigurować należy automatyczne pobieranie ustawień z centralnego serwera. Obecnie używane telefony VoIP (Grandstream GXP 1450) należy przekonfigurować w sposób pozwalający na korzystanie z nowej centrali oraz dodać do VLANu telefonicznego i automatycznego provisioningu).

Po stronie Wykonawcy pozostaje uzgodnienie wszystkich szczegółów z operatorem telefonicznym (Netia). Zamawiający przekaże odpowiednie dane kontaktowe i pełnomocnictwo do negocjowania parametrów połączenia.

1.13 Urządzenie wielofunkcyjne laserowe mono (4 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Informacje ogólne	Urządzenie wielofunkcyjne A4 posiadające funkcje: drukarka, skaner, kopiarka
Procesor i pamięć	Min. 800Mhz, 256MB RAM
Wyświetlacz	Min. 12cm LCD, dotykowy
Drukowanie	Laserowa drukarka monochromatyczna o rozdzielczości min. 1200x1200 Maksymalna szybkość wydruku min. 39 str./min. Automatyczny duplex
Skaner	Rozdzielczość min. 1200dpi Automatyczne dwustronne skanowanie DADF Podajnik ADF na min. 50 dokumentów

	Automatyczny podajnik na dokumenty min. 50 arkuszy Skanowanie do email, USB, PC, folder (SMB, FTP)
Kopiarka	Rozdzielczość min. 1200x1200 Prędkość min. 38 str./min.
Komunikacja	Min.1 złącze Ethernet 10/100Mbit/s Min. 1 port USB 2.0 WiFi 802.11 b/g/n (WEP, WPA/WPA2)
Podajniki o odbiorniki papieru	Taca odbiorcza na min. 150 arkuszy Podajnik automatyczny na min. 50 arkuszy Podajnik standardowy na min. 250 arkuszy Możliwość rozbudowy podajników do min.1100 arkuszy Maksymalna gramatyra papieru 199 g/m2
Waga	Maks. 17kg
Wysokość	Maks. 490mm
Inne	Możliwość wyposażenia urządzenia w toner na min. 8000 stron według normy ISO/IEC 19752
Gwarancja	Producenta min. 36 miesięcy (on site)

1.14 Urządzenie wielofunkcyjne laserowe kolor (3 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Informacje ogólne	Urządzenie wielofunkcyjne kolor A3 posiadające funkcje: drukarka, skaner, kopiarka, fax
Pamięć	Min. 512MB
Wyświetlacz	Min. 4.2 LCD, dotykowy
Drukowanie	Laserowa drukarka kolorowa o rozdzielczości min. 1200x2400 (dla czerni i koloru) Prędkość wydruku min. 20 str./min. dla A4 oraz min. 11 str./min. dla A3 (zarówno mono jak i w kolorze) Automatyczny duplex
Skaner	Rozdzielczość min. 600x600dpi Skanowanie do email, USB Skanowanie do plików PDF, JPEG, TIFF Skanowanie dwustronne
Kopiarka	Rozdzielczość min. 600x600 Prędkość min. 20 str./min. dla A4 oraz min. 11 str./min. dla A3 (zarówno mono jak i w kolorze) Maksymalna liczba kopii. min 999 Automatyczne kopiowanie dwustronne
Komunikacja	Min.1 złącze Ethernet 10/100Mbit/s Min. 1 port USB 2.0
Podajniki i odbiorniki papieru	Taca odbiorcza na min. 250 arkuszy Podajnik automatyczny na min. 100 arkuszy Podajnik standardowy na min. 250 arkuszy Maks. gramatura papieru min. 215 g/m2 Maksymalna pojemność podajników min. 850 arkuszy
Waga	Maks. 50kg
Wysokość	Maks. 635mm
Inne	czas nagrzewania maks.40s, poziom hałasu max.51dB, toner startowo mono na min. 8000 stron, toner startowy kolor na min.3000 stron
Maksymalne obciążenie	Min. 24000 str.
Gwarancja	Min. 24 miesiące On-Site

1.15 Drukarka laserowa monochromatyczna (30 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Informacje ogólne	Laserowa drukarka monochromatyczna z automatycznym drukiem dwustronnym

Procesor i pamięć	Min. 800Mhz, min 256 MB
Wyświetlacz	Min. 16 znakowy LCD
Drukowanie	Laserowa drukarka monochromatyczna o rozdzielczości min. 1200x1200 Maksymalna szybkość wydruku jednostronnego min. 40 str./min. Maksymalna szybkość wydruku dwustronnego min. 19 str./min. Automatyczny duplex
Komunikacja	Min.1 złącze Ethernet 10/100Mbit/s Min. 1 port USB 2.0
Podajniki o odbiorniki papieru	Taca odbiorcza na min. 150 arkuszy Podajnik automatyczny na min. 50 arkuszy Podajnik standardowy na min. 250 arkuszy Gramatura papieru podajnik zwykły min. 60-120 g/m2 Gramatura papieru podajnik wielofunkcyjny min. 60-200 g/m2
Waga	Maks. 11kg
Wysokość	Maks. 260mm
Inne	Toner startowy na min. 3000 stron, czas pierwszego wydruku maks.7.3, wsparcie dla 802.1x, w oficjalnych materiałach eksploatacyjnych producenta musi być dostępny toner o wydajności min. 8000 stron.
Poziom hałasu	Nie więcej niż 52.5dBA
Gwarancja	Producenta min. 36 miesiące

1.16 Projektor Full-HD wraz z ekranem projekcyjnym (4 kpl.)

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Informacje ogólne	Projektor multimedialny w technologii 3LCD
Natężenie światła	Min. 3000 Lumen
Obraz	Rozdzielczość min. 1920x1080p FullHD Proporcje 16:9 Kontrast min. 10 000:1 Odwzorowanie kolorów min. 1 mld Korekcja obrazu pion i poziom min. +/-30st. Rozmiar projekcji min. 30-300” Zoom manualny Ostrość manualna Automatyczna korekcja trapezu Tryby kolorów min. kino, dynamiczny, gra
Źródło światła	Lampa o żywotności min. 4400h w trybie normalnym
Komunikacja	Możliwość połączenia ze smartfonem, 1x USB 2.0 typu A, 1x USB 2.0 typu B, WiFi 802.11b/g/n, 1x wejście VGA, 2x wejście HDMI, Wejście sygnału kompozytowego, wejście audio cinch
Zużycie energii	Nie więcej niż 300W
Waga	Maks. 2.8 kg
Wyposażenie	Kabel zasilający, pilot, instrukcja obsługi
Inne	Kensington, otwór na linkę zabezpieczającą, ochrona hasłem, wbudowany głośnik min. 2W, funkcja podziału ekranu, możliwość montażu na suficie
Poziom hałasu	Nie więcej niż 38dBA
Ekran projekcyjny	Wymiary min. 200x200cm Powierzchnia projekcyjna Matt White Kąt widzenia min. 150st. Współczynnik odbicia 1 Obudowa: plastikowa kaseta z mechanizmem półautomatycznego zwijania
Gwarancja	Min. 24 miesiące

1.17 Zasilacz Awaryjny UPS do serwerowni (4 kpl.)

Nazwa komponentu	**Wymagane minimalne parametry techniczne**

Parametry podstawowe	- min. 3000VA/ min. 2700W - technologia On-Line Double Conversion - czas podtrzymywania przy obciążeniu 50% minimum 10.5 minuty - napięcie wejściowe min. 160-270V - akumulator bezobsługowy - przewód min. 2.3m
Gniazda	- min. 8 gniazda wyjściowe C13 - min. 2 gniazdo wyjściowe C19 - min. 1 gniazdo wejściowe C20
Informacja graficzna i dźwiękowa	- wyświetlacz LCD wyświetlający min: alarmy, parametry pracy, tryb pracy - informacja dźwiękowa o warunkach pracy z sieci i z UPS
Zarządzanie	- port konsoli RS-232 ze złączem RJ45 lub DB-9 - min. 1 port USB - min. 1 port Ethernet 10/100Mbit/s RJ45 - zdalna instalacja firmware przez FTP - slot na moduł zarządlający
Wymiary i waga	- waga maks. 32kg - wysokość maks. 2U - głębokość maks. 64cm
Inne funkcje	- wczesne ostrzeganie o usterkach - okresowy automatyczny test akumulatora - możliwość zimnego startu - ochrona przed zakłóceniami zasilania: impulsami elektrycznymi, przepięciami, uderzeniami pioruna - wewnętrzny bypass (automatyczny i ręczny) - możliwość montażu w szafie RACK 19” (wymagane dostarczenie niezbęp.ych elementów, np. szyn montażowych)
Gwarnacja	Gwarancja producenta min. 60 miesięcy

2 Oprogramowanie bazodanowe na potrzeby HIS (2 lic.)

Oprogramowanie dedykowane do współpracy z systemami Infomedica i AMMS będącymi w posiadaniu Zamawiającego wraz konfiguracją dedykowaną dla Zamawiającego i optymalizacją procesów bazodanowych wymaganych przez oprogramowanie dziedzinowe (AMMS, Infomedica)

System bazodanowy licencja – 2 szt.

L.p.	Min. wymagania funkcjonalne
1.	Wykonawca dostarczy wymaganą ilość licencji systemu bazodanowego zgodną z konfiguracją serwerów bazodanowych
2.	System bazodanowy zostanie skonfigurowany w trybie HA
3.	Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows jak i Linux.
4.	Oferowany Motor bazy danych dla systemu HIS musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych.
5.	Oferowany Motor bazy danych dla systemu HIS posiada komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open source.
6.	Oferowany Motor bazy danych HIS ma możliwość realizacji kopii bezpieczeństwa w trakcie działania (na gorąco).
7.	Oferowany Motor bazy danych generuje kopie bezpieczeństwa automatycznie (o określonej porze) i na żądanie operatora oraz umożliwia odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
8.	Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
9.	Administrator posiada możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych).
10.	Hasła użytkowników są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej).

11.	Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów PA-RISC i Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX), Intel/AMD Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach
12.	Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych
13.	Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego
14.	Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.
15.	Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.
16.	Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
17.	Możliwość migracji zestawu znaków bazy danych do Unicode
18.	Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
19.	Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych
20.	Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych
21.	Wsparcie protokołu XA
22.	Wsparcie standardu JDBC 3.0
23.	Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
24.	Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.
25.	Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
26.	Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu
27.	Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).
28.	Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej)
29.	Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).
30.	W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek
31.	Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych
32.	Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.
33.	Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywi-

	lejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.
34.	Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online
35.	Możliwość wykonywania kopii bezpieczeństwa w trybie online (*hot backup*).
36.	Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.
37.	W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników
38.	Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX (ang. Portable Operating System Interface) dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.
39.	Możliwość budowy klastra na węźle obsługiwanym przez maksymalnie 2 procesory
40.	Wsparcie producenta (prawo do otrzymywania bezpłatnych aktualizacji przez min.12 miesięcy)

3 Wykonywanie kopii bezpieczeństwa danych w chmurze kryptograficznej

Usługa z wdrożeniem: szyfrowana chmura - 20 TB – 36 miesięcy

3.1 Analiza architektury i opis rozwiązania, obejmuje:

1. Przegląd procedur i uzupełnienie polityki zarządzania backupem w organizacji Zamawiającego.
2. Weryfikację elementów mających zapewnić bezpieczeństwo przetwarzanych informacji (poufność, integralność i dostępność).
3. Przygotowanie rozwiązania dedykowanego do optymalizacji procesu backupu danych w trybie automatycznym na infrastrukturze Zamawiającego.
4. Wykonanie testów pozwalających na ocenę prawidłowości i funkcjonalności zastosowanych procedur i rozwiązań.
5. Wykonywanie backupów w trybie cyklicznym zgodnie z ustaloną polityką.
6. Czasowe użyczenie licencji na okres 36 miesięcy oprogramowania służącego do szyfrowania i bezpiecznego składowania danych zamawiającego w przestrzeni 20 TB z możliwością zwiększenia.
7. Czasowe użyczenie licencji na okres 36 miesięcy oprogramowania służącego do bezpiecznego przesyłania i współdzielenia plików w ramach struktury organizacyjnej Zamawiającego dla 10 komputerów z możliwością zwiększenia.
8. Rozwiązanie technologiczne musi być zgodne z:
   - „Rekomendacjami Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej" i
   - Kodeksem postępowania dla sektora ochrony zdrowia wydanym zgodnie z art. 40 RODO dotyczącym podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających

   i jednocześnie:
   a. posiadać moduł bezpiecznego przesyłania, jak również współdzielenia wszystkich rodzajów i wielkości plików w ramach struktur organizacyjnych jednostki oraz możliwość współdzielenia i przesyłania plików z podmiotami zewnętrznymi za pomocą oprogramowana,
   b. być rozwiązaniem bezpiecznym opartym o technologię kryptograficznej ochrony danych, gwarantującej podwyższony poziom ochrony prywatnych kluczy szyfrujących, który realizowany będzie poprzez technologię zapewniającą, że nie będą one nigdy przetrzymywane w całości w jednym miejscu,

c. zapewnić przesyłanie i współdzielenie plików na urządzeniu klienckim z wykorzystaniem mocy obliczeniowej zarówno jego mikroprocesora, jak i częściowo mocy obliczeniowych mikroprocesorów wykorzystywanych przez serwery, które będą wykorzystywane do bezpiecznego przesyłania i współdzielenia plików, o których mowa,
d. gwarantować wysoki poziom ochrony symetrycznych kluczy kryptograficznych przechowywanych na serwerach z wykorzystaniem mechanizmu kapsułkowania klucza (Key Encapsulation Mechanism),
e. zagwarantować, że wszelkie pliki, które klient umieszcza na serwerze przechowywane i wysyłane będą w formie zaszyfrowanej,
f. zagwarantować, że serwer nie jest w stanie uzyskać dostępu do plików klienta w postaci jawnej (serwer nie posiada, ani nie może wyznaczyć żadnego z kluczy kryptograficznych klienta usługi),
g. gwarantować, że klient nie jest w stanie wykonać żadnej operacji kryptograficznej na swoim kluczu prywatnym (podpisu, deszyfrowania) bez udziału serwera,
h. posiadać współdzielony dysk z możliwością nadawania uprawnień poszczególnym użytkownikom, do którego będzie możliwe dodawanie i przechowywanie plików w formie zaszyfrowanej,
i. zapewniać wysyłanie do określonych użytkowników zaszyfrowanych plików, w tym do pojedynczego odbiorcy jak również grupy odbiorców,
j. zapewniać szyfrowanie wybranych plików na lokalnych i sieciowych dyskach stacji roboczej,
k. zapewnia szyfrowanie z umieszczeniem na serwerze wybranych plików i folderów z poziomu stacji roboczych,
l. zapewniać współpracę z systemem operacyjnym Microsoft Windows w wersji 10 PL (32-bit, 64-bit) i w wersji starszej jakim jest MS Windows 7 (32-bit, 64-bit),
m. współpracować z urządzeniami mobilnymi tj. laptop, tablet z zainstalowanymi systemami operacyjnymi Microsoft Windows w wersji 10 PL (32-bit, 64-bit) i w wersji starszej jakim jest MS Windows 7 (32-bit, 64-bit).
n. posiadać interfejs użytkownika w postaci dedykowanej aplikacji na stacjach roboczych,
o. umożliwiać zarządzanie oprogramowaniem i użytkownikami w nim zdefiniowanymi,
p. pozwalać lokalnie definiować uprawnienia z poziomu użytkownika do poszczególnych zasobów,
q. posiadać kontrolę logowania do konta użytkownika (np. blokowanie logowania na konta prywatne) oraz ograniczać dostęp do konta użytkownika tylko dla wskazanego urządzenia (lub urządzeń),
r. realizować połączenie za pomocą mechanizmów asymetrycznych oraz symetrycznych.,
s. zapewniać szyfrowanie na stacjach roboczych użytkownika,
t. klucz prywatny nie jest przechowywany w jednym miejscu (na stacji roboczej lub serwerze) z wyjątkiem momentu generowania klucza na stacji roboczej,
u. zapewniać szyfrowanie kanału transferu danych na poziomie równym lub wyższym niż technologia Point to Point Tuneling Protocol.
v. interfejs graficzny musi posiadać cechy ułatwiające użytkownikowi zarządzanie informacją np.: cechy i wygląd podobny do klienta pocztowego tzn. posiadać skrzynkę nadawczą, odbiorczą, pozwalać na wpisanie tytułu wiadomości, adresatów, treści i dodawanie załączników.
w. szyfrować end-to-end – współdzielone lub przesyłane pliki muszą być szyfrowane i przekazywane zawsze w postaci zaszyfrowanej.
x. Posiadać funkcjonalność automatycznej synchronizacji szyfrowanych folderów serwera z folderem lokalnym stacji roboczej w kontekście każdego konta użytkownika. Synchronizowany folder musi być dostępny dla użytkownika dopiero po poprawnym zalogowaniu do systemu.
y. Posiadać funkcjonalność wersjonowania plików tak by każdy uprawniony użytkownik mógł przywrócić poprzednią wersję pliku. System musi umożliwiać przywrócenie dowolnej archiwalnej wersji jako wersję aktualną.
z. Posiadać funkcjonalność „kosza”, który przechowuje wszystkie usunięte przez użytkownika pliki i umożliwia ich przywrócenie.
aa. Umożliwiać automatyzację procesów logowania, szyfrowania, przesyłania danych przez zastosowanie API.

3.2 Zasady świadczenia wsparcia oraz opieki serwisowej oprogramowania.

Wykonawca zobowiązany jest w trakcie trwania umowy licencyjnej:

1. Dostarczać Zamawiającemu nowsze wersje oprogramowania, uaktualnienia oraz „support packi" poprzez wskazanie miejsca do pobrania i przesłania informacji drogą mailową, wraz z instrukcją instalacji i listą zmian – *release notes*;
2. Świadczyć usługi opieki serwisowej oraz wsparcia oprogramowania także na nowszych wersjach oprogramowania – dostarczonych w ramach umowy;
3. Udzielić wsparcia w trakcie instalacji dokonywanych przez Zamawiającego dostarczonego oprogramowania oraz poprawek;
4. Zapewnić rozwiązywanie problemów związanych z instalacją i funkcjonowaniem dostarczonego oprogramowania;
5. Zapewnić przyjmowanie zgłoszeń telefonicznych potwierdzanych zgłoszeniem elektronicznym (www lub e-mail) w trybie 24x7x365 od Zamawiającego z zachowaniem minimalnych warunków przyjęcia zgłoszenia, przez Wykonawcę, tj.:
   - w godzinach pomiędzy 08:00 a 16.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte danego dnia roboczego;
   - w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego;
   - w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 danego dnia roboczego;
   - w dniu ustawowo lub dodatkowo wolnym od pracy - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego;
6. Nie później niż w ciągu 30 minut od momentu otrzymania zgłoszenia awarii potwierdzić przyjęcie zgłoszenia;
7. Zapewnić czas reakcji na zgłoszone problemy, rozumiany jako przesłanie szczegółowego planu działania naprawczego Wykonawcy w związku z dokonanym zgłoszeniem przy zgłoszeniu:
   a. błędu krytycznego do 12 godzin od momentu zgłoszenia,
   b. błędu niekrytycznego naprawa powinna nastąpić w najbliższym wydaniu oprogramowania.

Status zgłoszenia określa Zamawiający, wg poniższych kryteriów:

a. błąd krytyczny – nie można zaszyfrować/odszyfrować danych;
b. błąd niekrytyczny – pozostałe błędy;

8. Zapewnić dostęp do bazy wiedzy o dostarczonym oprogramowaniu;
9. Zapewnić e-mail'owe i telefoniczne konsultacje w zakresie dostarczonego oprogramowania we wszystkie dni robocze w godz. 9.00 – 17.00.

3.3 Dokumentacja.

W ramach realizacji projektu, Wykonawca opracuje i dostarczy m.in. szczegółową dokumentację dotyczącą instalacji, konfiguracji i parametryzacji Systemu do szyfrowania danych oraz konfiguracji stacji roboczych wraz z opisem procedur i instrukcji eksploatacyjnych.

1. Wykonawca przygotuje:
   1.1. Procedury i instrukcje instalacji i rejestracji licencji.
   1.2. Procedury i instrukcje odzyskiwania kont użytkowników.
   1.3. Procedury i instrukcje bieżącego monitoringu zasobów serwerowych.
   1.4. Procedury i instrukcje aktualizacji i wdrażania łat.
   1.5. Politykę szyfrowania danych na stacjach roboczych.
   1.6. Metody odzyskiwania danych zaszyfrowanych lokalnie oraz na nośnikach zewnętrznych.
   1.7. Opis ról i ich uprawnień do Systemu.
   1.8. Procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów.

1.9. Procedury tworzenia płyty CD/DVD i pendrive z oprogramowaniem do odzyskiwania danych. W przypadku konieczności użycia do tworzenia płyty CD/DVD i pendrive oprogramowania firm trzecich, Wykonawca w ramach niniejszego projektu, bez dodatkowych kosztów dla Zamawiającego, dostarczy i przekaże na jego rzecz to oprogramowanie wraz z licencjami umożliwiającymi jego użytkowanie przez okres subskrypcji dla ilości zgodnej z ilością licencji.

1.10. Instrukcje obsługi Systemu do szyfrowania danych dla: Użytkowników oraz Administratorów.

2. Dokumentacja będzie weryfikowana i w razie potrzeby zaktualizowana po każdej modyfikacji/ aktualizacji Systemu do szyfrowania danych.
3. Dokumentacja dotycząca czynności administracyjnych związanych z utrzymaniem Sytemu do szyfrowania danych musi być dostarczana niezwłocznie wraz z nową wersją Systemu. Pozostała dokumentacja może być dostarczona nie później niż w terminie 14 dni od daty przekazania nowej wersji Systemu.

3.4 Szkolenia

Wykonawca zorganizuje szkolenie prowadzone przez certyfikowanego inżyniera oferowanego oprogramowania, z zakresu szyfrowania danych dla 1 grupy administratorów składającej się z 2 osób, w siedzibie Zamawiającego. Program szkolenia musi obejmować całość zagadnień z zakresu szyfrowania danych oraz szczegółowo omawiać proces zdalnej pomocy użytkownikom, odzyskiwania danych i mechanizmów szyfrowania danych.

4 System automatycznej digitalizacji dokumentów na potrzeby dokumentacji medycznej prowadzonej w formie elektronicznej zgodnie z normą PN-EN ISO 10781 (10 stanowisk)

4.1 Ogólne warunki

Przez system automatycznej digitalizacji dokumentów papierowych rozumiane jest sprzęt i oprogramowanie, które umożliwia jednoczesne powstawanie wersji papierowej i elektronicznej dowolnego, ustrukturyzowanego dokumentu. W ramach przetworzonego dokumentu powinna automatycznie powstawać wersja pdf tworzonego dokumentu oraz xml z danymi zawartymi w strukturze dokumentu.

W szczególności system powinien gwarantować zapisy z normy w zakresie:

- IN.1.1 – uwierzytelnianie podmiotu tworzącego dokumentację poprzez podpis biometryczny
- IN.1.5 – system powinien zawierać obiektywne znaczniki czasu identyfikujące czas początkowego wpisu oraz modyfikacji danych, oraz identyfikować aktora/podmiot biorący udział w powstawaniu lub zmianie dokumentu.
- IN.1.6 – dane powinny być zaszyfrowane w sposób uniemożliwiający ich odtworzenie na skutek zagubienia nośnika danych.
- IN.1.7 – system powinien zapewniać możliwość powiązania każdej treści z autorem tej treści
- IN.1.9 – system powinien zapewniać pacjentom możliwość weryfikacji dokumentacji w momencie jej powstawania, a także udzielania zgody na przetwarzane dane w sposób możliwy do zaakceptowania przez każdego pacjenta (złożenie podpisu odręcznego)

W ramach zamówienia Wykonawca zobowiązany jest do:

1. Przeprowadzenia audytu w zakresie obowiązujących w szpitalu dokumentów papierowych
2. Dostawy sprzętu umożliwiającego wykonanie funkcjonalności systemu – długopisów cyfrowych
3. Instalacji i wdrożenia systemu automatycznej digitalizacji dokumentacji
4. Przeprowadzenia odpowiednich szkoleń w zakresie administrowania i użytkowania systemu

5. Świadczenia usługi serwisowej wraz z nadzorem autorskim dla wszystkich przekazywanych licencji

Zamawiający zastrzega sobie prawo wezwania Wykonawców do przeprowadzenia prezentacji oferowanego Systemu. Brak podczas prezentacji funkcji zadeklarowanej jako posiadana będzie równoważny z niespełnieniem kryteriów w danym obszarze. Prezentacja może dotyczyć całości lub wybranych funkcjonalności według wyboru zamawiającego. Prezentacja odbywać się będzie wyłącznie w obecności zamawiającego i upoważnionych przedstawicieli wykonawcy dokonujących prezentacji. Przebieg prezentacji może zostać utrwalony za pomocą nagrania audio/video.

4.2 Szczegółowy opis systemu

4.2.1 Licencje

Zamawiający wymaga by Wykonawca dostarczył dodatkowe bezterminowe licencje Systemu

Wymagania dotyczące licencji:

a) Licencje mają być zainstalowane w systemie z określeniem uprawnień do ich wykorzystywania na serwerze i stacjach roboczych.
b) Wykonawca oświadcza, że przysługują mu prawa do sprzedaży licencji lub posiada nadane przez jej autora prawo do udzielania sublicencji na użytkowanie Oprogramowania Aplikacyjnego.
c) Wykonawca udzieli Zamawiającemu licencji/sublicencji na użytkowanie Oprogramowania Aplikacyjnego, którego zakres funkcjonalny został określony poniżej.
d) Licencja/sublicencja na użytkowanie Oprogramowania Aplikacyjnego jest licencją niewyłączną i zostaje udzielona Zamawiającemu na czas nieokreślony.
e) Zamawiający ma prawo tylko do takich kopii Oprogramowania, które są niezbędne do zapewnienia bezpieczeństwa ich działania. Kopia nie może być używana równocześnie z systemem.
f) Zamawiający nie ma prawa do sprzedaży, wypożyczania, powielania, odstępowania lub rozpowszechniania w innej formie, zmienienia, dekompilacji, tłumaczenia Oprogramowania Aplikacyjnego.
g) Zamawiający nie ma prawa do usuwania bądź zmiany znaków handlowych i informacji o Wykonawcy, bądź producencie podanych w Oprogramowaniu, Sprzęcie i materiałach towarzyszących.
h) Zamawiający ma prawo do rozpowszechniania bez ograniczeń danych i dokumentów utworzonych za pomocą Systemu.
i) Wykonawca zapewni, że jest autorem tworzonego systemu i posiada prawa autorskie i majątkowe do kodów źródłowych aplikacji, dzięki czemu może w dowolny sposób kształtować potencjalne nowe funkcjonalności Systemu.

4.2.2 Wdrożenie

Wymagania dotyczące wdrożenia:

a) Przeprowadzone zostanie:

- audyt dokumentacji papierowej funkcjonującej u Zamawiającego – na podstawie dokumentacji medycznej dostarczonej Wykonawcy przez Zamawiającego – jako podstawa do wykonania analizy przedwdrożeniowej
- instalacja, konfiguracja oraz parametryzacja elementów Systemu na serwerach wirtualnych oraz na stacjach roboczych,
- konfiguracja dostarczonych długopisów cyfrowych w zakresie umożliwiającym ich użytkowanie i przypisanie do użytkowników
- szkolenia w formie webinarium lub filmu instruktażowego dotyczące należytego posługiwania się Systemem dla wszystkich obsługujących System od strony administracyjnej oraz wyznaczonych przez Zamawiającego innych użytkowników Systemu

b) Zamawiający wymaga by System wdrożony przez Wykonawcę w ramach realizacji przedmiotu zamówienia były wdrożony w pełnej ich funkcjonalności opisanej poniżej.
c) Instalacja i wdrożenie winny odbywać się w godzinach pracy pracowników Zamawiającego tj. w dni robocze, w godz. 9.00-15:00. Zamawiający dopuszcza wykonywanie prac w innym czasie niż wskazany, po odpowiednim uzgodnieniu i jego akceptacji.
d) Prace wdrożeniowe na serwerach wirtualnych powinny odbywać się zdalnie - poza siedzibą Zamawiającego – z wykorzystywaniem zdalnego pulpitu i udzielonego wyznaczonym pracownikom Wykonawcy imiennego dostępu do wirtualnej sieci prywatnej
e) Prace wdrożeniowe związane z przygotowaniem stanowiska roboczego zostaną przeprowadzone przez personel Zamawiającego w asyście telefonicznej Wykonawcy. Wykonawca przekaże Zamawiającemu zestaw instalatorów niezbędnych do przeprowadzenia konfiguracji wraz z instrukcjami instalacji
f) Po dokonaniu instalacji i wdrożenia systemu, docelowo system powinien:

- spełniać wymagania określone niniejszym dokumentem,
- spełniać wymagania obowiązujących przepisów prawa i uwzględniać charakter prowadzonej przez Zamawiającego działalności,
- powstające dokumenty spełniać normę PN-EN ISO 10781,

e) Po zakończeniu realizacji przedmiotu zamówienia oraz po stwierdzeniu poprawności funkcjonowania Systemu działającego u Zamawiającego, podpisany zostanie przez Zamawiającego i Wykonawcę Końcowy Protokół Odbioru – bezusterkowy. Warunkiem podpisania Końcowego Protokołu Odbioru (bezusterkowego) będzie:

- wykonanie przez Wykonawcę testów poprawności działania systemu,
- pisemne zaakceptowanie przez Zamawiającego przekazanych przez Wykonawcę wyników testów.

f) Po zakończeniu realizacji przedmiotu zamówienia Wykonawca wykona i przekaże Zamawiającemu dokumentację powykonawczą dla administratorów zawierającą dokładny opis funkcjonalny Systemu z uwzględnieniem ich konfiguracji na etapie wdrożenia.

g) Zamawiający wymaga by elementy systemu zintegrowane z systemem medycznym HIS AMMS, z którego korzysta Zamawiający spełniały następujące warunki:

- zapewnienie możliwości generowania formularzy zintegrowanych systemów bezpośrednio z interfejsu systemu HIS AMMS
- zapewnienie możliwości umieszczania na generowanych formularzach danych identyfikacyjnych pacjenta
- zapewnienie możliwości automatycznego wiązania z kontem pacjenta i przekazywania wypełnionych formularzy do systemu HIS AMMS.
- zapewnienie pełnego dostępu do danych gromadzonych w Systemie,
- zachowanie ciągłości obecnie stosowanej przez Zamawiającego numeracji dokumentacji medycznej.

4.3 Wymagania dotyczące serwisu i nadzoru autorskiego

a) W ramach usług serwisowych i udzielonej gwarancji - przez okres 24 miesięcy od daty podpisania Protokołu Odbioru – bezusterkowego, Wykonawca zapewni pełną funkcjonalność systemu po-

przez nieodpłatne usuwanie awarii, błędów i usterek programistycznych w dostarczonym i istniejącym oprogramowaniu, nieodpłatne dostarczanie nowych wersji oprogramowania, aktualizacji i poprawek oraz ich aplikowanie, stałą nieodpłatną adaptację do wymogów obowiązującego prawa oraz bezpłatne udzielanie konsultacji telefonicznych, wykonawca będzie nieodpłatne dostarczał nowe wersje oprogramowania, aktualizacje i poprawki wraz z ich aplikowaniem, stałą nieodpłatną adaptację do wymogów obowiązującego prawa jak również świadczył bezpłatnie usługę nadzoru autorskiego w tym okresie.

b) Warunki brzegowe realizacji usług serwisowych przedstawiono w Tabeli

Warunki brzegowe realizacji usług serwisowych

Nazwa	minimalne warunki serwisu	Uwagi
Godziny pracy Serwisu	8^{00}-16^{00}	Okres godzin w ciągu dnia roboczego od poniedziałku do piątku.
Czas reakcji Serwisu	4h	Czas w godzinach liczony od chwili zaewidencjonowania w serwisie Zgłoszenia Serwisowego do momentu przyjęcia zgłoszenia tj. nadania mu statusu „przyjęte/ zarejestrowane” w godzinach pracy serwisu.
Czas usunięcia Awarii	48h	Czas liczony w dniach roboczych od upłynięcia czasu reakcji
Czas usunięcia Wady Aplikacji	7 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji
Czas usunięcia Usterki Programistycznej	30 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji
Czas obsługi Konsultacji	10 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji.

4.4 Wymagania dotyczące sprzętu

W ramach systemu zostaną dostarczone długopisy cyfrowe w ilości 10 szt.
Parametry:

- wytrzymałość na upadek na dowolną powierzchnię z wysokości 1,5 m
- pojemność do 1000 wypełnionych dokumentów
- możliwość transmisji danych przez bluetooth
- możliwość transmisji danych przez złącze USB
- ładowanie długopisów przez złącze USB
- wbudowany zegar wewnętrzny z możliwością synchronizacji
- możliwość działania w zakresie temperatur od 0-40 stopni Celsjusza
- Zasilanie - wbudowana bateria litowo-jonowa lub polimerowa
- dołączony program instalacyjny ze sterownikami umożliwiający zgrywanie danych i wysyłanie do centralnego repozytorium danych
- obsługiwane systemy operacyjne: Windows 7/8/10

4.5 Wymagania dotyczące gwarancji

Warunki gwarancji na sprzęt:

- 24 miesiące (dwa lata) gwarancji od momentu dostarczenia.

- Wszystkie naprawy gwarancyjne realizowane w siedzibie Zamawiającego, a w przypadku, gdy jest to niemożliwe z przyczyn technicznych w innym miejscu po uzgodnieniu z Zamawiającym.
- Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
- serwis obejmuje podmianę sprzętu w razie zaistnienia takiej konieczności

Warunki gwarancji na System:
- opisane w części dotyczącej serwisu

4.6 Wymagania Niefunkcjonalne Systemu

1. Możliwość uruchomienia Aplikacji Systemu (w tym zgrywania danych) na dowolnym komputerze z systemem operacyjnym Windows 7/8/10, wersje 32 lub 64-bitowe
2. Możliwość wydruku formularzy na dowolnej sieciowej drukarce laserowej autoryzowanej w Systemie
3. Możliwość zbierania danych na formularzach niezależnie od infrastruktury informatycznej (zbieranie danych off-line)
4. Możliwość zbierania danych na formularzach i odkładanie ich w repozytorium danych niezależnie od niedostosowania do przyjęcia danych Systemu HIS AMMS (możliwość uzupełnienia funkcjonalności Systemu back-hand'owego w terminie późniejszym).
5. Przygotowanie modułu transmisji danych do Zintegrowanego Systemu HIS AMMS.

- System będzie w szczególności udostępniał zestaw protokołów komunikacyjnych niskiego poziomu, które umożliwią pobieranie danych z repozytorium dokumentów do zewnętrznego Systemu w postaci dokumentów PDF oraz plików XML z metadanymi.
- System powinien udostępnić HIS AMMS sieciowy interfejs on-line umożliwiający wydruk sprofilowanych ankiet w postaci mikrodruków.
- System powinien udostępnić HIS AMMS sieciowy interfejs on-line umożliwiający błyskawiczne pozyskiwanie i przekazywanie wszystkich danych dotyczących przeanalizowanych formularzy papierowych.
- Wszystkie interfejsy sieciowe powinny zostać opracowane w technologiach zdalnego wywołania metod (WebService) i przekazane wraz z dokumentacją wykonawcom oprogramowania HIS AMMS.
- We współpracy z Zamawiającym powinna zostać opracowana określona liczba sztuk formularzy, które będą mogły być wypełniane za pomocą długopisu (z możliwością rozszerzania o kolejne formularze), a następnie archiwizowane w systemie HIS AMMS.

6. Implementacja nowych formularzy do Zintegrowanego Systemu ma odbywać się poprzez import do aplikacji edytora WYSIWYG (będącej elementem systemu) tła dokumentu w postaci PDF (tzn. obrazu niezmiennej części dokumentu), a następnie naniesienie na tło regionów aktywnych, z których pozyskiwane mają być wprowadzane dane oraz nadrukowywane serie danych. Każdy z tak utworzonych formularzy ma zostać powiązany z odpowiadającymi mu formularzem oraz szablonem pisma w systemie AMMS.
7. Integracja z systemem HIS AMMS ma zapewniać, że każdy dokument uzyskany z systemu może być spersonalizowany pod kątem pacjenta - tzn. na kartce papieru mają zostać nadrukowane uzgodnione z Zamawiającym dane pochodzące z systemu HIS AMMS – w szczególności dane identyfikacyjne pacjenta
8. Wywołanie zintegrowanego formularza na ekranie klienta lub zlecenie jego wydruku na drukarkę ma odbywać się z poziomu konta pacjenta w widoku Dokumentacji Medycznej w systemie HIS

AMMS. Tak wygenerowany dokument ma być jednoznacznie powiązany z pacjentem i kontekstem, w którym został utworzony

9. Zgodność powstających danych z normą PN-EN ISO 10781.
10. Brak możliwości odtworzenia danych z długopisu cyfrowego bez wgrania danych i zalogowania się do systemu.

4.7 Wymagania Funkcjonalne Systemu

1. System umożliwia odwzorowanie (tak jakby został zeskanowany) formularza papierowego w wersji elektronicznej.
2. System umożliwia automatyczne powiązanie z rodzajem formularza, który został z jego pomocą wypełniony.
3. System umożliwia stworzenie dowolnego formularza bazując na dowolnym dokumencie w formacie PDF.
4. System umożliwia w importowanej ankiecie zaznaczenie regionów aktywnych, pól tekstowych oraz nadanie im unikalnych nazw.
5. System umożliwia wydruk formularza w ten sposób, aby każdy wydrukowany formularz był unikalny (na zasadzie druku ścisłego zarachowania). Oznacza to, że wypełnienie papierowego formularza długopisem cyfrowym tworzy wzajemnie jednoznacznie przyporządkowaną do niego wersje elektroniczną dokumentu. Formularzy nie można kserować (skserowane formularze nie działają, a długopis sygnalizuje to). Funkcjonalność ta powinna być zrealizowana poprzez zapewnienie na każdym dokumencie unikalnego mikrodruku.
6. System umożliwia pobranie danych z długopisów cyfrowych za pomocą stacji dokującej USB bądź też komunikacji bezprzewodowej bluetooth. Dane są jednoznacznie przyporządkowywane do formularzy.
7. System umożliwia przeglądanie oraz eksport nieprzetworzonych danych z wypełnionych formularzy do formatu PDF będącego wizualizacją „skanów" wypełnionych dokumentów.
8. System umożliwia automatyczne rozpoznawanie zawartości pól tekstowych i pól numerycznych zarówno w obszarze pisma blokowego jak i pisma ciągłego (oprogramowanie typu ICR).
9. System umożliwia edycję i walidację przetworzonych danych zwizualizowanych na formularzu z pól tekstowych i pól numerycznych przy jednoczesnym podglądzie danych pochodzących bezpośrednio z urządzeń.
10. System umożliwia eksport rozpoznanych danych (tj. pól tekstowych liczb i pól wyboru) do formatów MS Excel oraz plików CSV lub XML.
11. System umożliwia nadawanie długopisom unikalnych nazw i przypisywania ich do użytkowników i stanowisk.
12. System umożliwia odtwarzanie całej historii powstałego dokumentu z podziałem na czas w jakim dane elementy powstały oraz autorów poszczególnych wpisów.
13. System umożliwia automatyczne umieszczenie elektronicznej wersji dokumentu w postaci PDF na koncie pacjenta w systemie HIS AMMS.
14. System umożliwia wersjonowanie dokumentów w HIS AMMS w taki sposób, że jeżeli po zgraniu danych do dokumentu zostanie cokolwiek dopisane, w systemie HIS AMMS mają być dostępne wszystkie kolejne etapy powstawania dokumentu w ramach kolejnych osadzonych w czasie wersji.

Wygenerowanie dla danego pacjenta kolejnego formularza tego samego typu ma być traktowane jako osobny dokument, a nie jako kolejna wersja wcześniejszego.

W ramach wymagań serwerowych Zamawiający zapewni wirtualną przestrzeń zawierającą co najmniej jeden serwer wirtualny. O minimalnych wymaganiach Serwera:

1. 500 GB przestrzeni dyskowej przeznaczonej na wyłączne potrzeby Systemu automatycznej digitalizacji dokumentu
2. 8 GB pamięci Ram
3. Co najmniej 8-rdzeniowy procesor
4. System operacyjny Windows Server 2012 r2 lub wyższej
5. Serwer bazy danych MS SQL w wersji Express 2012 lub wyższej
6. Możliwość uruchamiania aplikacji w technologii .NET
7. Możliwość zdalnego dostępu do serwera na wniosek Wykonawcy, na czas wykonywania prac serwisowych lub administracyjnych
8. Odblokowany ruch przychodzący z sieci wewnętrznej dla portów 40 (http) i 443 (https)
9. Odblokowany ruch przychodzący poprzez VPN dla portów 80 (http), 443 (https) i 3389 (rdp)

5 System Rejestracji Czasu Pracy (3 punkty)

W ramach realizacji zadania zostanie dokonana instalacja systemu wraz urządzeniami w miejscach wskazanych przez Zamawiającego.

Minimalne wymagania techniczne rejestratora:

Napięcie zasilania:	12V DC
Maksymalny pobór prądu:	300 mA przy 12V DC
Pamięć wewnętrzna RAM/FLASH:	1 MB/4GB
Max. ilość obsługiwanych identyfikatorów	100 000 szt.
Ilość zdarzeń w pamięci RAM:	1 000 000
Komunikacja:	Ethernet
Pomiar czasu:	zegar czasu rzeczywistego (RTC) pracujący w trybie 24h
Podtrzymanie RAM'u i zegara:	bateria litowa 3V/230 mAh
Wyświetlacz LCD:	graficzny 128x64 z podświetlaniem, technologia FSTN
Sygnalizacja:	3-kolorowy wskaźnik świetlny, sygnalizator akustyczny
Klawiatura:	pojemnościowa, dotykowa 4-przyciskowa
Obudowa:	ABS
Kolor obudowy:	czarny
Waga:	ok. 0,9 kg
Wymiary:	min. 138 x 176 x 42 mm
Temperatura pracy:	-10 ¸ 55°C
Temperatura przechowywania:	-20 ¸ 70°C
Wilgotność względna otoczenia:	poniżej 80% (bez kondensacji)
Inne:	Rejestrator współpracuje z wbudowanym czytnikiem zbliżeniowym identyfikatorów zgodnym ze standardem ABATrack II (opcjonalnie ze standardem Wiegand)

Rejestrator ma możliwość podłączenia dodatkowego zewnętrznego czytnika identyfikatorów zgodnym ze standardem ABATrack II. opcjonalnie ze standardem Wiegand.

Minimalne funkcjonalności rejestratora:

Rejestrator wyposażony jest w cztery dotykowe przyciski funkcyjne:

- przycisk wejścia,
- przycisk wyjścia,
- przycisk wejścia służbowego,
- przycisk wyjścia służbowego,

Wybór funkcji rejestratora realizowany jest poprzez dotknięcie jednego z tych przycisków.
Po upływie 5 sekund od chwili wyboru, któregokolwiek z w/w przycisków rejestrator wraca do stanu czuwania.

W rejestratorze wyboru trybu pracy można dokonać manualnie lub automatycznie z harmonogramu.
W przypadku, manualnego wyboru trybu pracy na ekranie głównym rejestratora wyświetlana jest aktualna godzina i data bez ustawionego domyślnego trybu pracy.
W przypadku, gdy tryb pracy rejestratora jest ustawiony automatycznie z harmonogramu na ekranie głównym wyświetlany jest aktualny tryb pracy oraz godzina i data.
Możliwość zdefiniowania harmonogramu tygodniowego, wewnątrz którego następuje ustawienie danego kierunku i trybu pracy czytników.
Możliwość realizowania przez rejestrator funkcji Kontroli Dostępu dla przejść z blokowanym drzwiami oraz kołowrotów z potwierdzeniem przejścia (ACK).
Możliwość wpięcia sygnału PPOŻ powodującego ustawienie na schemat "trwale odblokowany".
Poprawny zapis rejestracji dodatkowo sygnalizowany jest zmianą koloru wskaźnika świetlnego na zielony oraz krótkim sygnałem dźwiękowym.
Rejestrator ma posiadać funkcję „Informacja dla użytkownika” mającą na celu wyświetlenie użytkownikowi krótkiej informacji tekstowej.
Danemu pracownikowi może być przypisana jedna informacja. Istnieje możliwość zdefiniowania, kiedy informacja będzie wyświetlana: przy wejściu - jeden raz, przy wyjściu - jeden raz, przy wejściu - zawsze, aż do usunięcia lub nadpisania, przy wyjściu - zawsze, aż do usunięcia lub nadpisania, za każdym razem (przy wejściu lub wyjściu), zawsze, aż do usunięcia lub nadpisania.
Dodatkowo istnieje możliwość wpisania zakresu czasowego (data od – data do), kiedy informacja będzie wyświetlana.
O pojawieniu się informacji na wyświetlaczu rejestratora użytkownik informowany jest przerywanym sygnałem dźwiękowym i wskaźnikiem świetlnym, który miga w kolorze żółtym.
Wyświetlenie informacji dla użytkownika odbywa się wyłącznie po identyfikacji z użyciem identyfikatora, bez wykonywania, żadnych dodatkowych czynności.

Sygnalizacja zdarzeń:

- Wybór nieprawidłowego trybu pracy: na ekranie rejestratora jest wyświetlana informacja "zmień tryb", komunikat ma na celu poinformować użytkowania, że jego próba rejestracji jest nieudana, ponieważ upłynął maksymalny czas zmiany ustawiony w rejestratorze i wówczas można zmienić tryb rejestracji tylko na wejście. Przez maksymalny czas pracy należy rozumieć zakres czasu, po upływie, którego nie będzie możliwa rejestracja wyjścia. O wystąpieniu takiego błędu dodatkowo informuje krótki sygnał dźwiękowy oraz czerwony kolor wskaźnika świetlnego. Należy wówczas zmienić tryb rejestracji na wejście i zatwierdzić poprzez przyłożenie identyfikatora w pole odczytu. Komunikat jest wyświetlany przez 4 sekundy lub do momentu wciśnięcia przycisku wyboru trybu.
- W przypadku próby rejestracji identyfikatorem z systemu, któremu nie nadano uprawnień, na ekranie rejestratora wyświetlana jest informacja „Karta nieuprawniona” , o wystąpieniu takiego błędu dodatkowo informuje krótki sygnał dźwiękowy oraz czerwony kolor wskaźnika świetlnego. Należy wówczas sprawdzić, czy identyfikator został zarejestrowany w systemie. Komunikat jest wyświetlany przez 4 sekundy lub do momentu wciśnięcia przycisku wyboru trybu.
- W przypadku próby rejestracji identyfikatorem z poza systemu, na ekranie rejestratora wyświetlana jest informacja „Karta obca”, o wystąpieniu takiego błędu dodatkowo informuje krótki sygnał dźwiękowy

oraz czerwony kolor wskaźnika świetlnego. Komunikat jest wyświetlany przez 4 sekundy lub do momentu wciśnięcia przycisku wyboru trybu.

- Jeżeli następuje zapełnienie pamięci rejestracji: dostęp jest przyznawany normalnie, ale rejestracje nie są zapisywane; podczas zaliczenia przejścia dla uprawnionego identyfikatora wyświetlany jest komunikat: „Brak pamięci dla rejestracji”. Pozostałe zdarzenia skutkujące normalnie zapisem rejestracji nie są rejestrowane, bez ograniczenia zachowań odpowiednich dla danych zdarzeń.