

Znak sprawy: DZP.261.1.29.2025

Załącznik nr 14 do SWZ

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

### Spis treści

I.	Wstęp .....	3
II.	Podział projektu na części i zadania projektowe, zestawienie ilościowe .....	3
III.	Część nr 1 .....	6
1.1	Rozszerzenie funkcjonalności EDM o nowe dokumenty ustawowe (+9).....	6
1.2	Rozbudowa repozytoriów medycznych .....	7
	Zakup licencji na integrację oprogramowania AMMS z systemami centralnymi wraz w wdrożeniem: .....	7
1.2.1	Rejestr Endoprotezoplastyk .....	7
1.2.3	Ankieta SIMP .....	11
1.2.4	Narzędzie pozwalające wizualizować w sposób graficzny dane gromadzone w różnych systemach medycznych. ....	13
IV.	Część nr 2 .....	21
1.3	Rozbudowa Sieci .....	21
	Zakup nowych przełączników FC-2 szt. ....	21
	Przełączniki PoE 14 szt. ....	23
	Rozbudowa sieci WiFi (Punkty AP WiFi 6) .....	24
	Kontroler Sieci WiFi.....	25
1.5	Rozbudowa hurtowni danych poprzez rozbudowę istniejących macierzy (2 macierze Dell Unity 380F).....	26
1.6	Zakup serwerów wraz z systemem operacyjnym oraz licencjami dostępowymi z kartami FC do podłączenia do macierzy oraz systemem wirtualizacji .....	29
1.6	Zakup stacji roboczych tj. PC z systemami operacyjnymi oraz terminali tj tzw. cienki klient, laptopów oraz monitorów .....	39
1.13	Komputery medyczne. Panelowy komputer medyczny AIO specjalnie zaprojektowany do pracy w środowiskach medycznych, takich jak szpitale na salach operacyjnych, z powłoką antybakteryjną do użytku medycznego. ....	53
3.6	Segmentacja sieci, system NAC .....	54
3.8	Instalacja i konfiguracja systemu monitorowania infrastruktury IT (co najmniej 100 urządzeń) – rozwiązanie klasy enterprise obsługi problemów z urządzeniami sieciowymi oraz infrastrukturą krytyczną i powiadomienia o tym odpowiednio użytkownika .....	60
3.9	Zakup systemu klasy SIEM- wyposażonego w zautomatyzowane, pasywne i aktywne mechanizmy inwentaryzacji zasobów IT i mapowania sieci. ....	62

3.10 Zakup oprogramowania do wykonywania kopii bezpieczeństwa 15 maszyn wirtualnych ..	77
3.11 Macierz do przechowywania kopii zapasowych danych medycznych oraz obrazowych o pojemności 100TB.....	81
1.6 Zakup usługi kopia w chmurze dla newralgicznych systemów .....	83
V. Część nr 3 .....	85
Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, "Ekran dotykowy 13,3 " (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" oraz licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożenie oprogramowania oraz urządzeń mobilnych .....	85
1.8 Zakup urządzeń mobilnych.....	85
1.9 Zakup czytników z podwójnym interfejsem. e-Dowody oraz stykowych kart procesorowych (np. podpis elektroniczny) Czytnik musi spełniać wymagania techniczne wskazane przez MSWiA dla czytników e-Dowodów bez PINPADu. ....	85
1.10 Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, "Ekran dotykowy 13,3 " (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" oraz licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożenie oprogramowania. ....	86
1.10.8 Prawo weryfikacji oferowanego rozwiązania.....	<b>Błąd! Nie zdefiniowano zakładki.</b>
VI. Część nr 4.....	94
2.1 Zakup oprogramowania do integracji urządzeń z system AMMS w zakresie skanowanej dokumentacji papierowej w tym kart informacyjnych.....	94
2.3 Zakup oprogramowania do integracji z CeZ w zakresie digitalizacji karty leczenia - Ucyfrowienie oraz indeksacja.....	100
2.4 Wdrożenie oprogramowania.....	100
2.5 Zakup urządzeń do skanowania dokumentacji papierowej do postaci cyfrowej Urządzenie umożliwiające integrację z systemem szpitalnym .....	101
VII. Część nr 5 .....	105
Zakup rozwiązania integracyjnego PUI (Platformy Usług Inteligentnych).....	105
VIII. Część nr 6 .....	106
1.14 System telekonsultacji dostarczony na zasadach SaaS lub Managed Service, umożliwiający zdalną ocenę badań obrazowych w chmurze oraz przekazywanie opisów w standardzie HL7 CDA. ....	106
IX. Część nr 7 .....	108
3.5 Zakup platformy do kompleksowej ochrony z XDR zapobiegająca naruszeniom bezpieczeństwa oraz skanowanie podatności oraz Sandboxing.....	108
X. Część nr 8 .....	126
3.1 Podwójna autentykacja w logowaniu do głównych systemów szpitala w których przechowywane są dane osobowe oraz dane medyczne .....	126

## **I. Wstęp**

**Opis przedmioty zamówienia dla projektu KPO D1.1.2 „Wdrożenie e-usług w Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Leżajsku” w Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Leżajsku (Szpital p.w. Matki Bożej Pocieszenia Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Leżajsku)**

Zakres przedsięwzięcia obejmuje utrzymanie lub aktualizację lub rozbudowę urządzeń i systemów, przedłużenia posiadanych już licencji lub subskrypcji oraz wsparcia dla posiadanych urządzeń lub systemów, służących wytwarzaniu lub przetwarzaniu elektronicznej dokumentacji medycznej oraz przekazywaniu danych do systemu P1 lub NFZ w okresie trwałości przedsięwzięcia.

Postępowanie realizowane jest w czterech obszarach zdefiniowanych w projekcie :

1. Integracja i rozbudowa systemów informatycznych świadczeniobiorcy
2. Digitalizacja dokumentacji medycznej istotnej z punktu widzenia leczenia i profilaktyki.
3. Działania zwiększające poziom cyberbezpieczeństwa szpitala.
4. Wdrożenie rozwiązań AI i podłączenie do Centralnego Repozytorium danych medycznych.

## **II. Podział projektu na części i zadania projektowe, zestawienie ilościowe**

### **Część nr 1**

<b>Numer zadania we wniosku</b>	<b>Zadanie 1 Integracja i rozbudowa systemów informatycznych świadczeniodawcy</b>	
1.1	Rozszerzenie funkcjonalności EDM o nowe dokumenty ustawowe (+9) 1. e-wyniki i opisy badań histopatologicznych 2. e-wyniki i opisy badań cytologicznych 3. karta diagnostyki i leczenia onkologicznego (e-DILO) 4. plan leczenia onkologicznego 5. Patent Summary (Karta zdrowia pacjenta) 6. karta opieki kardiologicznej (e-KOK) 7. karta medycznych czynności ratunkowych 8. karta medyczna lotniczego zespołu ratownictwa medycznego 9. dokumenty medycyny pracy (dokument orzeczenia lekarskiego oraz wytyczne wynikające z warunków pracy lub stanowiska pracy)	kpl
1.2	Rozbudowa repozytoriów medycznych Zakup licencji na integrację oprogramowania AMMS z systemami centralnymi wraz w wdrożeniem	Kpl.
1.2.1	Rejestr Endoprotezoplastyk	1
1.2.2	Ankieta Udarowa	1
1.2.3	Ankieta SIMP	1
1.2.4	Narzędzie pozwalające wizualizować w sposób graficzny dane gromadzone w różnych systemach medycznych.	1

### **Część nr 2: Sprzęt:**

	<b>Zadanie 1 Integracja i rozbudowa systemów informatycznych świadczeniodawcy</b>	
1.3.1	Zakup nowych przełączników sieciowych	14 szt.
1.3.2	Rozbudowa sieci WiFi (Punkty AP WiFi 6)	100 szt.
1.3.3	Kontroler Sieci WiFi	1 szt.
1.3.4	Przełączniki FC do budowy sieci SAN	2 szt.
1.5	Rozbudowa hurtowni danych poprzez rozbudowę istniejących macierzy (2 macierze Dell Unity 380F) o 30 TB.	2 szt.
1.6	Zakup serwerów wraz z systemem operacyjnym – serwery 2-procesorowych, 512 GB pamięci RAM każdy z kartami FC do podłączenia do macierzy oraz systemem wirtualizacji	4 szt.
1.7.1	Zakup stacji roboczych tj. PC z systemami operacyjnymi oraz terminali tj. tzw. cienki klient.	Kpl.
1.7.2	Terminale 8GB RAM, 64GB pamięci eMMC, zintegrowana karta graficzna	200 szt.
1.7.3	Komputery PC proces 14 rdzeniowy, 16GB RAM, Dysk SSD512GB, System Win11P.	120 szt.
1.7.4	Monitory 24" 1920x1080 100Hz	50 szt.
1.7.5	Monitory 55" 3640x 2160 60Hz, moduł Wi-Fi/Bluetooth	15 szt.
1.7.6	Laptopy 15.6" proc.10rdz. 16GB RAM	31 szt.
1.13	Komputery medyczne. Panelowy komputer medyczny AIO specjalnie zaprojektowany do pracy w środowiskach medycznych, takich jak szpitale na salach operacyjnych, z powłoką antybakteryjną do użytku medycznego.	5 szt.
<b>Zadanie 3: Działania zwiększające poziom cyberbezpieczeństwa szpitala</b>		
3.6	Segmentacja sieci, system NAC	1 kpl.
3.8	Instalacja i konfiguracja systemu monitorowania infrastruktury IT (co najmniej 100 urządzeń) – rozwiązanie klasy enterprise obsługi problemów z urządzeniami sieciowymi oraz infrastrukturą krytyczną i powiadomienia o tym odpowiednio użytkownika	1 kpl.
3.9	Zakup systemu klasy SIEM- wyposażonego w zautomatyzowane, pasywne i aktywne mechanizmy inwentaryzacji zasobów IT i mapowania sieci.	1 kpl.
3.10	Zakup oprogramowania do wykonywania kopii bezpieczeństwa 15 maszyn wirtualnych	1 kpl.
3.11	Zakup macierzy do przechowywania kopii zapasowych danych medycznych oraz obrazowych o pojemności 100TB	1 kpl.
3.12	Zakup usługi kopia w chmurze dla newralgicznych systemów	1 kpl.

### Część nr 3

<b>Zadanie 1 Integracja i rozbudowa systemów informatycznych świadczeniodawcy</b>		
Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, "Ekran dotykowy 13,3 " (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" oraz licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożeniem oprogramowania oraz urządzeń mobilnych		
1.8	Zakup urządzeń mobilnych tj. tabletów Ekran: 12,4 ", TFT, 2304 x 1440 pikseli, System operacyjny: Android 13, Pamięć RAM i dysk: 6 GB RAM + dysk 128 GB,	12 szt.
1.9	Zakup czytników z podwójnym interfejsem. e-Dowody oraz stykowych kart procesorowych (np. podpis elektroniczny) Czytnik musi spełniać wymagania techniczne wskazane przez MSWiA dla czytników e-Dowodów bez PINPADu	20 szt.
1.10	Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, "Ekran dotykowy 13,3 " (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" oraz licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożeniem oprogramowania. Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, 2 szt. "Ekran Wacom DTH134W5Z 13,3" (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" 5 szt.	1 kpl.

### Część nr 4

#### **Zadanie 2 Digitalizacja dokumentacji medycznej istotnej z punktu widzenia leczenia i profilaktyki**

2.1	Zakup oprogramowania do integracji urządzeń skanujących z system HIS-AMMS w zakresie skanowanej dokumentacji papierowej w tym kart informacyjnych.
2.2	Zakup oprogramowania do zarządzania medyczną dokumentacją elektroniczną w zakresie archiwizacji oraz Zarządzania dokumentacją medyczną (papierową i elektroniczną), w szczególności w zakresie udostępniania dokumentacji oraz jej brakowania.
2.3	Zakup oprogramowania do integracji z CeZ w zakresie digitalizacji karty leczenia - Ucyfrowienie oraz indeksacja
2.4	Koszty wdrożenia oprogramowania
2.5	Zakup urządzeń do skanowania dokumentacji papierowej do postaci cyfrowej Urządzenie umożliwiające integrację z systemem szpitalnym

#### Część nr 5

<b>Zadanie 4. Zakup rozwiązania integracyjnego PUI (Platformy Usług Inteligentnych)</b>		
4.1	Zakup rozwiązania integracyjnego PUI (Platformy Usług Inteligentnych) Opis i uzasadnienie: zakup oprogramowania integrującego HIS, RIS z Platformą Usług Inteligentnych, co umożliwi przesyłanie danych obrazowych i wykorzystanie rozwiązań AI.	1 kpl.
4.2	Wdrożenie testowanie i zatwierdzenie działania platformy przez Centrum e-Zdrowia Opis i uzasadnienie: przekazanie co najmniej jednego badania obrazowego do PUI oraz uzyskanie potwierdzenia od Centrum e-Zdrowia, co jest warunkiem osiągnięcia wskaźnika projektu.	1 kpl.

#### Część nr 6

<b>Zadanie 1 Integracja i rozbudowa systemów informatycznych świadczeniodawcy</b>		
1.14	System telekonsultacji dostarczony na zasadach SaaS lub Managed Service, umożliwiający zdalną ocenę badań obrazowych w chmurze oraz przekazywanie opisów w standardzie HL7 CDA.	Kpl.

#### Część nr 7

<b>Zadanie 3: Działania zwiększające poziom cyberbezpieczeństwa szpitala</b>		
3.5	Zakup platformy do kompleksowej ochrony z XDR zapobiegająca naruszeniom bezpieczeństwa oraz skanowanie podatności oraz Sandboxing.	1 kpl.

#### Część nr 8

<b>Zadanie 3: Działania zwiększające poziom cyberbezpieczeństwa szpitala</b>		
3.1	Podwójna autentykacja w logowaniu do głównych systemów szpitala w których przechowywane są dane osobowe oraz dane medyczne	1 kpl.

### **III. Część nr 1**

#### **1.1 Rozszerzenie funkcjonalności EDM o nowe dokumenty ustawowe (+9)**

**1. Opis funkcjonalności oraz zależności w ramach modułu, w podziale:**

Wymagania funkcjonalne:

System musi posiadać możliwość generowania poniższych dokumentów w postaci elektronicznej, zgodnie z obowiązującym standardem i obowiązującymi przepisami prawa (o ile przepisy nie wskazują, że dokumenty są generowane poza systemem HIS):

- 1) opisy badań histopatologicznych,
- 2) opisy badań cytologicznych,
- 3) karta diagnostyki i leczenia onkologicznego (e-DILO),
- 4) plan leczenia onkologicznego,
- 5) Patient Summary (Karta zdrowia pacjenta),
- 6) karta opieki kardiologicznej (e-KOK),
- 7) karta medycznych czynności ratunkowych,
- 8) karta medyczna lotniczego zespołu ratownictwa medycznego,
- 9) dokumenty medycyny pracy (dokument orzeczenia lekarskiego oraz wytyczne wynikające z warunków pracy lub stanowiska pracy).

System musi umożliwiać integrację z Platformą P1 w zakresie poniżej wskazanych typów dokumentów:

- 1) e-wyniki i opisy badań histopatologicznych,
- 2) e-wyniki i opisy badań cytologicznych,
- 3) karta diagnostyki i leczenia onkologicznego (e-DILO),
- 4) plan leczenia onkologicznego,
- 5) Patient Summary (Karta zdrowia pacjenta),
- 6) karta opieki kardiologicznej (e-KOK),
- 7) karta medycznych czynności ratunkowych,
- 8) karta medyczna lotniczego zespołu ratownictwa medycznego,
- 9) dokumenty medycyny pracy (dokument orzeczenia lekarskiego oraz wytyczne wynikające z warunków pracy lub stanowiska pracy).

System musi umożliwiać monitorowanie stanu indeksacji dokumentów w P1 na poziomie zbiorczych statystyk (z dokładnością do typu dokumentu i przedziału czasowego) oraz poszczególnych dokumentów w szczególności monitorowanie zwiększenia poziomu zaindeksowanej EDM w zakresie wyników badań laboratoryjnych lub opisów badań diagnostycznych w P1 celem wykazania wzrostu procentowego lub liczbowego.

Wewnętrzne integracje:

W realizacji procesów objętych produktem biorą udział komponenty HIS, repozytorium EDM oraz komponenty brzegowe odpowiedzialne bezpośrednio za integrację z systemem P1

Zewnętrzne integracje:

Rozwiązanie obejmuje integrację z systemem P1 w zakresie związanym z obsługą i wymianą ww. dokumentów (usługi z zakresu ogólnej wymiany EDM lub usługi dedykowane dla danego typu dokumentu – jak np. usługa generacji Patient Summary, Karta eDiLO).

Zależności między modułami:

Funkcjonalność opiera się na systemie HIS zintegrowanym z repozytorium EDM oraz komponentami odpowiedzialnymi za komunikację z P1.

## 2. Wymagania do uruchomienia produktu

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

Warunki startowe (minimalna wersja HIS):

- 1) Licencja na funkcjonalność
- 2) Działająca integracja z systemem P1 w zakresie wymiany EDM

Wymagania techniczne:

W zakresie KSO – zapewnienie zasobów dla komponentu odpowiedzialnego za komunikację z usługami FHIR (wymagania jak dla komponentu brzegowego Zdarzeń Medycznych). W pozostałym zakresie rozwiązanie opiera się o istniejące komponenty. W przypadku braku jakichkolwiek rezerw wydajnościowych na maszynach obsługujących instalacje AMDX i komponent P1 adapter, zalecane jest zwiększenie zasobów o około 10%.

Wymagania organizacyjne:

Podmiot zintegrowany z platformą P1 (w szczególności aktywne konto podmiotu w P1 i aktualne certyfikaty dostępowe).

## 3. Opis wdrożenia

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

- 1) Instalacja komponentów odpowiedzialnych za integrację z usługami FHIR w zakresie KSO
- 2) Uzupełnienie konfiguracji zgodnie z dostarczoną dokumentacją (np. ustawienie adresów nowych usług P1)

## 4. Kryteria odbioru produktu

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru.

Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

- 1) Umożliwia wygenerowanie dokumentów zgodnie z obowiązującym formatem (w zakresie przyporządkowanym do systemu HIS; np. dokument Patient Summary jest generowany po stronie systemu P1).
- 2) Umożliwia przekazywanie dokumentów lub ich indeksów do systemu P1 (w zależności od usług dostępnych dla danego typu dokumentu).
- 3) Umożliwia wyszukiwanie i pobieranie w ramach platformy P1 dokumentów wymienionych typów (w zależności od usług dostępnych dla danego typu dokumentu).
- 4) Daje możliwość dostępu do statystyk wykorzystania poszczególnych usług centralnych, w szczególności umożliwia monitorowanie zwiększenia poziomu zaindeksowanej EDM w zakresie wyników badań laboratoryjnych lub opisów badań diagnostycznych.
- 5) Umożliwia wymianę danych w standardzie FHIR w zakresie KSO (karta eDiLO i plan leczenia onkologicznego).

### 1.2 Rozbudowa repozytoriów medycznych

*Zakup licencji na integrację oprogramowania AMMS z systemami centralnymi wraz w wdrożeniem:*

#### *1.2.1 Rejestr Endoprotezoplastyk*

### 1. Wymagania funkcjonalne

Opis wszystkich funkcjonalności oraz zależności w ramach modułu, w podziale:



System musi zapewniać ewidencję danych Ankiety endoprotezoplastyki – pełnej.

- 1) Ewidencja 3 rodzajów Ankiety pełnej tj. rozliczeniowa, rozliczeniowa - inna grupa JGP, statystyczna.
- 2) Kopiowanie leków stale przyjmowanych, podanych, wystawionych na receptę, kopiowanie zaleceń lekarskich, wystawionych skierowań na rehabilitację w ramach pobytu pacjenta w szpitalu.
- 3) Podpowiadanie danych w Ankiecie endoprotezoplastyki dotyczących poprzedniego i następnego pobytu, jednostkowych danych medycznych (waga, wzrost, BMI), daty operacji i operatora, daty operacji pierwotnej i miejsca wykonania.
- 4) Autoryzowanie danych oraz podpisanie w postaci elektronicznej Ankiety endoprotezoplastyki.

System musi zapewniać komunikację z systemem Rejestr Endoprotezoplastyki (RE) prowadzonym przez NFZ.

- 1) Logowanie do RE, w celu uwierzytelnienia i autoryzacji.
- 2) Wysyłka Ankiety endoprotezoplastyki - pełnej w wersji roboczej oraz oficjalnej.
- 3) Obsługa błędów z RE.
- 4) Wysyłka korekty Ankiety endoprotezoplastyki – pełnej.
- 5) Wysyłka anulowania wersji roboczej Ankiety endoprotezoplastyki - pełnej w RE.
- 6) Import słowników z systemu RE.

Integracje (wewnętrzne oraz zewnętrzne):

Wewnętrzne: Brak.

Zewnętrzne:

- 1) Produkt integruje się z zewnętrznym systemem Rejestr Endoprotezoplastyki (RE) w celu przekazywania danych dot. wszczepów endoprotez stawowych.
- 2) Komunikacja z systemem RE odbywa się poprzez API SOAP oraz platformę integracyjną HIS – moduł ENDO.
- 3) Zawartość ankiety przekazywana jest za pośrednictwem usług udostępnionych przez NFZ w formie dokumentu XML.

Zależności między modułami:

- 1) Funkcjonalność korzysta z danych hospitalizacji pacjenta m.in. w zakresie danych przyjęcia do szpitala (skierowanie, tryb przyjęcia), wyników badań, podań leków, zleceń/recept na produkty lecznicze, zaleceń lekarskich, skierowań na rehabilitację wprowadzonych w modułach Izba Przyjęć HIS oraz Oddział HIS.
- 2) Funkcjonalność korzysta z danych dot. zabiegu endoprotezoplastyki rejestrowanych w modułach Blok operacyjny HIS lub Oddział HIS.
- 3) Zbiór podgląd ankiet możliwy jest z poziomu modułów Oddział HIS oraz Statystyka RCH HIS.
- 4) Integracja z systemem RE oparta jest o konfigurację komunikacji z NFZ określoną w module Panel administracyjny HIS.

## 2. Wymagania do uruchomienia produktu

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

Warunki startowe (minimalna wersja HIS):

- 1) Licencja
- 2) Działająca komunikacja z NFZ.
- 3) Prawidłowo skonfigurowane logowanie do NFZ.
- 4) Import słowników z RE.

Wymagania techniczne: Instalacja Platformy Integracyjnej

Wymagania organizacyjne:



- 1) Ankiety pełne dotyczą wszczepów realizowanych w ramach umowy z NFZ. Jednostka musi mieć aktywną umowę z NFZ w zakresie realizacji endoprotez stawowych.
- 2) Nadanie uprawnień operatorom – administratorom
- 3) Nadanie uprawnień w systemie HIS – Odczyt / Wpis / Autoryzacja / Modyfikacja.

### 3. Opis wdrożenia

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

- 1) Platforma Integracyjna – instalacja usługi
- 2) Wgranie licencji
- 3) Weryfikacja konfiguracji komunikacji z NFZ.
- 4) Weryfikacja / konfiguracja logowania do NFZ – System / Użytkownik.
- 5) Import słowników z RE.
- 6) Nadanie uprawnień – Odczyt / Wpis / Autoryzacja / Modyfikacja.
- 7) Ustawienie parametrów systemowych
- 8) Konfiguracja dokumentacji medycznej

### 4. Kryteria odbioru produktu

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru:

Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

- 1) Umożliwia tworzenie, edycję Ankiety endoprotezoplastyki:
  - a) pełnej w 3 rodzajach tj. rozliczeniowa, rozliczeniowa inna grupa JGP, statystyczna.
- 2) Umożliwia kopiowanie leków stale przyjmowanych, podanych, wystawionych na recepcie, kopiowanie zaleceń lekarskich, wystawionych skierowań na rehabilitację w ramach pobytu pacjenta w szpitalu.
- 3) Podpowiadane są dane dotyczące poprzedniego i następnego pobytu, wyników pomiarów (waga, wzrost, BMI), daty operacji i operatora, daty operacji pierwotnej i miejsca wykonania.
- 4) Umożliwia autoryzację danych oraz podpisanie Ankiety endoprotezoplastyki.
- 5) Zapewnia komunikację z systemem Rejestr Endoprotezoplastyki (RE).
- 6) Umożliwia wysyłkę Ankiety w wersji roboczej oraz oficjalnej.
- 7) Poprawnie prezentuje wynik komunikacji z systemu RE.
- 8) Umożliwia wysyłkę korekty Ankiety.
- 9) Umożliwia anulowanie wersji roboczej dokumentu.
- 10) Obsługuje import słowników z systemu RE.
- 11) Umożliwia zbiorczy przegląd Ankiet endoprotezoplastyki.

#### 1.2.4 Ankieta Udarowa

##### 1. Wymagania funkcjonalne

Opis wszystkich funkcjonalności oraz zależności w ramach modułu, w podziale:

##### Wymagania funkcjonalne

System musi zapewniać ewidencję danych Ankiety udarowej:

- 1) Ewidencja Ankiety udarowej w 4 modelach obsługi: z trombektomią mechaniczną, bez trombektomii, z przekazaniem na trombektomię, ze skierowaniem na trombektomię przez inny szpital.
- 2) Podpowiadanie danych w Ankiecie udarowej dotyczących przybycia pacjenta do szpitala, badań diagnostycznych mózgu, zastosowanego leczenia, danych trombektomii mechanicznej, daty rehabilitacji, danych wypisowych w przypadku zgonu.
- 3) Autoryzowanie danych oraz podpisanie w postaci elektronicznej Ankiety udarowej.

System musi zapewniać komunikację z systemem Ankiety Medyczne (AM) prowadzonym przez NFZ:

- 1) Logowanie do AM, w celu uwierzytelnienia i autoryzacji.
- 2) Wysyłka Ankiety udarowej w wersji roboczej oraz oficjalnej.
- 3) Obsługa błędów z AM.
- 4) Wysyłka korekty Ankiety udarowej.
- 5) Wysyłka anulowania Ankiety udarowej do AM.
- 6) Wywołanie Ankiety z systemu HIS w systemie AM.

Integracje (wewnętrzne oraz zewnętrzne):

Wewnętrzne: Brak.

Zewnętrzne:

- 1) Produkt integruje się z zewnętrznym systemem Ankiety Medyczne (AM) w celu przekazywania danych dot. leczenia pacjentów z udarem mózgu, w tym pacjentów których poddano zabiegowi trombektomii mechanicznej.
- 2) Komunikacja z systemem AM odbywa się poprzez API SOAP oraz platformę integracyjną HIS – moduł RAUT.
- 3) Zawartość ankiety przekazywana jest za pośrednictwem usług udostępnionych przez NFZ w formie dokumentu XML.

Zależności między modułami:

- 1) Funkcjonalność korzysta z danych hospitalizacji pacjenta m.in. w zakresie danych przyjęcia do szpitala (skierowanie, tryb przyjęcia), rozpoznania, wyników badań diagnostycznych, zastosowanego leczenia, rehabilitacji, danych wypisowych w przypadku zgonu wprowadzonych w module Izba Przyjęć HIS oraz Oddział HIS.
- 2) Funkcjonalność korzysta z danych dot. zabiegu trombektomii mechanicznej rejestrowanych w module Blok operacyjny HIS lub Oddział HIS.
- 3) Zbiórczy podgląd ankiet możliwy jest z poziomu modułu Oddział HIS oraz Statystyka RCH HIS.
- 4) Integracja z systemem AM oparta jest o konfigurację komunikacji z NFZ określoną w module Panel administracyjny HIS.

## 2. Wymagania do uruchomienia produktu

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

Warunki startowe (minimalna wersja AMMS)

- 1) Licencja
- 2) Działająca komunikacja z NFZ.
- 3) Prawidłowo skonfigurowane logowanie do NFZ.

Wymagania techniczne: Instalacja Platformy Integracyjnej

Wymagania organizacyjne:

- 1) Jednostka musi mieć aktywną umowę z NFZ w rodzaju lecznictwo szpitalne lub umowę podstawowego systemu zabezpieczenia szpitalnego oraz wykonywać zabiegi trombektomii mechanicznej.
- 2) Nadanie uprawnień operatorom – administratorom w Portalu SZOI/Portalu
- 3) Świadczeniodawcy oraz nadanie uprawnień operatorom w systemie centralnym KAAS-MGRSYS do systemu AM.
- 4) Nadanie uprawnień do Ankiety udarowej w systemie HIS – Odczyt / Wpis / Autoryzacja / Modyfikacja.

### 3. Opis wdrożenia

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

- 1) Platforma Integracyjna – instalacja usługi, zmiana adresów usług na środowisko produkcyjne.
- 2) Wgranie licencji
- 3) Weryfikacja konfiguracji komunikacji z NFZ.
- 4) Weryfikacja / konfiguracja logowania do NFZ – System / Użytkownik.
- 5) Weryfikacja konfiguracji JOS.
- 6) Nadanie uprawnień – Odczyt / Wpis / Autoryzacja / Modyfikacja.
- 7) Ustawienie parametrów systemowych:
- 8) Konfiguracja dokumentacji medycznej.

### 4. Kryteria odbioru produktu

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru:

Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

- 1) Umożliwia tworzenie, edycję Ankiety udarowej w 4 modelach obsługi: z trombektomią mechaniczną, bez trombektomii, z przekazaniem na trombektomię, ze skierowaniem na trombektomię przez inny szpital.
- 2) Umożliwia podpowiadanie danych w Ankiecie udarowej dotyczących przybycia pacjenta do szpitala, badań diagnostycznych mózgu, zastosowanego leczenia, danych trombektomii mechanicznej, rehabilitacji, danych wypisowych w przypadku zgonu.
- 3) Umożliwia autoryzację danych oraz podpisanie Ankiety endoprotezoplastyki.
- 4) Zapewnia komunikację z systemem Ankiety Medyczne (AM).
- 5) Umożliwia wysyłkę Ankiety w wersji roboczej oraz oficjalnej.
- 6) Poprawnie prezentuje wynik komunikacji z systemem AM.
- 7) Umożliwia wysyłkę korekty Ankiety.
- 8) Umożliwia anulowanie dokumentu.
- 9) Umożliwia podgląd danych zabiegu trombektomii zrealizowanego w ramach Bloku operacyjnego.
- 10) Pozwala na bezpośrednie przejście do ankiety w systemie AM.
- 11) Umożliwia zbiorczy przegląd Ankiety udarowych.

#### *1.2.3 Ankieta SIMP*

##### 1. Wymagania funkcjonalne

Opis wszystkich funkcjonalności oraz zależności w ramach modułu, w podziale:

Wymagania funkcjonalne:

- 1) System musi umożliwiać gromadzenie i przetwarzanie danych o zrealizowanych badaniach w ramach programów profilaktycznych NFZ – Profilaktyka chorób układu krążenia oraz Profilaktyka raka piersi.
- 2) System musi zapewniać walidację danych na poziomie systemu HIS. o System musi wspierać wypełnianie ankiet danymi pacjenta zaewidencjonowanymi w systemie HIS, w tym danymi osobowymi pacjenta, wynikami badań oraz pomiarów. o System musi umożliwiać ewidencję badań realizowanych w ramach programów profilaktycznych bez konieczności ręcznego wprowadzania danych na portalu SIMP.

Wewnętrzne integracje:

- 1) Dane do systemu SIMP są przekazywane za pośrednictwem Platformy Integracyjnej

Zewnętrzne integracje:

- 1) System Informatyczny Monitorowania Profilaktyki (SIMP) - dane z HIS przekazywane są do SIMP w postaci pliku XML za pośrednictwem usługi udostępnionej przez NFZ.

Zależności między modułami:

- 1) Funkcjonalność korzysta z danych osobowych pacjenta oraz z danych pobytu pacjenta w zakresie wyników badań i pomiarów.
- 2) Integracja z SIMP wykorzystuje konfigurację komunikacji z systemami NFZ definiowaną na poziomie HIS.

## 2. Wymagania do uruchomienia produktu

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

Warunki startowe

- 1) Licencja
- 2) Działająca komunikacja z NFZ
- 3) Skonfigurowanie w HIS danych do logowania do portalu SIMP

Wymagania techniczne:

- 1) Zainstalowany moduł (pakiet Usługi NFZ) wraz z podaniem aktualnego adresu środowiska.

Wymagania organizacyjne:

- 1) Jednostka musi mieć aktywną umowę z NFZ w zakresie realizacji Profilaktycznych programów zdrowotnych.
- 2) Nadanie uprawnień do eksportu w systemie HIS

## 3. Opis wdrożenia

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

- 1) Instalacja Platformy Integracyjnej z modulem
- 2) Wgranie do systemu HIS licencji
- 3) Weryfikacja konfiguracji komunikacji z NFZ.
- 4) Weryfikacja konfiguracji umów NFZ w zakresie:
  - o Dla ankiety mammograficznej:
    - 10.7940.159.02 w celu realizacji wizyt mobilnych (w mammobusie),
    - 10.7940.158.02 w celu realizacji wizyty stacjonarnej.
  - o Dla karty ChUK:
    - 01.0032.180.11 – zakres dla pielęgniarki.
    - 01.0010.107.11 – zakres dla lekarza.
- 5) Uzupełnienie parametrów dla każdego użytkownika, który będzie eksportował dane
- 6) Nadanie uprawnienia – „Eksport danych” (w kontekście jednostki ewidencjonującej realizację programu profilaktycznego) każdemu użytkownikowi, który będzie eksportował dane.
- 7) Konfiguracja dokumentacji medycznej w zakresie Karty ChUK i Ankiety mammograficznej.

## 4. Kryteria odbioru produktu

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru:

Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

- 1) Umożliwia zarejestrowanie i zaewidencjonowanie danych ankiety mammograficznej oraz karty ChUK.

- 2) Umożliwia podpowiadanie danych zaewidencjonowanych w systemie HIS (w zakresie danych osobowych, wyników badań i pomiarów).
- 3) Daje możliwość autoryzacji danych i podpisania ankiet.
- 4) Umożliwia zarejestrowanie badania w SIMP.
- 5) Pozwala na przesłanie i poprawne zapisanie danych zrealizowanego badania profilaktycznego w SIMP.
- 6) Umożliwia bieżącą weryfikację statusu badania w SIMP.
- 7) Poprawnie wyświetla wynik komunikacji z SIMP.
- 8) Umożliwia korektę błędnie przesłanej ankiety.

#### 1.2.4 Narzędzie pozwalające wizualizować w sposób graficzny dane gromadzone w różnych systemach medycznych.

##### 1. Wymagania funkcjonalne

1.1 Ogólne	
1.	Aplikacja posiada przeglądarkowy interfejs użytkownika.
2.	Aplikacja nie może wymagać od użytkownika instalacji dodatkowych wtyczek/rozszerzeń w przeglądarce.
3.	Aplikacja umożliwia obsługę w dwóch językach: polski oraz angielski.
4.	Aplikacja powinna być dostępna cyfrowo dla osób z niepełnosprawnościami, zapewniając zgodność z WCAG 2.1 (ang. Web Content Accessibility Guidelines) na poziomie AA.
5.	Aplikacja udostępnia syntetyczne analizy biznesowe w formie kokpitu menadżerskiego, składającego się z powiązanych tematycznie interaktywnych kafelków.
6.	Aplikacja umożliwia eksport danych do arkusza kalkulacyjnego z poziomu:
1)	Tabel drażeniowych kafelków
2)	Tabel przestawnych
3)	Danych elementarnych kafelków wykresowych
7.	Aplikacja umożliwia użytkownikowi wybór motywu z dostępnej listy motywów oraz zmianę tła pulpitu
8.	Aplikacja pozwala na prognozowanie wartości wskaźników finansowych na bazie danych historycznych w oparciu o liczbę okresów wstecz zdefiniowaną przez użytkownika
9.	Aplikacja udostępnia kafelki oraz tabele przestawne z zakresów:
1)	Statystyka medyczna,
2)	Rozliczenia NFZ,
3)	Finanse
4)	Koszty leczenia
5)	Procedury medyczne
10.	Aplikacja pozwala na możliwości ustawiania alarmów na kafelkach, celem sygnalizowania sytuacji niepożądanych, odbiegających od przyjętych standardów.
11.	Użytkownik ma możliwość zapisania wielu zestawu filtrów, które ustawił w ramach danego pulpitu /tabeli przestawnej, a następnie odtworzenia ich w dowolnym momencie w przyszłości wraz z opcją udostępniania zestawów innym użytkownikom
12.	Aplikacja pozwala na definiowanie miar użytkownika na tabelach przestawnych
13.	Dla każdego zakresu producent dostarcza co najmniej jeden predefiniowany pulpit (kokpit) przykładowy, gotowy do użycia. Pulpity predefiniowane powinny zapewniać przykładową formę prezentacji kompletu analiz dostępnych w aplikacji.
14.	Pulpity predefiniowane mogą być uruchamiane, kopiowane, ale nie mogą być usuwane ani edytowane przez żadnego użytkownika.
15.	Dostępne kafelki są predefiniowane przez producenta, tak aby rozwiązanie nie wymagało od użytkownika kompetencji w zakresie modelowania czy przetwarzania danych. Konfiguracja źródła danych i ich prezentacji jest zdefiniowana przez producenta.
16.	Praca w aplikacji nie wymaga znajomości modelu danych systemów dziedzinowych ERP i HIS.
17.	Dane prezentowane w kafelkach pobierane są bezpośrednio z systemów HIS i ERP (on-line) występujących u Zamawiającego, poprzez udostępniane funkcje lub widoki. W celu

	przyspieszenia działania aplikacji, dopuszcza się wykorzystywanie mechanizmu własnego magazynu danych, w którym dane z systemów HIS i ERP będą przechowywane.
18.	Informacja o źródle pochodzenia danych prezentowana jest bezpośrednio na każdym kafelku analitycznym indywidualnie, z rozróżnieniem na pobieranie bezpośrednio z systemów dziedzicznych (on-line) oraz pobieranie z własnego magazynu danych aplikacji. Informacja ta powinna być sygnalizowana w sposób wizualny (np. różny kolor ikony dotyczącej źródła danych), a także wystarczająco szczegółowa, w zależności od źródła danych. W przypadku danych pobieranych bezpośrednio niezbędna jest informacja o systemie, z którego dane są pobierane, zaś w przypadku pobierania z własnego magazynu danych prezentowane powinny być informacje o ostatnim czasie aktualizacji danych, w rozbiu na wszystkie okresy, które poddawane są analizie.
19.	Aplikacja zapewnia integrację kont użytkowników z systemami dziedzicznymi HIS i ERP.
20.	System umożliwia zabezpieczenie danych wrażliwych pozwalających zidentyfikować konkretnego pacjenta. Zabezpieczenie jest realizowane w formie uprawnienia dla wskazanych użytkowników. Zestaw anonimizowanych cech pacjenta obejmuje co najmniej: nazwisko, pierwsze imię, drugie imię, PESEL, data urodzenia, płeć, data zgonu, kraj pochodzenia, ubezpieczyciel.
21.	System udostępnia trzy poziomy uprawnnień użytkowników:
	1) Do funkcji – np. funkcji administratora czy dostępu do danych wrażliwych,
	2) Do grup kafelków,
	3) Do komórek organizacyjnych szpitala i ośrodków kosztów.
22.	System umożliwia użytkownikowi z uprawnieniami Administratora określanie (w minutach) maksymalnego czasu bezczynności użytkownika, po którym następuje wylogowanie.
23.	System umożliwia użytkownikowi z uprawnieniami Administratora określanie minimalnego analizowanego roku kalendarzowego, w ramach którego prowadzone mogą być analizy (tzn. na liście dostępnych lat kalendarzowych widoczny będzie ustawiony minimalny rok kalendarzowy oraz wszystkie następujące po nim lata aż do bieżącego).
24.	System umożliwia użytkownikowi z uprawnieniami Administratora określanie waluty wyświetlanej na kafelkach analitycznych.
25.	Użytkownik z uprawnieniami administratora ma możliwość określenia/zmiany identyfikatora układu bilansowego dla danych pochodzących z systemów finansowych.
26.	Aplikacja udostępnia analizy biznesowe w formie tabel przestawnych oraz posiada mechanizm generowania wykresu w czasie rzeczywistym, na podstawie ustawienia zawartości danej tabeli przestawnej.
27.	Użytkownik ma możliwość zapisywania zestawu filtrów które ustawił w ramach danej tabeli przestawnej a następnie odtworzenia ich w dowolnym momencie w przyszłości wraz z opcją udostępniania zestawów innym użytkownikom
28.	Informacja o źródle pochodzenia danych prezentowana jest bezpośrednio na każdej tabeli przestawnej, z rozróżnieniem na pobieranie bezpośrednio z systemów dziedzicznych (on-line) oraz pobieranie z własnego magazynu danych aplikacji. Informacja ta powinna być sygnalizowana w sposób wizualny (np. różny kolor ikony dotyczącej źródła danych), a także wystarczająco szczegółowa, w zależności od źródła danych.
29.	W przypadku danych pobieranych bezpośrednio niezbędna jest informacja o systemie, z którego dane są pobierane, zaś w przypadku pobierania z własnego magazynu danych prezentowane powinny być informacje o ostatnim czasie aktualizacji danych, w rozbiu na wszystkie okresy, które poddawane są analizie.
<b>1.2 Własny magazyn danych</b>	
1.	Aplikacja posiada wewnętrzny magazyn danych (cache) wykorzystywany jako źródło danych dla elementów obciążających bazy danych systemów dziedzicznych celem ich odciążenia oraz dostarczenia wyników użytkownikom w krótszym czasie.
2.	Użytkownik ma możliwość zarządzania zasileniami magazynu danych (cache) w zakresie dodawania nowych zadań (tzw. harmonogramów zasileń), edycji istniejących oraz usuwania już niepotrzebnych.
3.	Administrator systemu ma możliwość określania maksymalnego czasu wykonywania zasilenia magazynu danych, tzn. czasu, po którym niezakończone zasilenie w magazynie danych zostaje przerwane ze statusem "Niepowodzenie".
4.	Aplikacja pozwala na zdefiniowanie harmonogramów zasileń jednokrotnych, czyli uruchamianych jeden raz we wskazanym przez użytkownika momencie (możliwość określenia daty oraz godziny).



5.	Aplikacja pozwala na zdefiniowanie harmonogramów cyklicznych, uruchamianych wiele razy, zgodnie z zadaną przez użytkownika konfiguracją. Ta ostatnia powinna obejmować co najmniej:
1)	określenie, w jakich odstępach czasu będzie uruchamiane zasilanie (dostępne opcje: codziennie, co miesiąc)
2)	określenie, za jaki okres będą zasilane dane (dostępne opcje: miesiąc, rok)
3)	określenie, ile okresów wstecz w stosunku do momentu uruchomienia zasilania ma być załadowane do magazynu danych (np. dwa miesiące wstecz).
6.	Dla harmonogramów cyklicznych użytkownik ma możliwość podania okresu w jakim pozostaje aktywny (tylko w tym przedziale czasu będą uruchamiane procesy zasilania, zgodnie z parametrami określonymi przez użytkownika).
7.	Dostęp do funkcjonalności zasilania magazynu danych (cache) jest możliwy tylko dla użytkowników posiadających stosowne uprawnienia (administrator).
8.	Aplikacja daje możliwość przeglądu logu wykonanych zasilień magazynu danych (cache) obejmującego co najmniej informacje o: nazwie zasilanego zakresu danych, okresie, czasie trwania operacji, dacie rozpoczęcia i zakończenia, statusie zakończenia procesu (pomyślny/błędny).
<b>1.3 Mechanizm grupowania danych</b>	
1.	Aplikacja musi posiadać, niezależny od systemów źródłowych, mechanizm grupowania danych (pozycji wybranych słowników) wykorzystywany na części kafelków celem prezentacji danych w układzie zdefiniowanych przez użytkownika agregatów.
2.	Użytkownik ma możliwość zarządzania mechanizmem grupowania danych w zakresie tworzenia, usuwania oraz zmiany (słownika, grup przypisanych do słownika oraz pozycji przypisanych do grup słownika).
3.	Użytkownik może zdefiniować więcej niż jedną grupę dla danego słownika.
4.	Użytkownik może upublicznić zdefiniowaną przez siebie grupę, celem wykorzystania jej w analizach przez innych użytkowników.
5.	Upubliczniona grupa może być zarządzana tylko przez osobę, która ją utworzyła i upubliczniła.
6.	Mechanizm grupowania danych musi obejmować co najmniej:
1)	słownik zakresów świadczeń wykorzystywany przez szpital do rozliczeń z NFZ;
2)	słownik kosztów OPK pozwalający na grupowanie kosztów wg dwóch kryteriów: kosztów rodzajowych oraz OPK przekazujących (narzucających) koszty;
3)	słownik kont księgowych;
4)	słownik ośrodków kosztowych (OPK), umożliwiający analizę danych na poziomie ośrodków kosztowych w ujęciu poszczególnych OPK lub utworzonych grup (stanowiących jedną wspólną pozycję);
5)	słownik jednostek organizacyjnych szpitala (JOS), umożliwiający analizę danych na poziomie jednostek organizacyjnych w ujęciu poszczególnych JOS lub utworzonych grup (stanowiących jedną wspólną pozycję).
7.	Każde ze zdefiniowanych grupowań powinno mieć możliwość określenia okresu obowiązywania.
<b>1.4 Komponowanie własnych pulpitów</b>	
1.	Użytkownik ma możliwość stworzenia, nazwania i usunięcia własnego pulpitu.
2.	W momencie utworzenia pulpitu użytkownik staje się administratorem pulpitu.
3.	Użytkownik ma możliwość skopiowania dowolnego, dostępnego dla niego pulpitu, co skutkuje utworzeniem kopii danego pulpitu, dla której użytkownik kopiujący staje się administratorem (właścicielem).
4.	Administrator pulpitu określa komu może być udostępniony pulpit.
5.	Administrator pulpitu może przyznać prawo administratora pulpitu dla użytkownika, któremu udostępniono pulpit.
6.	Administrator pulpitu może określać tzw. siatkę pulpitu. Siatka pulpitu definiuje miejsca w których użytkownik może położyć kafelek. W ramach konfiguracji siatki można wskazać, z ilu kolumn ma się składać oraz określić wysokość wiersza.
7.	Administrator pulpitu może ułożyć wybrany przez siebie kafelek na pulpicie w taki sposób, że zajmuje on jeden lub wiele pól siatki pulpitu (skalowanie kafelka)
8.	Aplikacja umożliwia stworzenie pulpitu zawierającego kafelki z różnych obszarów.
9.	Aplikacja posiada bibliotekę predefiniowanych przez producenta kafelków, z których użytkownik może definiować swoje pulpity menedżerskie



10.	Wszystkie kafelki zawarte w bibliotece są opisane w sposób merytoryczny wraz z informacją, skąd pobierane są dane w celu łatwej weryfikacji zgodności danych z systemami źródłowymi
11.	Administrator pulpitu ma możliwość edycji tytułu kafelka położonego na pulpicie.
12.	Aplikacja posiada konfigurowalny mechanizm tzw. filtrów pulpitu, które pozwalają na ustawienie wartości filtrów na wielu kafelkach jednocześnie.
13.	Administrator (właściciel) pulpitu ma możliwość ustalenia, które z filtrów kafelka mają reagować na zmianę wartości w filtrze pulpitu, a które mają pozostać na nią nieczułe.
14.	Wybrane kafelki mają możliwość interakcji między sobą w taki sposób, że kliknięcie elementu na jednym kafelku może powodować automatyczne ustawienie filtra na drugim i jego odświeżenie.
15.	Administrator pulpitu decyduje, czy kafelek umożliwiający wysyłanie informacji o zaznaczonym obiekcie będzie wysyłać stosowną informację wyjściową oraz decyduje, które kafelki mające odpowiednie filtry mają reagować na taką akcję poprzez ustawienie swojego filtra.
<b>1.5 Drażenia danych</b>	
1.	System, dla wybranych kafelków, posiada mechanizm drażeń pozwalający na prezentację danych szczegółowych (elementarnych) w formie tabelarycznej.
2.	Mechanizm drażeń pozwala na interaktywną pracę z danymi elementarnymi tj. filtrowanie oraz grupowanie.
3.	Aplikacja umożliwia zapisanie danych elementarnych do arkusza kalkulacyjnego w celu ich dalszej obróbki.
<b>1.6 Zakres danych: Statystyka medyczna</b>	
1.	W ramach zakresu danych dotyczącego statystyki medycznej aplikacja udostępnia kafelki prezentujące informacje o:
1)	statystyce ruchu chorych:
a)	obłożenie łóżek - informacja dostępna na wskazany dzień oraz za wybrany okres (od dnia do dnia)
b)	liczba pacjentów, przyjęć i wypisów - informacja dostępna na wskazany dzień oraz za wybrany okres (od dnia do dnia) wraz ze śledzeniem trendu
c)	średnia długość pobytu
d)	histogram długości pobytów (w rozbiciu na zakończone, niezakończone, wszystkie)
e)	obłożenie oraz przelotowość łóżek - informacja dostępna na wskazany dzień oraz za wybrany okres (od dnia do dnia)
f)	rozkład liczby pacjentów w funkcji grupy JGP
2)	śmiertelności (z rozbiciem na przyczyny zgonu)
3)	wartość wykonanych świadczeń w wybranym okresie:
a)	łącznie dla wybranych oddziałów w okresie wybranym przez użytkownika
b)	w podziale na poszczególne dni wg daty realizacji świadczeń
c)	w podziale na JGP (wraz z informacją o liczbie pacjentów rozliczonych daną grupą)
4)	statystyce kolejek na ostatni dzień miesiąca oraz w wybranym okresie liczoną w miesiącach
5)	statystyce Triage
6)	zakażeniach szpitalnych
2.	W ramach zakresu danych dotyczącego statystyki medycznej aplikacja udostępnia tabele przestawne prezentujące dane z zakresu:
1)	Zdarzenia niepożądane
2)	Zgony
3)	Pobyty pacjentów
4)	Łóżka
3.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia), związanych z obłożeniem łóżek, poprzez drażenie do poziomu pobytów poszczególnych pacjentów.
4.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia), związanych ze statystyką pacjentów, poprzez drażenie do poziomu pobytów poszczególnych pacjentów.
5.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia), związanych z wartością wykonanych świadczeń w jednostce organizacyjnej szpitala, poprzez drażenie do poziomu pobytów poszczególnych pacjentów z uwzględnieniem zarówno przychodów z NFZ, jak i działalności komercyjnej.
6.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia) związanych ze zgonami, poprzez drażenie do poziomu pobytów poszczególnych pacjentów.

<b>1.7 Zakres danych: Rozliczenia NFZ</b>	
1.	W ramach zakresu danych dotyczącego rozliczeń z Narodowym Funduszem Zdrowia aplikacja udostępnia kafelki prezentujące informacje o:
1)	poziomie realizacji umów NFZ kwotowo lub punktowo (do wyboru przez użytkownika) w wybranym roku, w przekroju świadczeń wykonanych, rozliczonych i wynikających z limitów w planie umowy:
a)	jako udział wartości wykonanych i rozliczonych w wartości określonej limitem w planie umowy;
b)	dodatkowe ujęcie wartości średniej (dla wszystkich wyświetlanych umów) udziału procentowego wykonanych i wartości rozliczonych
2)	wybranej na zestawieniu zbiorczym umowie jako rozbieżności wartości wykonano, rozliczono i limit wynikający z planu umowy, na poszczególne miesiące w ujęciu narastającym (wartość dla danego miesiąca jest sumą tego miesiąca oraz miesięcy poprzedzających, a więc grudzień powinien reprezentować wartość tożsamą z całym rokiem) lub rozłącznie (każdy miesiąc ma swoją wartość, które po zsumowaniu dają wartość tożsamą z całym rokiem) - do wyboru przez użytkownika
3)	poziomie realizacji konkretnej umowy NFZ w rozbieżności na poszczególne jednostki organizacyjne szpitala kwotowo lub punktowo (do wyboru przez użytkownika), w wybranym roku, w przekroju świadczeń wykonanych i rozliczonych, w formie graficznej oraz tabelarycznie (postać tabelaryczna zawiera ujęcie średniej dla wszystkich wyświetlanych JOSów) – z możliwością ograniczenia danych do wybranych zakresów świadczeń;
4)	jednostce organizacyjnej szpitala wybranej na zestawieniu JOSów jako rozbieżności wartości wykonano i rozliczono, na poszczególne miesiące, w ujęciu narastającym (wartość dla danego miesiąca jest sumą tego miesiąca oraz miesięcy poprzedzających, a więc grudzień powinien reprezentować wartość tożsamą z całym rokiem lub rozłącznie (każdy miesiąc ma swoją wartość, które po zsumowaniu dają wartość tożsamą z całym rokiem) - do wyboru przez użytkownika
5)	poziomie realizacji grup zakresów świadczeń kwotowo lub punktowo (do wyboru przez użytkownika) w wybranym roku, w przekroju świadczeń wykonanych, rozliczonych i wynikających z limitów w planie umowy:
a)	jako udział wartości wykonanych i rozliczonych w wartości limitów wynikających z planu umowy;
b)	dodatkowe ujęcie wartości średniej (dla wszystkich wyświetlanych umów) udziału procentowego wykonanych i wartości rozliczonych
6)	grupie zakresów świadczeń wybranej na zestawieniu grup zakresów świadczeń jako rozbieżności wartości wykonano, rozliczono i wynikających z limitów w planie umowy, na poszczególne miesiące w ujęciu narastającym (wartość dla danego miesiąca jest sumą tego miesiąca oraz miesięcy poprzedzających, a więc grudzień powinien reprezentować wartość tożsamą z całym rokiem) lub rozłącznie (każdy miesiąc ma swoją wartość, które po zsumowaniu dają wartość tożsamą z całym rokiem) - do wyboru przez użytkownika
7)	procentowym rozkładzie grup zakresów świadczeń w wybranym miesiącu
a)	możliwość wybrania elementu/elementów wyświetlanych, które powinny zostać wyłączone z prezentowanego kafelka (w przypadku, gdy wybrany element będzie mocno dominował nad pozostałymi, użytkownik ma mieć możliwość zaznaczenia go jako nieujętego na kafelku)
8)	dodatkowe informacje zarządcze wskazujące zakresy świadczeń o najniższym i najwyższym procencie realizacji wynikającej z limitów w planie umowy (top n - liczba n ustalana przez użytkownika)
9)	współczynnika pacjentów rozliczonych (względem wykonanych) w wybranym okresie wraz z odniesieniem do średniej rocznej
2.	Aplikacja pozwala na przegląd szczegółowych danych (drażnienia), związanych z realizacją umów NFZ, poprzez dwustopniowe drażnienie. W pierwszym stopniu z dokładnością do poszczególnych zakresów świadczeń. W drugim stopniu z dokładnością do pacjentów z uwzględnieniem informacji o pozycjach rozliczeniowych oraz zestawach świadczeń.
3.	W ramach zakresu danych dotyczącego rozliczeń z Narodowym Funduszem Zdrowia aplikacja udostępnia tabele przestawne prezentujące dane z zakresu:
a.	Umowy NFZ w ujęciu planu, realizacji oraz rozliczenia prezentowane w ujęciu kwotowym jak i punktowym (do wyboru użytkownika)
b.	Realizacja świadczeń NFZ
<b>1.8 Zakres danych: Finanse</b>	

1.	W ramach zakresu danych dotyczącego finansów aplikacja udostępnia kafelki prezentujące informacje o:
1)	finansach podmiotu w rozbiciu na:
a)	należności, prezentując dane o stanie należności na koniec danego miesiąca oraz miesięcy historycznych, w rozbiciu na strukturę tych należności, z możliwością filtrowania do dokumentów zaksięgowanych/niezaksięgowanych
b)	zobowiązania, prezentując dane o stanie zobowiązań na koniec danego miesiąca oraz miesięcy historycznych, w rozbiciu na strukturę tych zobowiązań, z możliwością filtrowania do dokumentów zaksięgowanych/niezaksięgowanych
2)	finansach OPK w rozbiciu na:
a)	koszty OPK w funkcji czasu, prezentując zarówno koszty bezpośrednie w podziale na koszty bezpośrednie (rodzajowe), jak i koszty pośrednie (narzuty od konkretnych OPK); analiza związana z kosztami OPK powinna być rozszerzona o informacje o statystykach medycznych (np. liczba hospitalizacji, liczba osobodni, liczba porad)
b)	przychody OPK w poszczególnych miesiącach, w ujęciu narastającym (wartość dla danego miesiąca jest sumą tego miesiąca oraz miesięcy poprzedzających, a więc grudzień powinien reprezentować wartość tożsamą z całym rokiem) lub rozłącznie (każdy miesiąc ma swoją wartość, które po zsumowaniu dają wartość tożsamą z całym rokiem) – do wyboru przez użytkownika
c)	przychody OPK z uwzględnieniem ich struktury, czyli w podziale na zdefiniowane w systemie finansowo – księgowym konta księgowe
d)	wyniki OPK w czasie jako zestawieniu kosztów i przychodów danego OPK w rozbiciu na miesiące, wraz z informacją o wyniku finansowym (wyliczonym jako różnica pomiędzy sumą przychodów i kosztów); wynik OPK powinien być prezentowany na wykresie oraz w tabeli, w ujęciu narastającym (wartość dla danego miesiąca jest sumą tego miesiąca oraz miesięcy poprzedzających, a więc grudzień powinien reprezentować wartość tożsamą z całym rokiem) lub rozłącznie (każdy miesiąc ma swoją wartość, które po zsumowaniu dają wartość tożsamą z całym rokiem) – do wyboru przez użytkownika
3)	sytuacji finansowej całego podmiotu (wyliczone w oparciu o sprawozdania roczne, prowadzone w systemie FK) z możliwością określenia:
a)	okresu, rodzaju sprawozdania (zdefiniowanego oraz przeliczonego w systemie FK) oraz pozycji, które zostaną zaprezentowane na kafelku
b)	okresu referencyjnego (historycznego) z którym będą porównywane dane za okres bazowy
c)	formy prezentacji: jako pojedyncza wartość na wybrany rok/miesiąc lub w postaci trendu (wykresu za wskazany przez użytkownika okres)
4)	rozchodach magazynowych wraz z prognozą wygenerowaną na podstawie danych historycznych
5)	Koszty jednostkowe (średnie koszty) w wybranym czasie
2.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia), związanych z kosztami ośrodka OPK, z dokładnością do poziomu kosztów szczegółowych.
3.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia), związanych z przychodami ośrodka OPK, z dokładnością do poziomu kont księgowych.
4.	W ramach zakresu danych dotyczącego finansów aplikacja udostępnia tabele przestawne prezentujące dane z zakresu:
1)	Koszty OPK z wykorzystaniem mechanizmu grupowania z możliwością definiowania grup przez użytkownika. Dane prezentowane w układzie miesięcznym bądź narastającym
2)	amortyzacji środków trwałych, zarówno dla metody bilansowej jak i podatkowej
3)	informacje o kontrahentach oraz umowach komercyjnych
4)	informacje o rozpięciu (narzucie) kosztów danego OPK na ośrodki znajdujące się w jego planie podziału kosztów z możliwością dalszego ich rozbicia na koszty rodzajowe
5)	kosztu pustych łóżek
<b>1.9 Zakres danych: Koszty leczenia</b>	
1.	Wynik JGP w rozbiciu na:
1)	analizę porównawczą kosztów, przychodów i wyniku pomiędzy poszczególne JGP
2)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego JGP w podziale na pobyty
3)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego JGP w podziale na lekarza prowadzącego

4)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego JGP w podziale na rozpoznanie
2.	Wynik lekarza prowadzącego w rozbiciu na:
1)	analizę porównawczą kosztów, przychodów i wyniku pomiędzy poszczególnymi lekarzami prowadzącymi.
2)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego lekarza prowadzącego w podziale na pobyty
3)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego lekarza prowadzącego w podziale na JGP
4)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego lekarza prowadzącego w podziale na rozpoznanie
3.	Wynik rozpoznania ICD10 w rozbiciu na:
1)	analizę porównawczą kosztów, przychodów i wyniku pomiędzy poszczególnymi rozpoznaniem ICD10
2)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego rozpoznania ICD10 w podziale na pobyty
3)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego rozpoznania ICD10 w podziale na JGP
4)	analizę porównawczą kosztów, przychodów i wyniku poszczególnych przypadków dla wybranego rozpoznania ICD10 w podziale na lekarza prowadzącego
4.	Aplikacja pozwala na przegląd szczegółowych danych (drażenia), związanych z JGP, poprzez drażnienie do poziomu poszczególnych przypadków, z uwzględnieniem informacji o:
1)	czasie pobytu/hospitalizacji,
2)	kosztach w podziale na osobodzień, rozchody i procedury,
3)	lekarzu prowadzącym,
4)	JGP,
5)	trybie wypisu,
6)	trybie przyjęcia,
7)	JOS pobytu.
5.	Analizy wyniku dla JGP, lekarza prowadzącego oraz rozpoznania ICD10 pozwalają na porównywanie danych za wybrany przez użytkownika okres z danymi historycznymi
6.	Analizy wyniku dla JGP, lekarza prowadzącego oraz rozpoznania ICD10 mogą być zawężane do interesującej grupy przypadków. Zawężenie powinno być efektem świadomego ustawienia przez użytkownika odpowiednich filtrów dodatkowych, obejmujących co najmniej:
1)	tryb wypisu,
2)	tryb przyjęcia,
3)	pleć
4)	długość pobytu.
7.	W ramach zakresu danych dotyczącego kosztów leczenia aplikacja udostępnia tabele przestawne prezentujące dane z zakresu
1)	Kosztów hospitalizacji pacjentów w łącznym ujęciu wszystkich pobytów danego pacjenta w ramach danej hospitalizacji, w danej jednostce organizacyjnej (JOS).
<b>1.10 Zakres danych: Procedury medyczne</b>	
1.	W ramach zakresu danych dotyczącego procedur medycznych aplikacja udostępnia kafelki oraz tabele przestawne prezentujące informacje zarówno o procedurach z bloku operacyjnego jak i spoza bloku
<b>1.11 Specjalne</b>	
1.	Aplikacja udostępnia kafelek prezentujący zawartość wprowadzoną przez użytkownika z wykorzystaniem wbudowanego edytora tekstowego.

## 1.10 OPIS WDROŻENIA

Element wdrożenia	Zakres prac
-------------------	-------------

Konfiguracja i instalacja	<p>Wsparcie w przygotowaniu środowiska dla aplikacji; zainstalowanie i skonfigurowanie systemu.</p> <p>Etap powinien być poprzedzony przygotowaniem środowiska sieciowego, w zakresie:</p> <ul style="list-style-type: none"> <li>a) Serwer aplikacji z minimalnymi wymaganiami (12GB RAM, 4 CPU, 100GB przestrzeni dyskowej)</li> <li>b) System operacyjny z środowiskiem graficznym (Windows lub Linux (CentOS / Ubuntu);</li> <li>c) Zainstalowana Java 21 (lub OpenJDK);</li> <li>d) Dostępny serwer PostgreSQL (jeżeli uruchomiony na innym serwerze niż serwer aplikacji to skonfigurowany do odbierania połączeń sieciowych);</li> <li>e) Dostępna platforma integracyjna HIS, z dostępnymi co najmniej usługami licencjonowania;</li> <li>f) Skonfigurowana sieć (maszyna powinna być widoczna w sieci szpitalnej oraz posiadać dwukierunkowy dostęp do baz (HIS i ERP);</li> <li>g) Dostęp VPN dla konsultantów, umożliwiający połączenie ze środowiskiem oraz zalogowanie do systemów HIS oraz ERP;</li> </ul>
Szkolenie ogólne	W ramach szkolenia ogólnego prezentowany jest ogólny wygląd i zasada działania aplikacji.
Szkolenie dla wybranych użytkowników podstawowych (4 grupy maksymalnie 5-osobowe, 2h/grupa)	W ramach szkolenia użytkowników podstawowych prezentowane jest korzystanie z aplikacji na poziomie przygotowanych już pulpitów, korzystanie z filtrów oraz omówienie zakresów analiz.
Szkolenie 10 użytkowników zaawansowanych	<p>Zawiera przygotowanie pulpitów „dedykowanych”.</p> <p>W ramach szkolenia użytkowników zaawansowanych prezentowane jest tworzenie własnych pulpitów, grupowań oraz zestawów filtrów, a także ich udostępnianie. Użytkownik zaawansowany powinien po szkoleniu posiadać umiejętność samodzielnego tworzenia kolejnych pulpitów. Szkolenie powinno odbyć się z uwzględnieniem przesunięcia czasowego względem szkolenia użytkowników podstawowych, tak aby w ramach szkolenia móc przygotować razem z użytkownikami pulpity „dedykowane”, tzn. oparte na potrzebach klienta – przesunięcie czasowe to okres, w którym użytkownicy mają możliwość zapoznać się z aplikacją i zastanowić się nad propozycjami stosowania konkretnych układów pulpitów.</p>
Szkolenie administratorów IT	W ramach szkolenia administratorów prezentowane jest wykonywanie zapytań danych, parametryzacja, aktualizacja, a także inne elementy administracyjne, jak tworzenie użytkowników oraz nadawanie im uprawnień.
Asysta powdrożeniowa (3 lata)	<p>W ramach asysty powdrożeniowej zapewniana jest dostępność konsultanta (wdrożeńiowca) w celu udzielania ewentualnego wsparcia, w zakresach:</p> <ol style="list-style-type: none"> <li>1. Dodatkowych szkoleń/wyjaśnień dla użytkownika,</li> <li>2. Przygotowywania i konfiguracji kafelków, grupowań i komponowaniu pulpitów,</li> <li>3. Konfiguracji uprawnień i parametrów systemowych,</li> <li>4. Wyjaśniania źródeł danych dla kafelków (wskazywanie z jakiego miejsca w systemie dziedziny jest pobierana informacja).</li> <li>5. Asysta powdrożeniowa <b>może być wydłużana w miarę potrzeb, na życzenie klienta, jednak okres dłuższy niż przewidziany we wdrożeniu jest dodatkowo płatny.</b></li> </ol>



## IV. Część nr 2

### 1.3 Rozbudowa Sieci

#### *Zakup nowych przełączników FC-2 szt.*

Wymagania funkcjonalne dla każdego oferowanego przełącznika FC:

1. Przełącznik FC musi być wykonany w technologii FC minimum 64 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 64, 32, 16, 10, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.
2. Dostarczony przełącznik FC musi być wyposażony, w co najmniej 24 aktywne porty FC obsadzone wkładkami SFP+ typu shortwave obsługujących prędkość 32/16/8 Gb/s.
3. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubskrypcji (ang. oversubscription), gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 64Gb/s.
4. Całkowita przepustowość przełącznika FC w konfiguracji z 24 aktywnymi portami wyposażonej we wkładki 64Gb/s musi wynosić minimum 1536 Gb/s end-to-end.
5. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 460ns dla portów pracujących z prędkością 64Gbps.
6. Rodzaj obsługiwanych portów, co najmniej: E, EX, D, F oraz N.
7. Przełącznik FC musi umożliwiać obsługę agregacji do 8 fizycznych połączeń ISL, między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk (magistrala) o przepustowości minimum 512 Gb/s half duplex (dla wkładek 64Gbps) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu ISL. Trunk musi być realizowany na poziomie pojedynczych ramek FC, a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.
8. Przełącznik FC musi być wyposażony w mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
9. Przełącznik FC musi być wyposażony w mechanizm jednoczesnej obsługi ISL. Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID.
10. Przełącznik FC musi być dostarczony z aktywnym mechanizmem routingu FC (FCR) zapewniającym możliwość komunikacji wybranych urządzeń z różnych izolowanych sieci fabric.
11. Przełącznik FC musi obsługiwać sprzętową kompresję ramek FC dla wybranych połączeń ISL na co najmniej 4 portach przełącznika.
12. Przełącznik FC musi być dostarczony z aktywną możliwością przydzielenia, co najmniej 1400 tzw. buffer credits do wybranego portu FC przełącznika.
13. W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zonu oraz możliwość przypisania własnego administratora.
14. Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą przeznaczonych do tego celu połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric.
15. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zonu.
16. Przełącznik FC musi być wyposażony w mechanizm automatycznej kategoryzacji przepływów danych na podstawie prędkości pracy portu docelowego z przydziałem przepływów o prędkościach 16/8/4Gbps, 32Gbps i 64Gbps do różnych grup. Przepływy danych przydzielone do różnych grup nie mogą wpływać wzajemnie na swoją gospodarkę tzw. buffer credits. wartości parametru
17. Przełącznik FC musi realizować kategoryzację ruchu na podstawie CS CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii wysokim, średnim lub niskim priorytecie.
18. Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych. urządzeń na pojedynczym porcie przełącznika.
19. Przełącznik FC musi realizować sprzętową obsługę zonu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
20. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
  - 1) mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 4 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów,

- 2) mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric,
  - 3) uwierzytelnianie (ang. authentication) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP,
  - 4) uwierzytelnianie (ang. authentication) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP,
  - 5) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
  - 6) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control),
  - 7) definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+,
  - 8) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS,
  - 9) obsługa SNMP v1 oraz v3,
  - 10) IP Filter dla portu administracyjnego przełącznika,
  - 11) wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP,
  - 12) wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.
21. Przełącznik FC musi mieć możliwość konfiguracji przez:
- 1) polecenia tekstowe w interfejsie znakowym konsoli terminala,
  - 2) przeglądarkę internetową z interfejsem graficznym lub przeznaczone do tego oprogramowanie.
22. Przełącznik FC być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:
- 1) logowanie zdarzeń poprzez mechanizm „syslog”,
  - 2) ciągle monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych, powiadamianie administratora musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu,
  - 3) port diagnostyczny tzw. D port, port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16/32/64Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16/32/64Gbps, testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric,
  - 4) FCping,
  - 5) FC traceroute,
  - 6) kopiowanie wybranych przepływów danych na wskazany lokalny port przełącznika,
  - 7) przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe,
  - 8) przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy,
  - 9) przełącznik musi obsługiwać wysyłanie komunikatów FPIN typu: Link Integrity Notification, Delivery Notification, Peer Congestion Notification, Congestion Notification,
  - 10) przełącznik musi obsługiwać wysyłanie sprzętowych sygnałów typu End Device Congestion za pomocą mechanizmu prymitywów FC typu ARB.
23. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
24. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet RJ45 oraz konsolowy mini-USB.
25. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.
26. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.
27. Przełącznik FC musi mieć wysokość maksymalnie 1U (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w standardowej szafie dystrybucyjnej 19".



28. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne. porty obsadzone optyką 64Gbps SWL nie może przekraczać 105W.
29. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 56 aktywne porty obsadzone optyką 64Gbps SWL. nie może przekraczać 350 BTU na godzinę.
30. Przełącznik FC musi posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika.
31. Przełącznik FC musi wydymuchiwać gorące powietrze od strony zasilania (od przodu do tyłu).
32. Co najmniej 3 letnie wsparcie w trybie 24x7 z czasem reakcji NBD onsite. Gwarancja producenta, serwis w miejscu instalacji sprzętu świadczony przez producenta lub autoryzowanego partnera serwisowego.

### *Przełączniki PoE 14 szt.*

Cechy sprzętowe:

1. Urządzenie musi być wyposażone w min. 48 gigabitowe porty RJ45 oraz min. cztery porty SFP+. Nie są dopuszczane porty SFP+ współdzielone z portami RJ45 (tzw. „combo”)
2. Porty SFP+ muszą również obsługiwać moduły pracujące z prędkością 1Gbps
3. Urządzenie musi posiadać port konsolowy RJ45 lub microUSB
4. Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward
5. Rozmiar tablicy adresów MAC urządzenia min. 16K
6. Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 176 Gbps
7. Min. szybkość przekierowań pakietów 130,2 Mpps
8. Urządzenie musi wspierać funkcjonalność PoE zgodną ze standardem 802.3af/at, minimalny wymagany budżet dostępny dla zasilanych urządzeń to 750W
9. Całkowity pobór mocy urządzenia (wliczając pełne obciążenie PoE) nie może przekraczać 800W
10. Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe
11. Głębokość urządzenia nie może przekraczać 450 mm

Standardy:

Urządzenie musi spełniać następujące standardy:

- 1) 802.3i
- 2) 802.3u
- 3) 802.3z
- 4) 802.3ab
- 5) 802.3ad
- 6) 802.3ae
- 7) 802.3af
- 8) 802.3at
- 9) 802.3az
- 10) 802.3x
- 11) 802.1ab
- 12) 802.1d
- 13) 802.1w
- 14) 802.1s
- 15) 802.1p
- 16) 802.1q

Funkcjonalność:

Wymaga się, aby urządzenie posiadało następujące funkcjonalności:

1. Zarządzanie za pomocą przeglądarki poprzez interfejs http/https
2. Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia
3. Obsługę stosu IPv4 i IPv6
4. Funkcję wykrywania pętli
5. Funkcję izolacji portów
6. Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji)
7. Obsługę protokołu LLDP/LLDP-MED

8. Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6
9. Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6)
10. Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP)
11. Obsługę 4K identyfikatorów VLAN
12. Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN)
13. IGMP Snooping oraz MLD Snooping
14. Obsługę min 500 grup multicastowych jednocześnie
15. MVR
16. Obsługę routingu statycznego i/lub dynamicznego
17. Możliwość konfiguracji co najmniej 16 interfejsów IP
18. Obsługę min 40 tras statycznych dla funkcji routingu statycznego
19. Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+
20. Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia
21. Obsługę list kontroli dostępu (ACL)
22. Obsługę SNMP w wersjach v1/v2c/v3
23. Obsługę grup RMON 1,2,3,9)

Pozostałe wymagania:

1. Urządzenie musi posiadać certyfikację CE
2. Gwarancja na urządzenie musi wynosić min. 3 lata
3. Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta

### *Rozbudowa sieci WiFi (Punkty AP WiFi 6)*

Punkt dostępowy sieci WiFi

1. Urządzenie musi być wyposażone w min. 1 port RJ45 pracujący z prędkością 10,100,1000,2500 Mbit/s obsługujący standard PoE 802.3at
2. Urządzenie musi być wyposażone w gniazdo umożliwiające zasilanie urządzenia bezpośrednio z wykorzystaniem zewnętrznego zasilacza lub injectora pasywnego PoE 48V
3. Urządzenie musi być wyposażone w przycisk przywracania ustawień fabrycznych
4. Maksymalna szybkość przesyłania danych (2.4 GHz) 1148 Mbit/s
5. Maksymalna szybkość przesyłania danych (5 GHz) 4804 Mbit/s
6. Prędkość transferu danych przez Ethernet LAN 10,100,1000,2500 Mbit/s
7. Pasmo częstotliwości 2.4 - 6 GHz
8. Liczba użytkowników 510 użyt.
9. Automatyczne skanowanie kanałów Tak
10. Standardy komunikacyjne
11. IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.3at
12. Szybki roaming Tak
13. Podstawowy standard Wi-Fi Wi-Fi 6 (802.11ax)
14. Obsługa jakości serwisu (QoS) Tak
15. Maksymalna szybkość przesyłania danych 6000 Mbit/s
16. Rodzaj kierunku anteny Antena dookólna
17. Funkcje anteny Zintegrowana antena
18. Poziom wzmacnienia anteny (max) 5 dBi
19. Typ anteny Wewnętrzny
20. Urządzenie powinno być dostosowane do montażu na ścianie lub suficie oraz posiadać dołączony zestaw montażowy
21. Urządzenie musi pracować zarówno jako urządzenie typu stand-alone lub w trybie podłączonym do kontrolera sieci bezprzewodowej
22. Kontroler sieci bezprzewodowej realizowany musi być jako oprogramowanie przeznaczone do instalacji na systemach operacyjnych Windows/Linux lub kontroler sprzętowy – oddzielne urządzenie
23. Oprogramowanie kontrolera sieci bezprzewodowych musi być realizowane jako oprogramowanie bezpłatne, bez dodatkowych opłat licencyjnych
24. Urządzenie musi posiadać funkcjonalność tworzenia wielu sieci WiFi – min. 14 SSID

25. Urządzenie musi posiadać funkcjonalność: wyłącznik sieci bezprzewodowej, automatyczny wybór kanału, kontrola mocy transmisji, QoS (WMM), sterowanie pasmem, równoważenie obciążenia pasma, kontrola przepustowości, harmonogram resetu oraz harmonogram sieci bezprzewodowej.
26. Urządzenie musi posiadać możliwość utworzenia strony powitalnej
27. Urządzenie musi posiadać możliwość mapowania SSID do VLAN oraz tworzenia sieci dla gości
28. Urządzenie musi posiadać możliwość wyłączenia diody LED na obudowie
29. Urządzenie musi być zarządzane z poziomu przeglądarki internetowej, oraz obsługiwać zarządzanie poprzez HTTPS
30. Urządzenie musi posiadać obsługę SNMP v1/v2c,v3
31. Urządzenie musi posiadać certyfikat CE, FCC oraz RoHS
32. W zestawie z urządzeniem powinien być dostarczony zestaw montażowy

Dopuszczalna temperatura pracy powinna zawierać się w przedziale od 0 do 40 stopni Celsjusza.

### *Kontroler Sieci WiFi*

Kontroler sprzętowy sieci bezprzewodowej WiFi

Cechy fizyczne:

- 1) Kontroler musi umożliwiać zarządzanie punktami dostępowymi w liczbie min 450.
- 2) Kontroler musi mieć możliwość zarządzania zarówno urządzeniami odpowiadającymi za segment bezprzewodowy sieci (punkty dostępowe) jak i urządzeniami tworzącymi warstwę dostępową i szkielet sieci (przełączniki)
- 3) Urządzenie musi być wyposażone w min. 2 porty RJ45 o prędkości 10/100/1000Mb/s
- 4) Urządzenie musi być wyposażone w port USB umożliwiający podłączenie zewnętrznego nośnika danych
- 5) Urządzenie musi mieć możliwość montażu w szafie rack 19", elementy montażowe muszą być zawarte w zestawie.
- 6) Urządzenie musi posiadać następujące certyfikaty: CE, RoHS
- 7) Dopuszczana temperatura pracy urządzenia musi zawierać się w przedziale od 0 do 40 stopni Celsjusza

Cechy funkcjonalne:

- 1) Urządzenie musi umożliwiać automatyczne wykrywanie wszystkich urządzeń w sieci lokalnej kompatybilnych z Kontrolerem
- 2) Urządzenie musi zapewniać możliwość zdalnego zarządzania siecią w danej lokalizacji wykorzystując chmurę lub inny mechanizm pozwalający na dostęp do kontrolera z dowolnego miejsca
- 3) W zakresie ogólnej funkcjonalności urządzenie musi wspierać funkcje:
  - a) Wyświetlania topologii sieci (wykorzystując urządzenia zarządzane przez kontroler)
  - b) Zarządzania wieloma lokalizacjami z poziomu pojedynczego kontrolera
  - c) ACL (listy kontroli dostępu) zarówno dla użytkowników łączących się do sieci przewodowo jak i bezprzewodowo
  - d) Uwierzytelniania użytkowników zarówno przewodowych jak i bezprzewodowych z wykorzystaniem strony powitalnej
- 4) W zakresie konfiguracji sieci WiFi urządzenie musi umożliwiać konfigurację następujących funkcji:
  - a) Multi SSID
  - b) Sieć dla Gości (odizolowanie klientów w tej sieci od innych klientów lokalnych bez wykorzystania VLAN)
  - c) Powiązanie SSID do VLAN
  - d) Filtrowanie adresów MAC (tryby blacklist/whitelist)
  - e) Kanał transmisji/moc nadawania konkretnych AP
  - f) Równoważenie obciążenia punktów dostępowych
  - g) Sterowanie pasmem
  - h) Ograniczenie prędkości transmisji
  - i) Tworzenie harmonogramu sieci WiFi oraz resetu urządzeń
  - j) QoS
  - k) Harmonogramowanie sieci bezprzewodowej oraz restartu urządzenia

### 1.5 Rozbudowa hurtowni danych poprzez rozbudowę istniejących macierzy (2 macierze Dell Unity 380F)

Zamawiający posiada 2 macierze Dell Unity 380F (CRK00223408238, CRK00223408237) wyposażone po 7 dysków SAS Flash 4 3,4TB każda, należy dostarczyć dyski pozwalające na rozszerzenie pojemności każdej macierzy do 30TB.

Dopuszcza się również dostarczenie nowej macierzy o parametrach poniżej:

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1	<b>Obudowa</b>	Rozmiar obudowy zawierającej kontrolery macierzowe nie może przekraczać 2U. Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo.
2	<b>Kontrolery</b>	<p>Wymagane minimum dwa kontrolery pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny kontroler musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz. Macierz zaprojektowana do pracy z dostępnością 99.9999%, musi to być potwierdzone na oficjalnej stronie producenta.</p> <p>System macierzy ma monitorować obciążenie kontrolerów i automatycznie przenosić własność wolumenów, gdy wymaga tego stan wydajności.</p> <p>Macierz musi posiadać dwa kontrolery pracujące równocześnie. Dla każdego wolumenu należy móc wskazać preferowanego właściciela oraz zmienić własność wolumenu z poziomu narzędzi administracyjnych.</p> <p>Rozwiązanie musi udostępniać do każdego wolumenu co najmniej dwie ścieżki:</p> <ol style="list-style-type: none"><li>1) ścieżki aktywne i zoptymalizowane (prowadzące do kontrolera będącego właścicielem wolumenu),</li><li>2) ścieżki aktywne, lecz niezoptymalizowane (prowadzące do kontrolera partnerskiego).</li></ol> <p>Systemy operacyjne mają korzystać z mechanizmów wielościeżkowych w celu wyboru właściwej ścieżki.</p> <p>Automatyczne równoważenie obciążenia System ma monitorować obciążenie kontrolerów i automatycznie je równoważyć, w tym poprzez zmianę własności wolumenów, gdy wykryje nierównowagę. Funkcja ma być domyślnie włączona z możliwością włączenia/wyłączenia przez administratora w narzędziu do zarządzania lub w wierszu poleceń.</p> <p>Dane buforowane do zapisu na jednym kontrolerze muszą być lustrzane do pamięci drugiego kontrolera, tak aby w razie awarii jednego z nich drugi mógł dokończyć wszystkie niezapisane operacje zapisu. Wymagane jest, aby funkcja była dostępna przy włączonej pamięci zapisu i obecnych dwóch kontrolerach oraz aby była domyślnie aktywna podczas tworzenia wolumenów.</p> <p>W przypadku utraty jednego kontrolera, ruch wejścia/wyjścia ma być nieprzerwanie kontynuowany przez ścieżki alternatywne oraz — w razie potrzeby — po automatycznej zmianie właściciela wolumenu.</p> <p>Administrator musi mieć możliwość włączania i wyłączania funkcji automatycznego równoważenia obciążenia zarówno w konsoli graficznej, jak i poprzez wiersz poleceń. Administrator musi mieć możliwość ręcznego przypisania preferowanego właściciela dla wybranego wolumenu w celu strojenia pracy systemu.</p>

3	<b>Dostępne porty</b>	Oferowana macierz musi posiadać: 1) minimum 4 porty typu 10/25 Gb iSCSI SFP28 do obsługi hostów 2) minimum 8 portów typu 16/32 Gb FC do obsługi hostów, wyposażonych we wkładki maksymalnie dostępnej prędkości 3) minimum 4 porty typu 12 Gb SAS x4 (Mini-SAS HD SFF-8644) do podłączania półek dyskowych 4) minimum 2x porty typu serial console (RJ-45 and Micro-USB)
	<b>Obsługiwane protokoły w zakresie modelu oferowanego przez producenta</b>	SAS, iSCSI, FC (możliwość obsługi FC i iSCSI jednocześnie) Musi być możliwość wystawienia danych do hostów po FC i replikacji asynchronicznej oraz synchronicznej po FC.
4	<b>Cache</b>	Każdy z kontrolerów macierzy musi być wyposażony w min 32 GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania. Rozwiązania wykorzystujące do tego celu tylko i wyłącznie tzw. podtrzymanie cache za pomocą baterii nie są akceptowalne. Bateria może być użyta tylko i wyłącznie na czas zrzutu danych z cache na pamięć nieulotną.
5	<b>Dyski</b>	Macierz musi obsługiwać dyski HDD oraz SSD. Dostarczona macierz musi być wyposażona w minimum 10 dysków 7.68TB 1DWD 2.5" SSD. Oferowana macierz musi umożliwiać rozbudowę o minimum 120 dysków SSD oraz 300 dysków HDD. Oferowana macierz musi umożliwiać użycie dysków typu: 3.84TB 1DWD 2.5" SSD, 3.84TB 1DWD 2.5" SSD FIPS, 7.68TB 1DWD 2.5" SSD, 15.36TB 1DWD 2.5" SSD SED, 2.4TB 10K 2.5" HDD, 2.4TB 10K 2.5" HDD FIPS
6	<b>Funkcjonalności</b>	Macierz musi obsługiwać typy protekcji RAID 0,1,3,5,6,10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na puli zbudowanej ze wszystkich pamięci SSD macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji i przyspieszania procesów odtwarzania dysków pojemnościowych. W przypadku awarii dysku, do jego obudowy musi być używany każdy dysk z opisanej wyżej puli.  Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.  Macierz musi umożliwiać zwiększanie i zmniejszanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „thin provisioning”). Macierz musi posiadać funkcjonalność sprawdzania integralności zapisywanych danych poprzez odczyt sumy kontrolnej z karty HBA podłączonego serwera. Macierz musi mieć możliwość wykonywania minimum 256 kopii migawkowych typu copy-on-write z opcją zwiększenia do 512 kopii. Macierz musi posiadać funkcjonalność klonowania danych. Wymagana możliwość definiowania maksymalnej ilości kopii migawkowych. W przypadku osiągnięcia zdefiniowanej ilości kopii system musi automatycznie kasować kopie najstarsze. Ponadto macierz powinna posiadać funkcjonalność tworzenia konsystentnych kopii migawkowych ze wskazanych przestrzeni dyskowych. Macierz musi mieć możliwość replikacji danych po FC w trybie asynchronicznym i synchronicznym. Wymaga się funkcjonalności replikacji asynchronicznej w momencie dostawy. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 256 partycji.

		<p>Wymagana możliwość definiowania globalnych dysków hot-spare. Wymagana możliwość logicznej zamiany dysków z wykorzystaniem dysków nieprzypisanych.</p> <p>Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wysyłane powiadomienia muszą zawierać nazwę macierzy, informacje o typie zdarzenia, datę i czas wystąpienia zdarzenia oraz krótki opis zdarzenia. Macierz musi mieć możliwość definiowania poziomu zajętości miejsca, po osiągnięciu którego nastąpi wysłanie powiadomienia pod wskazane adresy email.</p> <p>Macierz musi posiadać wbudowany mechanizm, który przyspiesza zapisy, gdy obciążenie spełnia kryteria pełnego paska (zapis obejmuje cały stripe grupy i jest do niego wyrównany). Dzięki temu kontroler będzie pomijać cykl „czytaj-modyfikuj-zapisz” i zapisuje jednorazowo dane oraz parzystość.</p> <p>Funkcja musi aktywować się automatycznie dla obciążeń sekwencyjnych, stripe-aligned i pełnopaskowych.</p> <p>System zarządzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego automatycznie w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.</p> <p>Macierz musi mieć funkcjonalność automatycznej detekcji podłączonych hostów (nazwa hosta oraz typ systemu operacyjnego). Musi być możliwość edycji hostów dodanych w sposób automatyczny.</p> <p>Wymagana jest funkcjonalność automatycznego tworzenia przestrzeni dyskowych zoptymalizowanych pod kątem używanych na nich aplikacji jak SQL Server, Exchange oraz VMware VMFS.</p> <p>Wymagana jest możliwość automatycznego logicznego grupowania dysków macierzy (dodawanie dysków do istniejącej grupy oraz tworzenie nowej grupy z dodanych dysków).</p> <p>Macierz musi mieć możliwość definiowania priorytetu operacji wprowadzanych zmian konfiguracji w odniesieniu do obciążenia generowanego przez podłączone hosty.</p> <p>Wymagana jest możliwość sprawdzenia aktualnych zadań macierzy.</p> <p>Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych z użyciem dysków FIPS. Nie wymaga się tej funkcjonalności w chwili dostawy.</p> <p>Macierz musi posiadać możliwość fizycznej identyfikacji (dioda LED) aktywowanej z interfejsu zarządzania oraz funkcjonalność fizycznego identyfikowania dysków (dioda LED) należących do jednej przestrzeni logicznej.</p> <p>Macierz musi mieć możliwość przypisania wolumenu danych tylko do wybranego hosta należącego do zdefiniowanego klastra.</p> <p>Linia produktowa, z której pochodzi macierz musi być wymieniona na liście Veeam w zakresie obsługi funkcjonalności Backup Target - Disk iSCSI dla Veeam Backup &amp; Replication 12.</p>
7	<b>Wydajność</b>	<p>Wymaga się możliwości rozbudowania macierzy do minimalnego poziomu wydajności deklarowanego przez Producenta:</p> <ol style="list-style-type: none"> <li>1) przynajmniej 900 000 operacji wejścia wyjścia dla losowego odczytu</li> <li>2) przynajmniej 100 000 operacji wejścia wyjścia dla losowego zapisu</li> <li>3) przynajmniej 12 GBps operacji wejścia wyjścia dla sekwencyjnego odczytu</li> </ol> <p>Wymagana pojemność LUN dla wolumenów z dynamiczną alokacją przestrzeni (thin provisioning) to przynajmniej 256 TB.</p>
8	<b>Zarządzanie macierzą</b>	<p>Dostępne minimum dwa porty 1 GbE port (UTP, RJ-45) w trybie primary/redundant.</p> <p>Zarządzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh.</p>



		<p>Interfejs zarządzania powinien wylogować sesje po maksymalnie 15 minutach bezczynności. Maksymalna ilość prób podania hasła administratora nie może być większa niż 5 do momentu zablokowania dostępu.</p> <p>Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control.</p> <p>Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy:</p> <ol style="list-style-type: none"> <li>1) storage admin – pełen dostęp wyłączeniem ustawień bezpieczeństwa</li> <li>2) security admin – dostęp do ustawień bezpieczeństwa</li> <li>3) support admin – pełen dostęp serwisowy</li> <li>4) monitor – możliwość odczytu konfiguracji</li> </ol> <p>Producent powinien udostępniać konsolę umożliwiającą dodawanie do domeny zarządzania wielu macierzy jednocześnie. Wymaga się możliwości importu konfiguracji z jednej macierzy na inne.</p>
9	<b>Inne</b>	<p>Wymagana jest bezprzerwowa wymiana następujących elementów macierzy: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+.</p> <p>Obsługa systemów operacyjnych hosta: Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere.</p> <p>Producent macierzy powinien posiadać oficjalne przedstawicielstwo w Polsce, które nie jest reprezentowane przez podmioty typu Dystrybucja, Partner, etc, oraz posiadać certyfikaty ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne</p> <p>Macierz musi być zgodna z regulacjami EU: CE Mark (EN55032 Class A, EN55024, IEC/EN60950-1 and 62368-1); ROHS Directive 2011/65/EU lub równoważne</p>
10	<b>Gwarancja</b>	<p>Co najmniej 3 letnie wsparcie w trybie NBD onsite. Gwarancja producenta, serwis w miejscu instalacji sprzętu świadczony przez producenta macierzy lub autoryzowanego partnera serwisowego.</p> <p>W przypadku awarii dyski pozostają własnością Zamawiającego.</p>

#### **1.6 Zakup serwerów wraz z systemem operacyjnym oraz licencjami dostępowymi z kartami FC do podłączenia do macierzy oraz systemem wirtualizacji**

Serwer typ 1 – 2 szt.

Nazwa elementu, parametru lub cechy	Opis wymagań Serwerów
Ilość Sztuk	2
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – nie więcej niż 8. Minimalna częstotliwość pracy procesora 3.5GHz. Wynik wydajności procesora nie powinien być niższy niż 210 pkt. base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org ( <a href="http://www.spec.org">www.spec.org</a> ), dla serwera oferowanego producenta.
Liczba zainstalowanych procesorów	2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje



<b>Pamięć operacyjna</b>	Zainstalowane minimum 512 GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w kościach 32GB Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
<b>Zabezpieczenie pamięci</b>	Memory mirroring, ECC, SDDC, ADDDC
<b>Procesor Graficzny</b>	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
<b>Rozbudowa dysków</b>	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków M.2 hot-plug o pojemności przynajmniej 480 GB sterowanych dedykowanym kontrolerem sprzętowym umożliwiającym redundancję raid-1. Dyski oraz dedykowany kontroler nie mogą zajmować żadnego slotu pci wymienionego w punkcie <b>Dodatkowe sloty I/O</b> . Wymagany jest wewnętrzny slot na kartę Micro SD.
<b>Zasilacz</b>	Minimum dwa redundantne zasilacze o mocy minimum 1300W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
<b>Interfejsy sieciowe</b>	Zainstalowana dwuportowa karta 10Gb/25Gb wyposażona w dedykowane wkładki 10/25Gbs MMF LC. Karta nie może zajmować żadnego ze slotów PCIe wymienionych w punkcie Sloty I/O. Zainstalowana dwuportowa karta FC 32GB wyposażona w dedykowane wkładki 32Gb MMF LC. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej..
<b>Sloty I/O</b>	Serwer w momencie dostawy powinien posiadać jeden slot PCIe 5 pełnej wysokości, 2 sloty OCP Gen5 oraz dedykowane połączenie PCIe dla kontrolera dyskowego niezajmujące slotów PCIe.
<b>Chłodzenie</b>	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
<b>Zarządzanie</b>	<p>Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty).</p> <p>Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)</p> <p>Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja</p> <p>Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.</p> <p>Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/installacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.</p> <p>Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3</p> <ol style="list-style-type: none"> <li>1) Update systemowego firmware</li> <li>2) Monitoring i możliwość ograniczenia poboru prądu</li> <li>3) Zdalne włączanie/wyłączanie/restart</li> <li>4) Zapis video zdalnych sesji</li> <li>5) Podmontowanie lokalnych mediów z wykorzystaniem Java client</li> <li>6) Przekierowanie konsoli szeregowej przez IPMI</li> <li>7) Zrzut ekranu w momencie zawieszenia systemu</li> <li>8) Możliwość przejęcia zdalnego ekranu</li> <li>9) Możliwość zdalnej instalacji systemu operacyjnego</li> <li>10) Alerty Syslog</li> <li>11) Przekierowanie konsoli szeregowej przez SSH</li> <li>12) Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera</li> <li>13) Możliwość mapowania obrazów ISO z lokalnego dysku operatora</li> </ol>

	<p>14) Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS</p> <p>15) Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę</p> <p>16) wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API</p> <p>17) Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzająca) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.</p> <p>18) Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.</p> <p>19) Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.</p> <p>20) Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.</p> <p>21) Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.</p> <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ol style="list-style-type: none"> <li>1) zarządzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta</li> <li>2) przedstawianie graficznej reprezentacji zarządzanych urządzeń</li> <li>3) możliwość skalowania do minimum 1000 urządzeń</li> <li>4) obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2</li> <li>5) wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych</li> <li>6) udostępnianie szybkiego podgląd stanu środowiska</li> <li>7) udostępnianie podsumowania stanu dla każdego urządzenia</li> <li>8) tworzenie alertów przy zmianie stanu urządzenia</li> <li>9) monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,</li> <li>10) konsola zarządzania oparta o HTML 5</li> <li>11) dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,</li> <li>12) automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja</li> <li>13) możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania</li> <li>14) definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń</li> <li>15) definiowanie roli użytkowników oprogramowania</li> <li>16) obsługa REST API oraz Windows PowerShell</li> <li>17) obsługa SNMP, SYSLOG, Email Forwarding</li> <li>18) autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML</li> <li>19) obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami</li> <li>20) przedstawianie historycznych aktywności użytkowników</li> <li>21) blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych</li> </ol>
--	---

	<p>22) tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv</p> <p>23) Obsługa NTP</p> <p>24) przesyłanie alertów do konsoli firm trzecich</p> <p>25) tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsolę albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)</p> <p>26) instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie</p> <p>27) możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,</p> <p>Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.</p>
<b>Funkcje zabezpieczeń</b>	<p>Zainstalowany czujnik otwarcia obudowy zintegrowany z modulem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płycie I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR). Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu karty zarządzania. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.</p>
<b>Urządzenia hot swap</b>	Dyski twarde, zasilacze, wentylatory.
<b>Obsługa</b>	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
<b>Diagnostyka</b>	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.
<b>Systemy operacyjne</b>	Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux 9.x; SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3; Ubuntu 22.04, 24.04
<b>Gwarancja</b>	<p>Min. 36 miesięcy gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 24 godzin. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.</p>
<b>System wirtualizacji</b>	<p>Zamawiający wymaga dostarczenia i wdrożenia systemu do zarządzania środowiskiem wirtualnym, spełniającego poniższe wymagania:</p> <ol style="list-style-type: none"> <li>1. Typ rozwiązania: Oprogramowanie klasy hypervisor typu 1 (bare-metal), działające na systemie Linux, umożliwiające zarządzanie maszynami wirtualnymi oraz kontenerami.</li> <li>2. Architektura: <ol style="list-style-type: none"> <li>1) Obsługa wirtualizacji KVM (Kernel-based Virtual Machine).</li> <li>2) Obsługa kontenerów LXC (Linux Containers).</li> <li>3) Możliwość tworzenia klastra z wielu węzłów.</li> </ol> </li> </ol>

	4) Zarządzanie: 5) Centralny interfejs WWW do zarządzania wszystkimi węzłami klastra. 6) Wbudowany mechanizm zarządzania użytkownikami i uprawnieniami (RBAC). 7) Możliwość integracji z LDAP/Active Directory.  3. Funkcjonalności: 1) Obsługa migracji maszyn wirtualnych „na żywo” (live migration). 2) Wbudowany mechanizm wysokiej dostępności (HA). 3) Możliwość wykonywania kopii zapasowych i przywracania maszyn wirtualnych. 4) Obsługa wielu typów pamięci masowej (np. lokalna, NFS, iSCSI, Ceph). 5) Licencjonowanie: Oprogramowanie typu open source lub z licencją umożliwiającą jego legalne użytkowanie w instytucji publicznej.
<b>Certyfikaty i standardy</b>	Dla producenta sprzętu: ISO 9001, ISO 14001, ISO 50001 lub równoważne  Dla serwera: 1) Deklaracja zgodności CE 2) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Ww. dokumenty na wezwanie Zamawiającego.

Serwer typ 2 – 2 szt.

<b>Opis wymagań Serwerów</b>	<b>Opis wymagań Serwerów</b>
<b>Ilość Sztuk</b>	2
<b>Obudowa</b>	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami
<b>Procesor</b>	Architektura x86, maksymalny TDP dla procesora – maksymalnie 350W. Wymagana ilość rdzeni dla procesora – nie mniej niż 32. Minimalna częstotliwość pracy procesora 2.4GHz..Wynik wydajności procesora nie powinien być niższy niż 960 pkt. base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org ( <a href="http://www.spec.org">www.spec.org</a> ), dla serwera oferowanego producenta.
<b>Liczba zainstalowanych procesorów</b>	2
<b>Płyta główna</b>	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
<b>Pamięć operacyjna</b>	Zainstalowane minimum 1024 GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w kościach 64GB Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
<b>Zabezpieczenie pamięci</b>	Memory mirroring, ECC, SDDC, ADDDC
<b>Procesor Graficzny</b>	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
<b>Rozbudowa dysków</b>	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków M.2 hot-plug o pojemności przynajmniej 480 GB sterowanych dedykowanym kontrolerem sprzętowym umożliwiającym redundancję raid-1. Dyski oraz dedykowany kontroler nie mogą zajmować żadnego slotu pci wymienionego w punkcie <b>Dodatkowe sloty I/O</b> .  Wymagany jest wewnętrzny slot na kartę Micro SD.
<b>Zasilacz</b>	Minimum dwa redundantne zasilacze o mocy minimum 1300W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
<b>Interfejsy sieciowe</b>	Zainstalowana dwuportowa karta 10Gb/25Gb wyposażona w dedykowane wkładki 10/25Gbs MMF LC. Karta nie może zajmować żadnego ze slotów PCIe wymienionych w punkcie Sloty I/O.

	<p>Zainstalowana dwuportowa karta FC 32GB wyposażona w dedykowane wkładki 32Gb MMF LC.</p> <p>Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej..</p>
<b>Sloty I/O</b>	Serwer w momencie dostawy powinien posiadać jeden slot PCIe 5 pełnej wysokości, 2 sloty OCP Gen5 oraz dedykowane połączenie PCIe dla kontrolera dyskowego niezajmujące slotów PCIe.
<b>Chłodzenie</b>	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
<b>Zarządzanie</b>	<p>Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty).</p> <p>Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)</p> <p>Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja.</p> <p>Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.</p> <p>Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.</p> <p>Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3</p> <ol style="list-style-type: none"> <li>1) Update systemowego firmware</li> <li>2) Monitoring i możliwość ograniczenia poboru prądu</li> <li>3) Zdalne włączanie/wyłączanie/restart</li> <li>4) Zapis video zdalnych sesji</li> <li>5) Podmontowanie lokalnych mediów z wykorzystaniem Java client</li> <li>6) Przekierowanie konsoli szeregowej przez IPMI</li> <li>7) Zrzut ekranu w momencie zawieszenia systemu</li> <li>8) Możliwość przejęcia zdalnego ekranu</li> <li>9) Możliwość zdalnej instalacji systemu operacyjnego</li> <li>10) Alerty Syslog</li> <li>11) Przekierowanie konsoli szeregowej przez SSH</li> <li>12) Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera</li> <li>13) Możliwość mapowania obrazów ISO z lokalnego dysku operatora</li> <li>14) Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS</li> <li>15) Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę</li> <li>16) wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API</li> <li>17) Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.</li> <li>18) Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.</li> <li>19) Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.</li> </ol>

	<p>20) Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.</p> <p>21) Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.</p> <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ol style="list-style-type: none"> <li>1) zarządzanie infrastrukturą serwerów storage bez udziału dedykowanego agenta</li> <li>2) przedstawianie graficznej reprezentacji zarządzanych urządzeń</li> <li>3) możliwość skalowania do minimum 1000 urządzeń</li> <li>4) obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2</li> <li>5) wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych</li> <li>6) udostępnianie szybkiego podglądu stanu środowiska</li> <li>7)</li> <li>8) - udostępnianie podsumowania stanu dla każdego urządzenia</li> <li>9) tworzenie alertów przy zmianie stanu urządzenia</li> <li>10) monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,</li> <li>11) konsola zarządzania oparta o HTML 5</li> <li>12) dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,</li> <li>13) automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja</li> <li>14) możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania</li> <li>15) definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń</li> <li>16) definiowanie roli użytkowników oprogramowania</li> <li>17) obsługa REST API oraz Windows PowerShell</li> <li>18) obsługa SNMP, SYSLOG, Email Forwarding</li> <li>19) autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML</li> <li>20) obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami</li> <li>21) przedstawianie historycznych aktywności użytkowników</li> <li>22) blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych</li> <li>23) tworzenie dziennika zdarzeń ukończonych sukcesem lub błędem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv</li> <li>24) obsługa NTP</li> <li>25) przesyłanie alertów do konsoli firm trzecich</li> <li>26) tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsolę albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)</li> <li>27) instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie</li> </ol>
--	--



	<p>28) możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,</p> <p>Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.</p>
<b>Funkcje zabezpieczeń</b>	<p>Zainstalowany czujnik otwarcia obudowy zintegrowany z modulem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płycie I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR).,Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu karty zarządzania. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej.</p> <p>Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.</p>
<b>Urządzenia hot swap</b>	Dyski twarde, zasilacze, wentylatory.
<b>Obsługa</b>	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
<b>Diagnostyka</b>	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.
<b>Systemy operacyjne</b>	Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux 9.x; SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3; Ubuntu 22.04, 24.04
<b>Gwarancja</b>	<p>Min. 36 miesięcy gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 24 godzin. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera..</p>
<b>System wirtualizacji</b>	<p>Zamawiający wymaga dostarczenia i wdrożenia systemu do zarządzania środowiskiem wirtualnym, spełniającego poniższe wymagania:</p> <ol style="list-style-type: none"> <li>1. Typ rozwiązania: Oprogramowanie klasy hypervisor typu 1 (bare-metal), działające na systemie Linux, umożliwiające zarządzanie maszynami wirtualnymi oraz kontenerami.</li> <li>2. Architektura: <ol style="list-style-type: none"> <li>1) Obsługa wirtualizacji KVM (Kernel-based Virtual Machine).</li> <li>2) Obsługa kontenerów LXC (Linux Containers).</li> <li>3) Możliwość tworzenia klastra z wielu węzłów.</li> <li>4) Zarządzanie: <ol style="list-style-type: none"> <li>5) Centralny interfejs WWW do zarządzania wszystkimi węzłami klastra.</li> <li>6) Wbudowany mechanizm zarządzania użytkownikami i uprawnieniami (RBAC).</li> <li>7) Możliwość integracji z LDAP/Active Directory.</li> </ol> </li> </ol> </li> <li>3. Funkcjonalności: <ol style="list-style-type: none"> <li>1) Obsługa migracji maszyn wirtualnych „na żywo” (live migration).</li> <li>2) Wbudowany mechanizm wysokiej dostępności (HA).</li> <li>3) Możliwość wykonywania kopii zapasowych i przywracania maszyn wirtualnych.</li> <li>4) Obsługa wielu typów pamięci masowej (np. lokalna, NFS, iSCSI, Ceph).</li> </ol> </li> </ol>



	5) Licencjonowanie: Oprogramowanie typu open source lub z licencją umożliwiającą jego legalne użytkowanie w instytucji publicznej.
<b>Certyfikaty i standardy</b>	<p>Dla producenta sprzętu: ISO 9001, ISO 14001, ISO 50001 lub równoważne</p> <p>Dla serwera:</p> <ol style="list-style-type: none"> <li>1) Deklaracja zgodności CE</li> <li>2) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki</li> </ol> <p>Ww. dokumenty wymagane na żądanie Zamawiającego.</p>

Licencje na serwerowy system operacyjny.

#### **Licencje na 2 serwery fizyczne wyposażone w procesor o liczbie core do 32 każdy łącznie 128.**

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie minimum 1000 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanych serwerach.

Dostarczane oprogramowanie musi być w najnowszej, obecnie dostępnej wersji na rynku.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 128 procesorów oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 wątków, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
  - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
  - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
  - c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
  - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologii ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
  - a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
  - b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:

- a) a. Login i hasło,
  - b) b. Karty z certyfikatami (smartcard),
  - c) c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. 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.
  20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
  21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
  22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
  23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
  24. Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
  25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - 1) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    - 2) 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, urządzenia sieciowe), z możliwością wykorzystania następujących funkcji:
      - a) Podtroczenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną,
      - b) Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania,
      - c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
      - d) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    - 3) Zdalna dystrybucja oprogramowania na stacje robocze.
    - 4) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    - 5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
      - a) Dystrybucja certyfikatów poprzez http
      - b) Konsolidacja CA dla wielu lasów domeny,
      - c) Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
      - d) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    - 6) Szyfrowanie plików i folderów.
    - 7) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    - 8) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    - 9) Serwis udostępniania stron WWW.
    - 10) Wsparcie dla protokołu IP w wersji 6 (IPv6),
    - 11) Wsparcie dla algorytmów Suite B (RFC 4869),
    - 12) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    - 13) m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000
    - 14) aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu fail-over z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mającą zapewnić wsparcie dla:
      - a) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
      - b) Obsługa ramek typu jumbo frames dla maszyn wirtualnych.
      - c) Obsługi 4-KB sektorów dysków
      - d) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
      - e) Możliwość wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
      - f) możliwość kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).

26. 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.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Ponadto należy dostarczyć 150 licencji dostępowych do serwera typu CAL oraz 150 licencji dostępowych CAL RDS (usługi pulpitu zdalnego) licencje na urządzenie.

### *1.6 Zakup stacji roboczych tj. PC z systemami operacyjnymi oraz terminali tj. tzw. cienki klient, laptopów oraz monitorów*

#### Zakup terminali 8GB RAM, 64GB pamięci eMMC, zintegrowana karta graficzna 200 szt

Szczegółowy opis		
Komputer stacjonarny.		
Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.		
Zamawiający zastrzega sobie prawo do sprawdzenia režimu gwarancyjnego oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	<b>Komputer</b>	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.
2.	<b>Obudowa</b>	Małogabarytowa typu micro/tiny, wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych  Obudowa o sumie wymiarów nieprzekraczającej 400 mm.
3.	<b>Chipset</b>	Dostosowany do zaoferowanego procesora
4.	<b>Płyta główna</b>	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny oraz model komputera.
5.	<b>Procesor</b>	Procesor wielordzeniowy klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i3-N305 na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na <a href="http://www.cpubenchmark.net/">http://www.cpubenchmark.net/</a> .
6.	<b>Pamięć operacyjna</b>	Min. 8 GB DDR5-5600 MHz Możliwość rozbudowy do min. 16GB
7.	<b>Dysk twardy</b>	Dysk M.2 256 GB SSD PCIe 4.0 NVMe samoszyfrujący w technologii OPAL 2.0
8.	<b>Karta graficzna</b>	Zintegrowana karta graficzna z procesorem.
9.	<b>Audio</b>	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
10.	<b>Sieć</b>	Karta sieciowa LAN obsługująca prędkości 10/100/1000
11.	<b>Porty/złącza</b>	Obudowa komputera wyposażona w złącza: 1. Na przodzie urządzenia 1) min. 2x USB 3.2 Gen 2 2) złącze słuchawkowo-mikrofonowe typu combo 2. Z tyłu urządzenia

		<ol style="list-style-type: none"> <li>1) min. 2x USB 2.0</li> <li>2) min. 1x USB 3.2 Gen 2</li> <li>3) min. 1x HDMI 2.1</li> <li>4) min. 1x DisplayPort 1.4</li> <li>5) złącze Gigabit Ethernet (RJ-45)</li> </ol> <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p>
12.	<b>Klawiatura/mysz</b>	Przewodowa USB: klawiatura w układzie US + mysz z rolką
13.	<b>Zasilacz</b>	Energooszczędny zasilacz o mocy nie większej niż 65W oraz sprawności na poziomie min. 89%
14.	<b>BIOS</b>	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.</p> <p>Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ol style="list-style-type: none"> <li>1) wersji BIOS</li> <li>2) modelu komputera</li> <li>3) nr seryjnym komputera</li> <li>4) Ilości i taktowaniu zainstalowanej pamięci RAM</li> <li>5) typie i taktowaniu procesora</li> <li>6) informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS</li> </ol> <p>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:</p> <ol style="list-style-type: none"> <li>1) Możliwość ustawienia hasła Administratora</li> <li>2) Możliwość ustawienia hasła Użytkownika</li> <li>3) Możliwość ustawienia hasła dysku twardego</li> <li>4) Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS</li> <li>5) Możliwość włączenia/wyłączenia urządzeń zewnętrznych z listy bootowania</li> <li>6) Możliwość wyłączenia/włączania: karty sieciowej, kontrolera audio, kontrolera portów USB, bluetooth</li> </ol>
15.	<b>Zintegrowany System Diagnostyczny</b>	<p>Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający wykonanie diagnostyki następujących podzespołów:</p> <ol style="list-style-type: none"> <li>1) wykonanie testu pamięci RAM</li> <li>2) test dysku twardego</li> <li>3) test magistrali PCI-e</li> <li>4) test portów USB</li> <li>5) test płyty głównej</li> </ol>
16.	<b>System operacyjny</b>	<p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> <li>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> <li>a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych</li> </ol> </li> <li>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego</li> <li>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim</li> <li>4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.</li> <li>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe</li> </ol>

		<ol style="list-style-type: none"> <li>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,</li> <li>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</li> <li>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim</li> <li>9. Wbudowany system pomocy w języku polskim.</li> <li>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</li> <li>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</li> <li>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</li> <li>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</li> <li>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</li> <li>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</li> <li>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</li> <li>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.</li> <li>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</li> <li>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</li> <li>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</li> <li>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</li> <li>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</li> <li>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</li> <li>24. Wbudowany mechanizm wirtualizacji typu hypervisor.</li> <li>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</li> <li>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</li> <li>27. Wbudowana zaporą internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</li> <li>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.).</li> <li>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie</li> </ol>
--	--	--



		<p>bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ol style="list-style-type: none"> <li>Login i hasło,</li> <li>Karty inteligentne i certyfikaty (smartcard),</li> <li>Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> <li>Certyfikat/Klucz i PIN</li> <li>Certyfikat/Klucz i uwierzytelnienie biometryczne</li> </ol> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p>
17.	<b>Certyfikaty i standardy</b>	<p>Dla producenta sprzętu: ISO 9001, ISO 14001, ISO 50001 lub równoważne</p> <p>Dla komputera:</p> <ol style="list-style-type: none"> <li>1) Deklaracja zgodności CE</li> <li>2) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki</li> </ol> <p>Ww. dokumenty wymagane na żądanie Zamawiającego.</p>
18.	<b>Bezpieczeństwo</b>	<ol style="list-style-type: none"> <li>1. Złącze typu Kensington Lock</li> <li>2. fTPM 2.0</li> <li>3. Czujnik otwarcia obudowy</li> </ol>
19.	<b>Wirtualizacja</b>	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
20.	<b>Oprogramowanie</b>	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta, w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać ich zbiorczą instalację. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie.
21.	<b>Gwarancja i wsparcie techniczne producenta</b>	Min. 36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site). W przypadku awarii dysku twardego pozostaje on własnością Zamawiającego.



		<p>Firma serwisująca posiadająca certyfikat ISO 9001:2000 lub równoważny na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta</p> <p>Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:</p> <ol style="list-style-type: none"> <li>1) fabrycznej konfiguracji urządzenia,</li> <li>2) rodzaju gwarancji,</li> <li>3) dacie wygaśnięcia gwarancji,</li> <li>4) aktualizacjach.</li> </ol> <p>Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.</p>
--	--	--

Zakup Komputerów PC proces 14 rdzeniowy, 16GB RAM, Dysk SSD512GB, System Win11P. 120 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	<b>Komputer</b>	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.
2.	<b>Obudowa</b>	Typu Small Form Factor, umożliwiająca montaż minimum dwóch dysków SSD oraz jednego dysku HDD 3,5". Obudowa trwale oznaczona nazwą producenta i modelem komputera oraz posiadająca fabrycznie wbudowany napęd DVD-RW.
3.	<b>Chipset</b>	Dostosowany do zaoferowanego procesora
4.	<b>Płyta główna</b>	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w: <ol style="list-style-type: none"> <li>a) 3 sloty M.2</li> <li>b) 4 sloty DIMM na pamięć RAM</li> <li>c) 2 sloty PCIe min. 3.0 o niskim profilu</li> <li>d) 2 złącza SATA</li> </ol>
5.	<b>Procesor</b>	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core Ultra 5 235 na podstawie PerformanceTest w teście CPU Mark według wyników Average CPU Mark opublikowanych na stronie <a href="http://www.cpubenchmark.net">http://www.cpubenchmark.net</a> .
6.	<b>Pamięć operacyjna</b>	Fabrycznie zainstalowane min. 16GB DDR5 5600MHz w trybie Dual Channel.  Możliwość rozbudowy pamięci do min. 128 GB. Min. 2 sloty wolne.
7.	<b>Dysk twardy</b>	Min. 512GB SSD PCIe NVMe Opal, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy jednostki komputerowej o 2 dodatkowe dyski twarde.
8.	<b>Karta graficzna</b>	Zintegrowana z procesorem
9.	<b>Audio</b>	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  Wbudowany głośnik multimedialny o mocy 1W.
10.	<b>Sieć</b>	Karta sieciowa LAN obsługująca prędkości 10/100/1000 i WoL
11.	<b>Porty/złącza</b>	<ol style="list-style-type: none"> <li>1. Z przodu obudowy: <ol style="list-style-type: none"> <li>a) 1x USB 3.2 typu C z możliwością ładowania podłączonych urządzeń</li> <li>b) 4x USB 3.2 typu A</li> <li>c) złącze audio combo</li> </ol> </li> <li>2. Z tyłu obudowy: <ol style="list-style-type: none"> <li>a) 4x USB 3.2 typu A</li> <li>b) 1x HDMI 2.1</li> <li>c) 2x DisplayPort 1.4a</li> <li>d) 1x RJ-45</li> <li>e) 1x line-out</li> </ol> </li> </ol> <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p>
12.	<b>Klawiatura/mysz</b>	Przewodowe USB: klawiatura w układzie US + mysz z rolką

13.	<b>Zasilacz</b>	Energooszczędny zasilacz o mocy min. 200W oraz sprawności na poziomie min. 90%.
14.	<b>System operacyjny</b>	<p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> <li>Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> <li>Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.</li> </ol> </li> <li>Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego.</li> <li>Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.</li> <li>Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.</li> <li>Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe.</li> <li>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.</li> <li>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</li> <li>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.</li> <li>Wbudowany system pomocy w języku polskim.</li> <li>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</li> <li>Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</li> <li>Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</li> <li>Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</li> <li>Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</li> <li>Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</li> <li>Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</li> <li>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.</li> <li>Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</li> <li>Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</li> <li>Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</li> <li>Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</li> <li>Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</li> <li>Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</li> <li>Wbudowany mechanizm wirtualizacji typu hypervisor.</li> </ol>

		<p>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</p> <p>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>27. Wbudowana zaporą internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>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.).</p> <p>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.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> <li>a) Login i hasło,</li> <li>b) Karty inteligentne i certyfikaty (smartcard),</li> <li>c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> <li>d) Certyfikat/Klucz i PIN</li> <li>e) Certyfikat/Klucz i uwierzytelnienie biometryczne.</li> </ul> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.</p>
15.	<b>BIOS</b>	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> <li>a) modelu komputera,</li> <li>b) numerze seryjnym,</li> <li>c) wersji BIOS,</li> <li>d) zainstalowanym procesorze wraz z taktowaniem,</li> <li>e) zainstalowanej pamięci RAM wraz z taktowaniem,</li> <li>f) adresie MAC karty sieciowej.</li> </ul> <p>Administrator z poziomu BIOS musi mieć możliwość:</p> <ul style="list-style-type: none"> <li>a) wyłączenia portów USB</li> <li>b) wyłączenia karty sieciowej</li> <li>c) wyłączenia karty audio</li> </ul>

		<ul style="list-style-type: none"> <li>d) wyłączenia funkcji Wake on LAN</li> <li>e) wyłączenia wirtualizacji</li> <li>f) ustawienia hasła: administratora, Power-On, dysku twardego</li> <li>g) zdefiniowania sekwencji bootowania</li> <li>h) załadowania optymalnych ustawień BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych</li> </ul>
16.	<b>System Diagnostyczny</b>	<p>Zaimplementowany w UEFI BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednocześnie przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych:</p> <ol style="list-style-type: none"> <li>1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: <ul style="list-style-type: none"> <li>a) pamięci ram,</li> <li>b) procesora,</li> <li>c) - pamięci masowej,</li> <li>d) - płyty głównej</li> </ul> </li> <li>2. Identyfikację jednostki i jej komponentów w następującym zakresie: <ul style="list-style-type: none"> <li>a) urządzenie (producent, model, numer seryjny),</li> <li>b) bios (wersja oraz data wydania),</li> <li>c) procesor (nazwa, taktowanie, ilości pamięci L1, L2, L3, liczba rdzeni),</li> <li>d) pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny),</li> <li>e) dysk twardy (producent, model, numer seryjny, pojemność),</li> <li>f) płyta główna (liczba złącz USB, liczba złącz PCI)</li> </ul> </li> </ol>
17.	<b>Certyfikaty i standardy</b>	<p>Dla producenta sprzętu: ISO 9001, ISO 14001, ISO 50001 lub równoważne</p> <p>Dla komputera:</p> <ol style="list-style-type: none"> <li>1) Deklaracja zgodności CE</li> <li>2) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki</li> <li>3) EPEAT min. Silver</li> <li>4) TCO</li> </ol> <p>Ww. dokumenty wymagane na żądanie Zamawiającego.</p>
18.	<b>Bezpieczeństwo</b>	<ol style="list-style-type: none"> <li>1. Złącze typu Kensington Lock</li> <li>2. Oczko na kłódkę, zabezpieczającą urządzenie przed nieautoryzowanym otwarciem</li> <li>3. Sprzętowy moduł TPM 2.0 (dTPM 2.0) z certyfikacją TCG</li> <li>4. Czujnik otwarcia obudowy</li> <li>5. Fabryczna osłona przeciw kurzowa</li> </ol>
19.	<b>Wirtualizacja</b>	<p>Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).</p>
20.	<b>Oprogramowanie</b>	<p>Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta, w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać ich zbiorczą instalację.</p>
21.	<b>Gwarancja i wsparcie techniczne producenta</b>	<p>Min. 36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site). W razie awarii dysku twardego pozostaje on własnością Zamawiającego.</p>

		<p>Firma serwisująca posiadająca certyfikat ISO 9001:2000 lub równoważny na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.</p> <p>Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:</p> <ol style="list-style-type: none"> <li>1) fabrycznej konfiguracji urządzenia,</li> <li>2) rodzaju gwarancji,</li> <li>3) dacie wygaśnięcia gwarancji,</li> <li>4) aktualizacjach.</li> </ol> <p>Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.</p>
--	--	---

Zakup monitorów Monitory 24" 1920x1080 100Hz- 50 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne monitorów
1.	<b>Monitor</b>	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo.
2.	<b>Wielkość ekranu</b>	Przekątna ekranu min. 23,8"
3.	<b>Matryca</b>	Powłoka matrycy o wykończeniu matowym typu IPS
4.	<b>Nominalna rozdzielczość</b>	Rozdzielczość nie mniejsza niż: FHD (1920x1080)
5.	<b>Kąty widzenia</b>	Kąty widzenia min. 178 stopni w pionie i w poziomie
6.	<b>Plamka</b>	Wielkość plamki (pojedynczego piksela) nie większa niż 0.275mm
7.	<b>Częstotliwość odświeżania</b>	Nie mniejsza niż 100Hz
8.	<b>Jasność</b>	Nie mniejsza niż 250 nitów
9.	<b>Czas reakcji matrycy</b>	Nie większy niż 6ms
10.	<b>Zakres kolorów</b>	Nie mniejszy niż 99% sRGB Obsługa min. 16,7 miliona kolorów
11.	<b>Kontrast statyczny</b>	Nie mniejszy niż: 1300:1
12.	<b>Porty/złącza</b>	1x HDMI 1x DisplayPort 1x VGA
13.	<b>Waga</b>	Nieprzekraczająca 5 kg z podstawą według karty katalogowej producenta
14.	<b>Ergonomia</b>	Możliwość regulacji ustawienia monitora w zakresie: <ol style="list-style-type: none"> <li>1) Przód / tył w zakresie min. -5 do 21 stopni</li> <li>2) Lewo / prawo w zakresie 360 stopni</li> <li>3) Pivot w zakresie min. -90 do 90 stopni</li> </ol> Wysokość do min. 150mm
15.	<b>Obudowa</b>	Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej  Możliwość zainstalowania monitora na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100)  Wbudowane głośniki min. 2x 1,5W
16.	<b>Bezpieczeństwo</b>	Złącze typu Kensington Lock
17.	<b>Certyfikaty i standardy</b>	Dla producenta sprzętu należy dostarczyć certyfikat: ISO 9001, ISO 14001 lub równoważne  Dla urządzenia: <ol style="list-style-type: none"> <li>1) Energy Star</li> <li>2) TCO min. 9.0</li> </ol>

		3) EPEAT Gold dla kraju Polska według danych widocznych na stronie <a href="https://epeat.net/search-computers-and-displays">https://epeat.net/search-computers-and-displays</a> Ww. dokumenty wymagane na żądanie Zamawiającego.
18.	<b>Ukompletowanie</b>	Kabel HDMI o długości min. 1,8m Kabel zasilający o długości min. 1,8m
19.	<b>Gwarancja i wsparcie</b>	Minimum 36 miesięcy

Monitory 55" 3640x 2160 60Hz, moduł Wi-Fi/Bluetooth – 15 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne monitorów
1.	<b>Monitor</b>	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo.
2.	<b>Wielkość ekranu</b>	Przekątna ekranu min. 54-55"
3.	<b>Matryca</b>	LED typu IPS lub VA
4.	<b>Nominalna rozdzielczość</b>	Rozdzielczość nie mniejsza niż: 4K (3840x2160)
5.	<b>Kąty widzenia</b>	Kąty widzenia min. 178 stopni w pionie i w poziomie
6.	<b>Plamka</b>	Wielkość plamki (pojedynczego piksela) nie większa niż 0.315mm
7.	<b>Częstotliwość odświeżania</b>	Nie mniejsza niż 60Hz
8.	<b>Jasność</b>	Nie mniejsza niż 400 nitów
9.	<b>Czas reakcji matrycy</b>	Nie większy niż 8ms
10.	<b>Zakres kolorów</b>	Nie mniejszy niż 95% sRGB, 75% DCI-P3
11.	<b>Kontrast statyczny</b>	Nie mniejszy niż: 5000:1
12.	<b>Porty/złącza</b>	a) 2x HDMI 2.1 b) 1x DisplayPort 1.4 c) 1x DisplayPort 1.4 (Out) d) 1x line-out e) 4x USB-A 3.2 f) 1x USB-B 3.2 g) 1x USB-C 3.2 z PD 90W i DP 1.4 h) 1x RJ-45
13.	<b>Waga</b>	Nieprzekraczająca 19 kg z według karty katalogowej producenta
14.	<b>Ergonomia</b>	Możliwość regulacji ustawienia monitora w zakresie: 1) Przód / tył w zakresie min. 0 do 5 stopni
15.	<b>Obudowa</b>	1) Możliwość zainstalowania monitora na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (300x300) 2) Wbudowane głośniki min. 2x 10W
16.	<b>Certyfikaty i standardy</b>	Dla producenta sprzętu należy dostarczyć certyfikat: ISO 9001, ISO 14001 lub równoważne  Dla urządzenia: 1) Energy Star 2) EPEAT min. Silver dla UE według danych widocznych na stronie: <a href="https://epeat.net/search-computers-and-displays">https://epeat.net/search-computers-and-displays</a> Ww. dokumenty wymagane na żądanie Zamawiającego.
17.	<b>Ukompletowanie</b>	Kabel HDMI o długości min. 1,8m Kabel zasilający o długości min. 1,8m Pilot sterujący
18.	<b>Gwarancja i wsparcie</b>	Minimum 36 miesięcy

Laptopy 15.6" proc.10rdz. 16GB RAM – 31 szt.

<b>Szczegółowy opis</b>
Komputer przenośny.



Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.		
Zamawiający zastrzega sobie prawo do sprawdzenia režimu gwarancyjnego oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	<b>Procesor</b>	Procesor min. 16-rdzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core Ultra 5 225U na podstawie wyników Passmark CPU Mark, opublikowanych na stronie <a href="http://www.cpubenchmark.net/">http://www.cpubenchmark.net/</a> .
2.	<b>Pamięć operacyjna RAM</b>	Min. 16GB DDR5 5600MHz Możliwość rozbudowy pamięci do min. 64GB
3.	<b>Parametry pamięci masowej</b>	M.2 512GB SSD PCIe 4.0 x4 NVMe Przygotowana, wolna zatoka do rozbudowy komputera o dodatkowy dysk SSD.
4.	<b>Karta graficzna</b>	Zintegrowana z procesorem
5.	<b>Wyposażenie multimedialne</b>	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo 2x 2W, port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu oraz obsługująca logowanie za pomocą danych biometrycznych z Windows Hello, dwa mikrofony z funkcją wygłuszania niechcianych odgłosów tła, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszenia głośników oraz mikrofonu (mute).
6.	<b>Obudowa</b>	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H.
7.	<b>Płyta główna</b>	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny urządzenia.
8.	<b>Zgodność z systemami operacyjnymi</b>	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym
9.	<b>Bezpieczeństwo</b>	Moduł fTPM 2.0 lub dTPM 2.0  Slot typu Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington.  Dysk systemowy zawierający partycję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
10.	<b>Wirtualizacja</b>	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
11.	<b>BIOS</b>	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: 1) wersji BIOS 2) nr seryjnym komputera 3) typie procesora 4) ilości pamięci RAM  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: 1) Możliwość ustawienia hasła administratora 2) Możliwość ustawienia hasła dysku twardego

		3) Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS 4) Możliwość włączenia/wyłączenia bootowania z USB oraz PXE 5) Możliwość Wyłączania/Włączania: karty sieciowej, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, USB
12.	<b>Bezpieczeństwo – System Diagnostyczny</b>	<p>Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednocześnie przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych:</p> <ol style="list-style-type: none"> <li>Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: <ol style="list-style-type: none"> <li>pamięci ram,</li> <li>procesora,</li> <li>pamięci masowej,</li> <li> płyty głównej.</li> </ol> </li> <li>Identyfikację jednostki i jej komponentów w następującym zakresie: <ol style="list-style-type: none"> <li>urządzenie (producent, model, numer seryjny),</li> <li>bios (producent, wersja oraz data wydania),</li> <li>procesor (nazwa, taktowanie, ilości pamięci cache),</li> <li>pamięć ram (ilość zainstalowanej pamięci ram, producent),</li> <li>dysk twardy (producent, model, numer seryjny, pojemność).</li> </ol> </li> </ol>
13.	<b>Ekran</b>	Matowy, matryca IPS min. 16” 16:10 z podświetleniem w technologii LED, rozdzielczość min. WUXGA 1920x1200, jasność min. 300 nits, kąt otwarcia pokrywy ekranu min. 180 stopni.
14.	<b>Interfejsy / Komunikacja</b>	<ol style="list-style-type: none"> <li>2x USB 3.2 typu A</li> <li>1x ThunderBolt 4</li> <li>1x USB 3.2 typu C</li> <li>1x HDMI 2.1</li> <li>1x złącze audio combo</li> <li>1x RJ-45</li> <li>1x czytnik kart SD wbudowany</li> </ol> <p>Nie dopuszcza się osiągnięcia wymaganych portów USB poprzez zastosowanie przejściówek.</p>
15.	<b>Karta sieciowa WLAN</b>	Wbudowana karta sieciowa, pracująca w standardzie Wi-Fi 6E 11ax Bluetooth min. 5.3
16.	<b>Klawiatura</b>	Klawiatura odporna na zalanie cieczą, układ US, wyposażona w min. 2 tryby podświetlania przycisków (włączone, wyłączone).
17.	<b>Czytnik linii papilarnych</b>	Czytnik linii papilarnych wbudowany w klawiaturę lub przycisk zasilania. Przycisk zasilania znajdujący się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia. Nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury.
18.	<b>Akumulator</b>	O pojemności min. 45Wh
19.	<b>Zasilacz</b>	Zasilacz zewnętrzny USB-C 65W
20.	<b>Certyfikaty, oświadczenia i standardy</b>	<p>Dla producenta sprzętu certyfikat: ISO 9001, ISO 14001, ISO 50001 lub równoważne</p> <p>Dla komputera:</p> <ol style="list-style-type: none"> <li>TCO dostępne na stronie <a href="https://tcocertified.com/product-finder">https://tcocertified.com/product-finder</a></li> <li>EPEAT Gold dla kraju Polska według danych widocznych na stronie <a href="https://epeat.net/search-computers-and-displays">https://epeat.net/search-computers-and-displays</a></li> <li>Mil-STD-810H</li> <li>Deklaracja zgodności CE</li> </ol>

		<p>5) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki</p> <p>Ww. dokumenty wymagane na żądanie Zamawiającego.</p>
21.	<b>Waga</b>	Waga startowa urządzenia nie większa niż 1.75kg według karty katalogowej producenta
22.	<b>System operacyjny</b>	<p>Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> <li>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> <li>a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b) Dotykowy umożliwiający sterowanie dotykkiem na urządzeniach typu tablet lub monitorach dotykowych</li> </ol> </li> <li>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego.</li> <li>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.</li> <li>4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.</li> <li>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe.</li> <li>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.</li> <li>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</li> <li>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.</li> <li>9. Wbudowany system pomocy w języku polskim.</li> <li>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</li> <li>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</li> <li>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</li> <li>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</li> <li>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</li> <li>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</li> <li>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</li> <li>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.</li> <li>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</li> <li>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</li> <li>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</li> <li>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</li> <li>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</li> </ol>

		<p>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</p> <p>24. Wbudowany mechanizm wirtualizacji typu hypervisor.</p> <p>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</p> <p>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>27. Wbudowana zaporą internetową (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>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.).</p> <p>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.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ol style="list-style-type: none"> <li>a) Login i hasło,</li> <li>b) Karty inteligentne i certyfikaty (smartcard),</li> <li>c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> <li>d) Certyfikat/Klucz i PIN</li> <li>e) Certyfikat/Klucz i uwierzytelnienie biometryczne</li> </ol> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.</p>
23.	<b>Oprogramowanie do aktualizacji sterowników</b>	<p>Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.</p>
24.	<b>Gwarancja i wsparcie techniczne producenta</b>	<p>Minimum 36 miesięcy gwarancji producenta sprzętu, świadczonej w miejscu użytkowania (on-site).</p> <p>Bezpłatna infolinia w języku polskim, funkcjonująca minimum w godzinach 9:00 – 16:00 oraz obsługująca zgłoszenia serwisowe i oferująca wsparcie techniczne w zakresie co najmniej:</p> <ol style="list-style-type: none"> <li>1) wsparcia technicznego dla zakupionego sprzętu,</li> <li>2) weryfikacji konfiguracji fabrycznej zakupionego sprzętu,</li> <li>3) weryfikacji statusu gwarancji zakupionego sprzętu.</li> </ol>

		<p>Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:</p> <ol style="list-style-type: none"> <li>1) fabrycznej konfiguracji urządzenia,</li> <li>2) rodzaju gwarancji,</li> <li>3) dacie wygaśnięcia gwarancji,</li> <li>4) aktualizacjach.</li> </ol> <p>Diagnostyka sprzętowa dostępna na stronie internetowej producenta</p>
--	--	---

*1.13 Komputery medyczne. Panelowy komputer medyczny AIO specjalnie zaprojektowany do pracy w środowiskach medycznych, takich jak szpitale na salach operacyjnych, z powłoką antybakteryjną do użytku medycznego.*

Mobilna stacja robocza składająca się z:

#### 1. Panelu PC

- 1) Procesor minimum 13 generacji spełniający minimalne wymagania nie gorsze niż zgodny z oferowaną płytą główną: Procesor umożliwiający osiągnięcie wyniku min. 22000 punktów w teście Passmark CPU Mark dostępnym na stronie [http://www.cpubenchmark.net/cpu\\_list.php](http://www.cpubenchmark.net/cpu_list.php). Wyniki dla oferowanego modelu procesora powinny być dostępne na stronie [http://www.cpubenchmark.net/cpu\\_list.php](http://www.cpubenchmark.net/cpu_list.php)., oraz potwierdzać spełnianie wymagań zamawiającego nie wcześniej niż w dniu ukazania się ogłoszenia o zamówieniu w formie wydruku.
- 2) Wejście liniowe HDMI do wprowadzania obrazu przykładowo z kardiomonitora.
- 3) Przycisk umieszczony na panelu sterowania zapewniający szybki dostęp.
- 4) Przycisku umożliwiający czyszczenia ekranu w trakcie pracy.
- 5) Przycisku umożliwiający zabezpieczenia wyświetlacza przed niepowołanymi osobami.
- 6) Obudowa aluminiowa odprowadzająca ciepło stosownie do wydajności stacji, antybakteryjna z możliwością powierzchniowej dezynfekcji potwierdzona dokumentem MSRA.
- 7) Zintegrowany układ graficzny Minimum UHD wyjście 1 x DP 1 x HDMI, 1 x HDMI In.
- 8) Moduł pamięci komputerowej (RAM) typu DIMM DDR5 o pojemności min. 16GB maksymalnie 64MB ze wsparciem Dual-Channel.
- 9) Dysk twardy o pojemności min 512GB M2 NVME.
- 10) Liczba portów USB 3.2 : min 4.
- 11) Liczba portów RS-232C: min: 2.
- 12) Liczba portów sieci komputerowej: min 2 x RJ45 (w tym 1 x 1.0 Gbps, 1 x 2.5 Gbps).
- 13) Łączność WIFI / BT minimum 7 / 5.4.
- 14) Zasilanie 230V/50Hz złącze AC wbudowany zasilacz medyczny.
- 15) Przekątna ekranu min. 23,8" format ekranu min. 16:9 o rozdzielczość min. 1920 x 1080 i jasności min. 250 cd/m2 kontrast 1000:1, zabezpieczona powłoką antyrefleksyjną.
- 16) Panel dotykowy co najmniej 10 punktowy / przepustowość światła co najmniej 85% ± 3% / Twardość: co najmniej 6H nacisk co najmniej 750g/45° / powłoka antyrefleksyjna.
- 17) Kąt widzenia w poziomie min. 178 / w pionie min. 178 stopni.
- 18) System operacyjny: Windows 11 Enterprise IOT LTSC (64-bit.) lub równoważny. Pod pojęciem „równoważności” Zamawiający rozumie oprogramowanie posiadające co najmniej poniższe funkcjonalności:
  - a) w zakresie systemu operacyjnego zgodnego i gotowego do podłączenia do domeny z aktualnie wykorzystywaną przez zamawiającego wersją Microsoft Active Directory do zarządzania autentykacją, PKI, stacjami roboczymi, wydrukami, etc.
  - b) natywne uruchamianie aplikacji dedykowanych dla Windows będących w posiadaniu Zamawiającego w tym w szczególności oprogramowania do obsługi, systemu HIS, dostępu zdalnego i innych.
  - c) możliwość adresacji całej pamięci RAM.
- 19) Mocowanie komputera VESA 100.
- 20) Klawiatura USB z blokiem numerycznym, antybakteryjna przeznaczona do dezynfekcji powierzchniowej i mycia w wodze z detergentem.
- 21) Mysz USB antybakteryjna przeznaczona do dezynfekcji powierzchniowej i mycia w wodze z detergentem.
- 22) Przedmiot oferty zgodnie z MDR Rozporządzenie (UE) 2017/745.



## 2. Wózek jezdny zapewniający transport komputera AIO:

- 1) Wózek pod komputer i monitor pacjenta wyposażony:
  - a) Mocowanie VESA panelu PC
  - b) Kolumna aluminiowa wyposażona w szyny montażowe z przodu i z tyłu dla akcesoriów
  - c) Błat roboczy z pojemnikiem oraz przepustami kablowymi o wymiarach co najmniej 450x405mm
  - d) Półka wysuwana na klawiaturę o wymiarach co najmniej 490x150
  - e) półka na mysz przesuwana dla L i P ręcznych,
  - f) uchwyt do prowadzenia wózka,
  - g) podstawa o 4 kołach z hamulcami o wymiarach co najmniej 520x520,
- 2) Przedmiot oferty zgodnie z MDR Rozporządzenie (UE) 2017/745.

## 3.6 Segmentacja sieci, system NAC

### Segmentacja sieci, NAC Licencje

#### **Podstawowa funkcjonalność systemu NAC:**

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 1000 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 5000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
  - 1) VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
  - 2) Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
  - 1) serwera RADIUS dla infrastruktury sieciowej,
  - 2) serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
  - 3) serwera SYSLOG,
  - 4) serwera TACACS+,
  - 5) serwera Monitoringu,
  - 6) serwera DHCP,
  - 7) serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
  - 8) serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now.



16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsięciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokena wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.

47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. W języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
  - 1) Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
  - 2) Czy włączony jest firewall
  - 3) Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
  - 4) Czy jest włączone szyfrowanie dysku systemowego
  - 5) Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
  - 6) Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
  - 7) Czy w systemie są uruchomione procesy wskazane przez administratora
  - 8) Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
  - 9) Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
    - a) Wartości klucza rejestru
    - b) Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfigurator sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
  - 1) Microsoft Windows
  - 2) Mac OS
  - 3) iOS
  - 4) Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

### **Mechanizmy uwierzytelniania**

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
  - 1) MAC,
  - 2) PAP/ASCII,

- 3) CHAP,
- 4) SNMP,
- 5) 802.1X.
3. Wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
  - 1) Tożsamość/Urządzenie końcowe,
  - 2) Grupa tożsamości/urządzeń końcowych,
  - 3) Parametry urządzeń końcowych, min: system operacyjny, wersja,
  - 4) Atrybuty Active Directory,
  - 5) Jednostka organizacyjna tożsamości/urządzeń końcowych,
  - 6) Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
  - 7) Grupy urządzeń sieciowych,
  - 8) Porty urządzeń sieciowych,
  - 9) Grupy portów urządzeń sieciowych,
  - 10) Jednostka organizacyjna portów,
  - 11) Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
  - 12) Data, czas ważności polityki,
  - 13) Wewnętrzny Captive Portal,
  - 14) Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
20. System musi umożliwiać przysyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

### Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.

2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
  - 1) możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
  - 2) możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
  - 3) Możliwość generowania certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
  - 4) usługę OCSP (Online Certificate Status Protocol).

### **Obsługa serwerów DHCP**

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
  - 1) Uruchamianie usługi dla wybranych podsieci,
  - 2) Przypisanie ustalonego adresu IP dla adresu MAC.
  - 3) Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
  - 4) Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
  - 5) Możliwość określania braku dostępu dla wybranych adresów MAC,
  - 6) Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
  - 7) Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
  - 8) Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
  - 9) Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
  - 10) Dokonywanie zmian bez konieczności wyłączania usług.

### **Obsługa serwerów TACACS+**

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

### **Raportowanie i monitoring**

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostatek aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.

10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
  - 1) Logowania, wylogowania z system w tym błędne logowania
  - 2) Logowania do sieci 802.1X

### **Alarmy**

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
  - 1) wiadomości e-mail,
  - 2) Syslog,
  - 3) notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
  - 1) Ilości obsługiwanych transakcji RADIUS,
  - 2) Opóźnienie obsługi transakcji RADIUS,
  - 3) Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
  - 1) badanie łączności IP za pomocą ping, traceroute,
  - 2) tcpdump protokołów RADIUS, TACACS+,
  - 3) wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
    - a) nazwy użytkownika,
    - b) adresu MAC,
    - c) statusu uwierzytelnienia (udana lub nieudana),
    - d) powodu, jeżeli uwierzytelnienie nieudane,
    - e) zakresu czasowego, co do dnia, godziny i minuty,
  - 4) wykonanie zdalnego polecenia na urządzeniu sieciowym.

### Segmentacja sieci, NAC wdrożenie

#### **Wymagania dotyczące wdrożenia i harmonogram ramowy:**

1. Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
2. Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
3. Konfiguracja urządzenia firewall (dodatknie VLAN-u gościnnego, ustawienie polityk, etc.).
4. Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
5. Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
6. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
7. Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
8. Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie.
9. Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

#### **Szkolenia/warsztaty:**



1. Wykonawca zapewni 1-dniowe warsztaty w zakresie użytkowania i administrowania wdrożonym systemem NAC.
2. Warsztaty zostaną przeprowadzone dla maksymalnie 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC.
3. Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC.
4. Warsztaty odbędą się w formie zdalnej.
5. Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
6. Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.

#### **Licencja wsparcia technicznego producenta oprogramowania:**

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 36 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:

1. Kontakt mailowy z działem wsparcia technicznego w celu rozwiązywania problemów związanych z wdrożeniem lub obsługą systemu NAC
2. Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
3. Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
4. Dostęp do dokumentacji i instrukcji na stronie internetowej.

Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

### *3.8 Instalacja i konfiguracja systemu monitorowania infrastruktury IT (co najmniej 100 urządzeń) – rozwiązanie klasy enterprise obsługi problemów z urządzeniami sieciowymi oraz infrastrukturą krytyczną i powiadomienia o tym odpowiednio użytkownika*

1. Przedmiotem zamówienia jest zaprojektowanie, dostawa, instalacja, konfiguracja oraz uruchomienie nowoczesnego, skalowalnego i wysokodostępnego systemu monitoringu infrastruktury informatycznej, umożliwiającego kompleksowe zarządzanie stanem technicznym i wydajnością zasobów cyfrowych oraz fizycznych elementów środowiska IT Zamawiającego. System będzie monitorował krytyczne urządzenia, serwery, usługi sieciowe oraz aplikacje, zapewniał automatyczne alarmowanie i raportowanie oraz umożliwił integrację z pozostałymi systemami zarządzania.

#### **2. Wymagania funkcjonalne**

##### **2.1 Architektura i skalowalność**

System musi funkcjonować w architekturze rozproszonej z możliwością skalowania do minimum 5 tysięcy hostów i 200 tysięcy punktów pomiarowych (itemów).

Wdrożona architektura powinna zapewniać wysoką dostępność krytycznych komponentów systemu, w tym serwerów centralnych, mechanizmów baz danych oraz proxy do komentowanego środowiska monitoringu rozproszonego.

System winien umożliwiać realizację strategii backupu i szybkiego odtwarzania danych skonfigurowanych monitorowanych parametrów oraz historii zdarzeń.

##### **2.2 Monitorowane elementy i usługi**

Monitorowanie systemów operacyjnych (Linux, Windows, macOS) oraz ich kluczowych parametrów, m.in. obciążenia CPU, pamięci RAM, przestrzeni dyskowej i procesów systemowych.

Monitorowanie usług sieciowych (np. HTTP, HTTPS, FTP, SMTP, POP3, LDAP), w tym czasów odpowiedzi i statusów działania.

Monitorowanie dostępności i wydajności baz danych (m.in. MySQL, PostgreSQL, Oracle, MS SQL).



Możliwość monitorowania aplikacji biznesowych oraz dedykowanych, zgodnie ze specyficznymi wymaganiami Zamawiającego, a także urządzeń sieciowych (routery, switchy, firewalle) przy pomocy protokołów SNMP, IPMI, SSH, REST API.

Możliwość definiowania szablonów monitoringu, ułatwiających zarządzanie złożonym środowiskiem i wieloma komponentami jednocześnie.

### 2.3 Bezpieczeństwo i dostęp

Integracja mechanizmów uwierzytelniania i autoryzacji przy wykorzystaniu katalogów centralnych (LDAP, Active Directory, SAML) oraz mechanizmów jednokrotnego logowania (SSO).

Szyfrowanie danych w trakcie przesyłania (min. protokół TLS 1.2 lub wyższy).

Centralne rejestrowanie zdarzeń i audyt działań administratorów i użytkowników systemu.

### 3. Integracja i automatyzacja

System musi umożliwiać integrację z systemami obsługi zgłoszeń i zarządzania incydentami (np. ITSM, Jira, Remedy) w celu automatycznego tworzenia i aktualizacji ticketów.

Wymagana jest integracja z systemem zarządzania konfiguracją (CMDB), aby dynamicznie odzwierciedlać aktualną konfigurację środowiska.

Konfiguracja automatycznych powiadomień (email, SMS, komunikatory, webhooki) z pełnym wsparciem harmonogramów, eskalacji i reguł powiadamiania.

Możliwość definiowania działań automatycznych po wykryciu zdarzenia (np. uruchomienie skryptu naprawczego, restart usługi, generowanie raportu).

### 4. Raportowanie i wizualizacja

System musi dostarczać narzędzi do definiowania wskaźników jakości usług (SLA) i monitorowania ich realizacji.

Generowanie pełnych raportów operacyjnych i statystycznych (pdf, csv), dostępnych na żądanie oraz zaplanowanych cyklicznie.

Możliwość tworzenia konfigurowalnych dashboardów, dostosowanych do potrzeb różnych grup interesariuszy (zarząd, administratorzy, dział wsparcia).

Eksport danych i kompatybilność z narzędziami analitycznymi i BI.

### 5. Szkolenia i dokumentacja

Wykonawca zobowiązany jest zapewnić co najmniej 24 godziny szkoleń dla zespołu administratorów i operatorów systemu, obejmujące instalację, konfigurację, zarządzanie i generowanie raportów.

Dostarczenie pełnej dokumentacji wdrożeniowej i użytkowej, w tym procedur backupu, odtwarzania, zarządzania i eskalacji zdarzeń.

### 6. Wsparcie i gwarancja

Minimum 36 miesięczny okres wsparcia technicznego i gwarancji z deklarowanym czasem reagowania do 4 godzin.

Całodobowa dostępność wsparcia (24/7) dla krytycznych incydentów.

Usługi obejmujące aktualizacje oprogramowania oraz poprawki bezpieczeństwa.

### 7. Warunki kwalifikacyjne

Wykonawca musi wykazać doświadczenie w realizacji co najmniej trzech projektów wdrożenia systemów monitoringu dużej skali.

Wykonawca dysponuje wykwalifikowanym zespołem specjalistów z potwierdzonymi kompetencjami.

### *3.9 Zakup systemu klasy SIEM- wyposażonego w zautomatyzowane, pasywne i aktywne mechanizmy inwentaryzacji zasobów IT i mapowania sieci.*

**Platforma przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności.**

1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.
2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.
4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
5. System powinien pozwalać na pracę z logami zdarzeń jednoliniowych oraz wieloliniowych.
6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianę wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie
8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware
10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.
14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.
16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapelnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
17. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.
18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.

19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.
25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.
27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:
  - 1) nowe zasoby wykryte w sieci,
  - 2) typy wykrytych zasobów (np.: serwer lub stacja robocza),
  - 3) zastosowane na nich zabezpieczenia,
  - 4) usługi z którymi się komunikują,
  - 5) nowe usługi wykryte na zasobie
  - 6) komunikację do usług wykrytych na zasobie.
30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.
33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:
  - 1) fqdn,
  - 2) e-mail,

- 3) nazwa pliku,
  - 4) ścieżka do pliku,
  - 5) hash,
  - 6) adres IP,
  - 7) klucz rejestru,
  - 8) cmd.
34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>).
  35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).
  36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).
  37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.
  38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
  39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwany wynik analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).
  40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
  41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
  42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
  43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:
    - 1) id techniki,
    - 2) taktykę,
    - 3) platformy których dotyczy,
    - 4) potencjalne źródła,
    - 5) opis zagrożenia,
    - 6) mityzację,
    - 7) sposób detekcji,
    - 8) referencje.
  44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
  45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).
  46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:
    - 1) rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
    - 2) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
    - 3) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,

- 4) rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).
48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.
49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).
50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
52. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:
  - 1) sparsowane pola oraz ich wartości,
  - 2) listy referencyjne,
  - 3) atrybuty użytkowników z Active Directory,
  - 4) atrybuty komputerów z Active Directory,
  - 5) bazę wskaźników kompromitacji (IOC),
  - 6) informacje z elektronicznej dokumentacji,
  - 7) anomalie w zachowaniu użytkowników (UBA),
  - 8) anomalie w zachowaniu zasobów (EBA),
  - 9) podatności na zasobach,
  - 10) wyniki analizy konfiguracji,
  - 11) techniki MITRE ATT&CK®,
53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:
  - 1) wykrycie dowolnej treści w logach,
  - 2) wykrycie zmiany jednego z kilku pól,
  - 3) wykrycie zaniku wiadomości,
  - 4) wykrycie nowej wartości pola w zadanym okresie czasu,
  - 5) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
  - 6) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
  - 7) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
  - 8) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
  - 9) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
  - 10) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
  - 11) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
  - 12) wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
  - 13) wykrycie skanowania portów.
54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:
  - 1) wykrycie wystąpienia wartości pola na wybranej liście,
  - 2) wykrycie niewystępowania wartości pola na wybranej liście,
  - 3) wykrycie wystąpienia pary wartości na wybranej liście<sup>[1]</sup> (np.: proces i obraz pliku z którego został uruchomiony),
  - 4) wykrycie niewystąpienia pary wartości na wybranej liście
  - 5) (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).
55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:
  - 1) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
  - 2) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
  - 3) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
  - 4) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory



- (np.: Domain Admins),
- 5) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.
56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:
- 1) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
  - 2) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
  - 3) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.
57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:
- 1) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
  - 2) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
  - 3) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji.
58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:
- 1) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
  - 2) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
  - 3) wykrycie nieautoryzowanej usługi na serwerze,
  - 4) wykrycie nieautoryzowanego połączenia do usługi na serwerze,
  - 5) wykrycie nieautoryzowanego połączenia z serwera usług,
  - 6) wykrycie nieautoryzowanego połączenia do sieci Internet.
59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:
- 1) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
  - 2) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
  - 3) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
  - 4) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:
- 1) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
  - 2) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
  - 3) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
  - 4) wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:
- 1) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
  - 2) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
  - 3) wykrycie zdarzeń o wysokim „severity” na zasobach posiadających krytyczne podatności,
  - 4) wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.
62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:
- 1) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,
  - 2) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:
- 1) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
  - 2) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
  - 3) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.
64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiających, m.in.:
- 1) wykrycie anomalii na koncie uprzywilejowanym użytkownika,
  - 2) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
  - 3) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
  - 4) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z



- którego następuje nieautoryzowana próba dostępu do usługi,
- 5) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:
- 1) sparsowane pola oraz ich wartości,
  - 2) atrybuty użytkowników z Active Directory,
  - 3) atrybuty komputerów z Active Directory,
  - 4) informacje z elektronicznej dokumentacji.
66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:
- 1) adresie IP,
  - 2) koncie domenowym użytkownika,
  - 3) strefie bezpieczeństwa,
  - 4) zakresie adresów IP.
67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.
68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.
69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.
- 1) wszystkie skorelowane zdarzenia,
  - 2) korespondencja pocztowa,
  - 3) załączniki z próbkami lub dowodami,
  - 4) wskaźniki kompromitacji (IoC),
  - 5) informacje pozyskane z innych systemów.
70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.
71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.
72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:
- 1) identyfikację celu i źródła zagrożenia,
  - 2) nazwę oraz adres IP źródła zagrożenia,
  - 3) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
  - 4) lokalizację z której pochodzi zagrożenie np.: Internet,
  - 5) strefę bezpieczeństwa z której pochodzi zagrożenie,
  - 6) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
  - 7) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
  - 8) nazwę oraz adres IP celu zagrożenia,
  - 9) zabezpieczenia lokalne chroniące cel zagrożenia,
  - 10) strefę bezpieczeństwa w której znajduje się cel zagrożenia.
73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.
75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:
- 1) nazwy zasobu,
  - 2) rodzaju zasobu,
  - 3) ważności zasobu dla organizacji,
  - 4) rodzaj przetwarzanych informacji,
  - 5) usług, które ten zasób świadczy,
  - 6) lokalizację użytkowników, którzy z niego korzystają,
  - 7) usługi z których zasób korzysta.
76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.
77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:
- 1) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
  - 2) segregacja – segregacja i kwalifikacja zdarzeń,
  - 3) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
  - 4) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
  - 5) zdarzenie obsłużone – zdarzenie, które zostało obsłużone w systemie.

System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.

78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.
79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.
80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.
81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.
83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.
84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

- 1) podgląd aktywności zagrożonego zasobu na linii czasu,
  - 2) w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
  - 3) w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
  - 4) podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
  - 5) w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
  - 6) listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
  - 7) gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o:
    - a) listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
    - b) listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
  - 8) gotowe i proste w użyciu filtry rozszerzające analizę logów o:
    - a) listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
    - b) listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.
85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
- 1) warunki powiadomień,
    - a) zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
    - b) zdarzeń o przekroczonych czasach SLA o definiowalny okres,
    - c) zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
    - d) zdarzeń, których priorytet osiągnął określoną wartość,
    - e) zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
    - f) zdarzeń na których doszło do naruszenia bezpieczeństwa,
    - g) zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
    - h) zdarzeń realizujących zdefiniowaną usługę,
    - i) zdarzeń przetwarzających sklasyfikowane informacje,
    - j) zdarzeń przetwarzanych na krytycznych zasobach,
  - 2) odbiorców powiadomień, w tym:
    - a) operatora, któremu zostało przydzielone zdarzenie,
    - b) właściciela zasobu na którym wystąpiło zdarzenie,
    - c) zespół obsługi, który odpowiada za obsługę zdarzeń,
    - d) właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
    - e) podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
  - 3) kanały powiadomień, m.in. e-mail, sms, komunikator,
  - 4) zastosowanie mechanizmów grupowania:
    - a) grupowanie wielu powiadomień w jednej wiadomości,
    - b) ograniczenie liczby wierszy powiadomienia do określonej wartości.
86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
- 1) utworzenia nowego zdarzenia z określonym priorytetem,
  - 2) utworzenia nowego zdarzenia na zasobie krytycznym,
  - 3) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
  - 4) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
  - 5) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
  - 6) modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
  - 7) zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
  - 8) przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.
87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:
- 1) wybór raportu, który ma zostać wysłany,
  - 2) zdefiniowanie jego tytułu,
  - 3) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
  - 4) możliwość ograniczenia cyklu do dni powszednich,
  - 5) określenie daty przesłania pierwszego raportu,
  - 6) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
    - a) zdefiniowanej daty końcowej,
    - b) określonej liczby raportów,
  - 7) określenie odbiorców raportu.
88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczają dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:
- 1) strefę bezpieczeństwa w której została wykryta podatność,
  - 2) prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
  - 3) rodzaj zasobu którego dotyczy ta podatność,
  - 4) ważność tego zasobu dla organizacji,
  - 5) przetwarzane na tym zasobie informacje, np.: dane osobowe,
  - 6) usługi realizowane przez ten zasób, np.: DNS,
  - 7) wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
  - 8) poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
  - 9) szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.
90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:
- 1) wyliczonym priorytecie podatności,
  - 2) aktualnym statusie obsługi,
  - 3) ważności zasobu na którym została wykryta,
  - 4) adresie IP tego systemu,
  - 5) parametrów SLA związanych z tym statusem,
  - 6) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
  - 7) parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV)” = „Network”.
92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:
- 1) przekroczenia czasu reakcji o określony czas np.: o godzinę,
  - 2) możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
  - 3) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
  - 4) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
  - 5) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
  - 6) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
  - 7) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
  - 8) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
  - 9) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
  - 10) przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
  - 11) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,
93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
- 1) warunki powiadomień,
    - a) podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
    - b) podatności o przekroczonych czasach SLA o definiowalny okres,
    - c) podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
    - d) podatności, których priorytet osiągnął określoną wartość,
    - e) zdarzeń realizujących zdefiniowaną usługę,
    - f) zdarzeń przetwarzających sklasyfikowane informacje,
    - g) zdarzeń przetwarzanych na krytycznych zasobach,
  - 2) odbiorców powiadomień, w tym:

- a) operatora, któremu została przydzielona podatność,
  - b) właściciela zasobu na którym wystąpiła podatność,
  - c) zespół obsługi, który odpowiada za obsługę podatności,
  - d) właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
  - e) podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.
- 3) kanały powiadomień, m.in. e-mail, sms, komunikator,
  - 4) zastosowanie mechanizmów grupowania:
    - a) grupowanie wielu powiadomień w jednej wiadomości,
    - b) ograniczenie liczby wierszy powiadomienia do określonej wartości.
94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
- 1) przydzielenia nowej podatności do obsługi z określonym priorytetem,
  - 2) przydzielenia nowej podatności do obsługi na zasobie krytycznym,
  - 3) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
  - 4) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
  - 5) modyfikacji przydzielonej operatorowi podatności przez innego operatora,
  - 6) zamknięcia przydzielonej operatorowi podatności przez innego operatora,
  - 7) przejścia przydzielonej operatorowi podatności przez innego operatora.
95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:
- 1) wybór raportu który ma zostać wysłany,
  - 2) zdefiniowanie jego tytułu,
  - 3) zdefiniowanie cyklu w jakim ma zostać wysłany, np.: tygodniowy lub miesięczny,
  - 4) możliwość ograniczenia cyklu do dni powszednich,
  - 5) określenie daty przesłania pierwszego raportu,
  - 6) określenie okresu przez jaki będą one przesyłane, poprzez:
    - a) zdefiniowanie daty końcowej,
    - b) bez daty końcowej,
    - c) określenie liczby raportów,
  - 7) określenie odbiorców raportu.
96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.
97. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących:
- 1) zestaw wykresów dla bieżącego użytkownika,
  - 2) zestaw wykresów dla wybranego użytkownika,
  - 3) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
  - 4) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).
98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:
- 1) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
    - a) ilość zdarzeń nowych i niesklasyfikowanych,
    - b) ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
    - c) ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
  - 2) wykres przedstawiający skalę zagrożeń, który uwzględnia:
    - a) ilość zasobów krytycznych na których są obsługiwane zdarzenia,
    - b) ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
  - 3) wykres przedstawiający źródła zagrożeń, który uwzględnia:
    - a) ilość nowych zdarzeń dotyczących użytkowników,
    - b) ilość podjętych zdarzeń dotyczących użytkowników,
    - c) ilość nowych zdarzeń dotyczących zasobów,
    - d) ilość podjętych zdarzeń dotyczących zasobów,
  - 4) wykres przedstawiający poziom zagrożeń, który uwzględnia:
    - a) ilość nowych zdarzeń w podziale na priorytety,
    - b) ilość podjętych zdarzeń w podziale na priorytety,
  - 5) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
    - a) ilość zdarzeń zarejestrowanych w bieżącym dniu,
    - b) ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
    - c) ilość zdarzeń zarejestrowanych w ostatnim miesiącu,



- d) ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
  - 6) wykres przedstawiający zagrożone usługi, który uwzględnia:
    - a) ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
    - b) ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
  - 7) wykres przedstawiający zagrożone dane, który uwzględnia:
    - a) ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
    - b) ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
    - c) ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
    - d) ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
  - 8) wykres przedstawiający skalę podatności, który uwzględnia:
    - a) ilość zasobów krytycznych na których są obsługiwane podatności,
    - b) ilość zasobów niekrytycznych na których są obsługiwane podatności,
  - 9) wykres przedstawiający czas obsługi podatności, który uwzględnia:
    - a) ilość podatności zarejestrowanych w bieżącym dniu,
    - b) ilość podatności zarejestrowanych w ostatnim tygodniu,
    - c) ilość podatności zarejestrowanych w ostatnim miesiącu,
    - d) ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
  - 10) wykres przedstawiający wagę podatności, który uwzględnia:
    - a) ilość nowych podatności w podziale na priorytety,
    - b) ilość podjętych podatności w podziale na priorytety,
99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:
- 1) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
  - 2) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
  - 3) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
  - 4) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
  - 5) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
  - 6) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.
100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:
- 1) kolektor parsujący;
  - 2) kolektor logów;
  - 3) kolektor korelacyjny;
  - 4) kolektor zdarzeń;
  - 5) kolektor sztucznej inteligencji;
  - 6) kolektor reakcyjny;
  - 7) kolektor kontrolujący.
102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na



- sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.
103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tys zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.
  104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.
  105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).
  106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.
  107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.
  108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.
  109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszą być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.
  110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.
  111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.
  112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.
  113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tys zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.
  114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.).
  115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.
  116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.
  117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.
  118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.
  119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów,

- raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.
120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).
  121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.
  122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów.
  123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).
  124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).
  125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:
    - 1) zdolność do definiowania wzorców które powtarzają się jako zmienne;
    - 2) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;
    - 3) zdolność do testowania poszczególnych funkcji;
    - 4) zdolność do przekształcania danych w trakcie ich parsowania.
  126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:
    - 1) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;
    - 2) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;
    - 3) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;
    - 4) zdolność do monitorowania integralności plików;
    - 5) zdolność do monitorowania rejestru systemowego;
    - 6) zdolność do monitorowania urządzeń zewnętrznych (removable devices);
    - 7) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;
    - 8) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemem;
    - 9) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;
    - 10) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.
  127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.
  128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI.
  129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Intelligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.
  130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).
  131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi.
  132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal.
  133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.
  134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.
  135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.
  136. System musi wierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyłeń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać

wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.

## System SOAR

1. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.
2. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalnościami będzie mógł je potwierdzić lub im zaprzeczyć.
3. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.
4. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencja nie może nakładać limitów w tym zakresie.
5. Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać 100 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.
6. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
7. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.
8. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
9. Dostarczone rozwiązanie musi być objęte 36 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędów krytycznych lub poważnych).
10. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.
11. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 10 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/systemów. Szkolenia mogą odbyć się w formie zdalnej.
12. System XDR powinien posiadać następujące cechy i funkcjonalności
  - a) Powinien posiadać możliwość instalacji agenta XDR na systemach:
    - b) Windows 10 i nowsze,
    - c) Windows Server 2016 i nowsze.Agent umożliwia: zbieranie logów ze stacji końcowej/serwera do modułu SIEM, dodawania i wyłączanie reguł zapory sieciowej na stacji końcowej/serwerze, zawieszanie i odwieszanie procesu na stacji końcowej/serwerze. Dodatkowo zapewnia mechanizm do instalacji oraz zarządzania konfiguracją narzędzia Microsoft Sysmon na stacjach końcowych/serwerach, w celu rozszerzenia logów systemowych o aktywność procesów, plików oraz rejestrów.
  - 2) System powinien być wyposażony w serwer aplikacji udostępniający konsolę graficzną dla operatorów oraz sterujący działaniem orkiestratora oraz kontrolera

- 3) System powinien posiadać Orkiestrator służący do wykonania akcji na innych systemach niż komputery, na których zainstalowany jest agent XDR, np.: zablokowanie ruchu wychodzącego na Firewall dla hosta na którym zainstalowany jest agent służy do zarządzania agentami XDR i jest odpowiedzialny zarówno za ich monitorowanie, aktualizację oraz zlecanie im zadań, np.: izolacja procesu czy izolacja sieciowa
- 4) Agent XDR powinien wzbogacać analizę zdarzeń na nim występujących o pełne dane telemetryczne.
- 5) System powinien posiadać centralny kontroler zarządzający agentami XDR oraz monitorujący ich pracę
- 6) System powinien posiadać mechanizm wykrywania zagrożeń zgodny z taktykami i technikami Mitre Att&ck™
- 7) System powinien umożliwiać wykrywanie zagrożeń na komputerze na bazie wielu wskaźników naruszeń bezpieczeństwa (IoC)
- 8) System powinien umożliwiać centralną korelację zdarzeń z komputera względem innych zdarzeń (sieć, chmura, Threat Intel)
- 9) System powinien być wyposażony w mechanizmy uczenia maszynowego obejmujące analizę behawioralną komputera oraz jego użytkownika
- 10) System powinien posiadać wiele algorytmów wykrywania anomalii oraz profilowania komputera i jego użytkownika
- 11) System powinien umożliwiać rozszerzoną analizę behawioralną użytkownika komputera względem pracy innych użytkowników
- 12) System powinien umożliwiać kontrolę aplikacji zainstalowanych na stacjach roboczych i serwerach
- 13) System powinien umożliwiać kontrolę podatności, zgodności oraz zainstalowanych poprawek
- 14) System powinien mieć możliwość zaawansowanej analizy zdalnej np.: uruchomione procesy czy połączenia sieciowe
- 15) System powinien posiadać mechanizmy automatyzujące reakcję na komputerze z poziomu agenta, np.: wstrzymanie procesu, blokada portu
- 16) System powinien posiadać funkcjonalność dostosowania reakcji na zagrożenia w zależności od rodzajów zagrożeń (konfigurowalne playbooks)
- 17) System musi być wyposażony w autonomiczny mechanizm oceny ryzyka dla wykrytych zagrożeń
- 18) System powinien umożliwiać zarządzanie zgodnością (Compliance): KSC/KRI/GDRP
- 19) System powinien posiadać panel do zarządzania incydentami oraz podatnościami wsparty playbookami
- 20) System powinien posiadać przejrzyste dashbordy z możliwości drążenia danych oraz wizualizacji zagrożeń
- 21) System powinien posiadać możliwości powiadamiania o zagrożeniach poprzez e-mail, sms.
13. System umożliwia stworzenie kompletnych w zasoby informacji rejestrów spełniających wymogi art. 30 RODO m. in. rejestru czynności oraz rejestru kategorii czynności przetwarzania zawierających informacje dotyczące przede wszystkim:
  - 1) celu/kategorii przetwarzania
  - 2) związku z procesem,
  - 3) określenia kategorii danych wraz z kategorią osób, których dane są przetwarzane
  - 4) oznaczenia podstawy prawnej oraz wymaganej zgody na przetwarzanie danych
  - 5) określenia źródła danych
  - 6) informacją na temat retencji danych / planowanego terminu usunięcia
  - 7) wskazania systemów i oprogramowania do przetwarzania danych wraz z określeniem ich zabezpieczeń
  - 8) określenia zastosowanych środków bezpieczeństwa - organizacyjnych i technicznych i wielu innych istotnych z punktu widzenia właściwej ochrony dla przetwarzanych danych osobowych.
14. System umożliwia ewidencjonowanie umów powierzenia przetwarzania danych osobowych zarówno dla danych, których użytkownik jest Administratorem jak i Procesorem.
15. System umożliwia prowadzenie rejestru udostępnień danych osobowych wraz z określeniem wszystkich stosownych, wymaganych przepisami prawa informacji na temat udostępnień.
16. System pozwala na nadawanie upoważnień dla osób przetwarzających dane osobowe w sposób indywidualny jak i zbiorczy. Ponadto dzięki wbudowanemu elektronicznemu obiegowi dokumentów (workflow) proces nadawania i akceptacji upoważnień jest w pełni zautomatyzowany.
17. System maksymalnie usprawnia proces inwentaryzacji obszarów przetwarzania danych osobowych poprzez wyszukiwanie systemów IT przetwarzających tego typu dane jak również grup i kategorii danych osobowych.
18. System wyznacza dostępne zabezpieczenia techniczne w odniesieniu do potencjalnych źródeł zagrożenia dla systemów IT przetwarzających dane osobowe
19. System automatycznie wykonuje analizę ryzyka danych osobowych w odniesieniu do zagrożeń natury informatycznej oraz wykonuje ocenę skutków dla ochrony danych dla trzech głównych ryzyk: ryzyka utraty poufności, integralności oraz dostępności danych osobowych.
20. Analiza ryzyka obejmuje również aspekty nie informatyczne i jest wyliczana zgodnie z wytycznymi



opisanymi standardem ISO 29134.

21. System wykonuje analizę ryzyka dla przetwarzanych danych osobowych wraz z określeniem zarówno zagrożeń jak i konsekwencji na jakie narażone są osoby fizyczne z związku z przetwarzaniem ich danych osobowych.
22. System umożliwia szacowanie ryzyka od momentu wdrażania organizacyjnych i technicznych środków bezpieczeństwa przez cały proces przetwarzania danych osobowych w organizacji. Cały proces monitorowania poziomu zagrożeń oraz zapewniania rozliczalności w odniesieniu do zastosowanych zabezpieczeń jest więc procesem ciągłym i na bieżąco dostrajanym.
23. System zapewnia spełnienie wymagań formalno-prawnych dotyczących raportowania naruszeń bezpieczeństwa danych osobowych zgodnie z art. 33 pkt 5 RODO umożliwiając w pełni automatyczne generowanie „Raportu naruszenia ochrony danych osobowych dla organu nadzorczego” łącznie z wyznaczeniem możliwych konsekwencji naruszenia bezpieczeństwa
24. System automatyzuje wykonywanie oceny skutków dla ochrony danych osobowych wraz z automatycznym generowaniem raportów w obszarze analizy ryzyka cyberzagrożeń (art. 35 RODO)
25. System umożliwia rejestrację zgłoszeń incydentów dotyczących danych osobowych związanych ze zbiorami danych osobowych, jednostkami organizacyjnymi, osobami, lokalizacjami oraz zasobami informatycznymi.
26. System umożliwia obsługę incydentów związanych z przetwarzaniem danych osobowych zapewniając możliwość automatycznego ich wykrywania na podstawie logów z systemów informatycznych biorących udział w ich przetwarzaniu. System umożliwia dostrojenie reguł wykrywania zarówno w kontekście informacji pozyskanych z logów jak i parametrów elektronicznej dokumentacji związanej z ich przetwarzaniem. Dedykowana obsługa pozwala na automatyczne przydzielenie zespołu obsługi do incydentu, dotyczącego zasobu przetwarzającego dane osobowe oraz uruchomieniu adekwatnego scenariusza obsługi, np.: dla konsekwencji wycieku danych osobowych.
27. System zapewnia możliwość rejestracji i obsługi wniosków i roszczeń klientów związanych z przetwarzaniem danych osobowych np.: żądanie usunięcia czy sprostowania danych osobowych oraz żądanie otrzymania kopii tych danych.
28. System umożliwia drukowanie prowadzonych rejestrów czynności przetwarzania/kategorii czynności przetwarzania, rejestrów powierzeń oraz udostępnień ja również pojedynczych rekordów z wymienionych rejestrów.
29. System pozwala opracowywać plany postępowania z ryzykiem wraz z określeniem terminowości, ustanowieniem poszczególnych zadań, przypisaniem zespołów obsługi oraz pełną ich rozliczalnością.
30. System pozwala na przechowywanie dokumentów dotyczących systemu ochrony danych osobowych umożliwiając użytkownikom śledzenie zmian w dokumentach, informowanie o zmianach oraz pełnym nadzorem nad dostępem do dokumentów.

### *3.10 Zakup oprogramowania do wykonywania kopii bezpieczeństwa 15 maszyn wirtualnych*

#### **1. Wymagania ogólne**

- 1) Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 20 VM oraz 3 serwerach fizycznych.
- 2) Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- 3) Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- 4) Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
- 5) Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

#### **2. Całkowite koszty posiadania**

- 1) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- 2) Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)

- 3) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
- 4) Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- 5) Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
- 6) Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- 7) Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- 8) Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
- 9) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- 10) Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji
- 11) Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- 12) Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- 13) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

### 3. Wymagania RPO

- 1) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
- 2) Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- 3) Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
- 4) Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
- 5) Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- 6) Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
- 7) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
- 8) Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- 9) Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- 10) Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- 11) Repozytoria oparte o XFS muszą pozwalać na niezmienną danych przez określoną ilość czasu (tzw Immutability).
- 12) Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-



V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

- 13) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
- 14) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
- 15) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

#### 4. Wymagania RTO

- 1) Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- 2) Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- 3) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
- 4) Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
- 5) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- 6) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- 7) Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- 8) Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- 9) Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
  - a) Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  - b) BSD: UFS, UFS2
  - c) Solaris: ZFS, UFS
  - d) Mac: HFS, HFS+
  - e) Windows: NTFS, FAT, FAT32, ReFS
  - f) Novell OES: NSS
- 10) Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- 11) Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- 12) Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- 13) Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
- 14) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
- 15) Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
- 16) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych.
- 17) Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
- 18) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych.
- 19) Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

- 20) Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
- 21) Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

## **5. Ograniczenie ryzyka**

- 1) Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- 2) Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- 3) Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- 4) Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
- 5) Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

## **6. Monitoring**

- 1) System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- 2) System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsolę vCenter Server lub pracujące samodzielnie
- 3) System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- 4) System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
- 5) System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- 6) System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- 7) System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- 8) System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- 9) System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- 10) System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- 11) System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- 12) System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- 13) System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- 14) System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- 15) System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

- 16) System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy Vmware.
- 17) System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x.

## 7. Raportowanie

- 1) System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022
- 2) System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- 3) System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
- 4) System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- 5) System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- 6) System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- 7) System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- 8) System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- 9) System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- 10) System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- 11) System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- 12) System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- 13) System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- 14) System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
- 15) System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
- 16) System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- 17) System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

### 3.11 Macierz do przechowywania kopii zapasowych danych medycznych oraz obrazowych o pojemności 100TB

Macierz dyskowa		
Lp.	Nazwa parametru	Minimalna wartość parametru
1.	<b>Obudowa</b>	Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19". Obudowa umożliwiająca instalację min. 12 dysków 2,5" i 3,5" z możliwością wkładania i wyjmowania, bez wyłączania macierzy (dyski typu Hot Swap)
2.	<b>Pojemność:</b>	Macierz musi zostać dostarczona w konfiguracji zapewniającej min. 175TB powierzchni użytkowej przy zastosowaniu grupy RAID5. Macierz musi wspierać dyski: 1) SSD: od 960GB do 3.84TB 2) NLSAS: od 4TB do 22TB. Macierz musi mieć możliwość rozbudowy do minimum 84 dysków hot-swap. Macierz musi być macierzą umożliwiającą jednoczesną konfigurację dysków SSD i NLSAS HDD.

3.	<b>Kontroler</b>	Dwa kontrolery macierzy wyposażone w przynajmniej 8GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania baterijnego przez 72 godziny lub jako zrzut na pamięć flash. Zawartość cache musi być mirrorowana (kopia lustrzana) między kontrolerami.
4.	<b>Interfejsy</b>	Oferowana macierz musi posiadać minimum: 1) 4 porty 16Gb FC na kontroler, 2) 1 porty RJ-45 1000 Mb Ethernet typu out-of-band management, na kontroler. 3) 2 porty SAS 12Gb/s do podłączenia dodatkowych półek, na kontroler. Macierz musi pozwalać na wymianę 4 portów FC na 4 porty 10/25Gb iSCSI SFP28 lub 2 porty SAS 12Gb bez potrzeby wymiany kontrolera macierzy. Powinny zostać dostarczone 4 wkładki 16Gb FC.
5.	<b>RAID</b>	Kontrolery macierzy muszą umożliwiać konfigurację dysków w RAID: 0, 1, 5, 6, 10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 48 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.
6.	<b>Obsługiwane protokoły</b>	Macierz musi obsługiwać protokoły FC, iSCSI.
7.	<b>Inne wymagania</b>	<p>Macierz musi posiadać wsparcie dla systemów: Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere.</p> <p>Macierz musi posiadać funkcjonalność wykonywania minimum 128 kopii migawkowych typu copy-on-write, z możliwością rozbudowy do 512 kopii migawkowych na system. Macierz musi posiadać funkcjonalność replikacji asynchronicznej. Jeżeli do funkcjonalności replikacji wymagana jest dodatkowa licencja, nie musi być ona obecnie dostarczona.</p> <p>Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.</p> <p>Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji.</p> <p>Macierz musi pochodzić od tego samego producenta co serwery rack objęte niniejszym zapytaniem.</p> <p>Macierz musi posiadać funkcjonalność thin provisioning.</p> <p>Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.</p> <p>Macierz musi posiadać oprogramowanie pozwalające na integrację z VMware vCenter.</p> <p>Macierz musi zapewniać możliwość szyfrowania danych przy użyciu dysków typu FIPS SSD oraz FIPS NLSAS HDD. Realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.</p> <p>Producent macierzy musi posiadać oficjalne przedstawicielstwo w Polsce oraz posiadać certyfikaty ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne.</p>
8.	<b>Gwarancja i serwis</b>	Minimum 36 miesięczny okres gwarancyjny realizowany przez producenta w trybie 365x7x24. Wymagana jest obsługa zgłoszeń między 9:00-17:00 w dni robocze w języku polskim. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych

		<p>następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Wszystkie uszkodzone dyski pozostają u Zamawiającego.</p> <p>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta powinien rozpocząć naprawę minimum następnego dnia roboczego od zakończenia diagnostyki zdalnej. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</p> <p>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja/ portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników.</p> <p>Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.</p> <p>Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Możliwość rozszerzenia gwarancji przez producenta do 5 lat. Możliwość rozszerzenia wsparcia o serwis z lepszym SLA – gwarantującym 24 godzinny czas naprawy sprzętu.</p>
--	--	--

## 1.6 Zakup usługi kopia w chmurze dla newralgicznych systemów

### 1. Przedmiot zamówienia obejmuje:

- 1) Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych poprzez dostawę, konfigurację oraz wdrożenie **Odmiejscowionej Infrastruktury Backupowej** (zakup praw do korzystania z usługi **Oracle Paas& IaaS Universal Credit lub równoważnej** wraz z weryfikacją poprawności wykonanej kopii na okres **36 miesięcy**;
- 2) Usługa backupu świadczona będzie zgodnie z warunkami i zasadami zawartymi w dokumencie „*Oracle PaaS and IaaS Universal Credits Service Descriptions*”, publikowanymi przez dostawcę usługi chmurowej na stronie: <https://www.oracle.com/a/ocom/docs/paas-iaas-universal-credits-3940775.pdf>;
- 3) Usługa świadczona będzie przez **36** kolejnych miesięcy od dnia podpisania Umowy, poprzez udostępnienie na potrzeby Zamawiającego Universal Credits w ilości 40 000 jednostek.

### 2. Zakres prac obejmuje:

- 1) Konfigurację tenanta w OCI
- 2) Uruchomienie usługi backupu baz danych Oracle w chmurze OCI
- 3) Comiesięczną weryfikację poprawności odtworzenia kopii RMAN każdej bazy danych nie rzadziej niż raz w miesiącu przez cały okres 36 miesięcy + każdorazowe dostarczenie raportu
- 4) Przeszkolenie administratorów Zamawiającego w zakresie wdrożonego rozwiązania,

### 3. Wymagania:

#### 4. Równoważność

- 1) Wykonawca jest partnerem Oracle, posiadającym prawo odsprzedaży usług chmurowych dla Sektora Publicznego w Polsce, który podpisał z Oracle Polska Sp. z o.o. dodatek dotyczący sektora publicznego do Ramowej Umowy Dystrybucyjnej w ramach Programu Oracle Partner Network oraz załącznik dotyczący sektora publicznego do dodatku dotyczącego dystrybucji usług w chmurze do Ramowej Umowy Dystrybucyjnej w ramach Programu Oracle Partner Network.

Zakup praw do korzystania z usługi równoważnej usłudze Oracle Paas & IaaS Universal Credit

Za usługę równoważną Zamawiający uzna taką, która spełniać będzie poniższe warunki:

- 1) umożliwia dostęp do usług chmurowych typu Platform as a Services (PaaS) oraz Infrastructure as a Service (IaaS) bez określania, jakie to mają być usługi i bez konieczności oddzielnego zakupu licencji (niezbędne do uruchomienia i funkcjonowania usługi licencje będą dostępne w modelu „License Included”),
- 2) Zamawiający będzie mógł dowolnie zmieniać usługi, z jakich będzie korzystał w okresie realizacji zamówienia,
- 3) zakres zastosowania technologii zapewni Zamawiającemu możliwość implementacji funkcjonalności, które Zamawiający realizuje w oparciu o technologię Oracle, w szczególności umożliwi Zamawiającemu utrzymywanie jego systemu szpitalnego AMMS produkcji Asseco SA (Asseco Medical Management System) opartego o bazę danych Oracle w wersji Enterprise nie niższej niż 11.2, bez konieczności zakupu dodatkowych licencji, wykonywania dodatkowych prac dostosowawczych czy migracji,
- 4) będzie współdziałać z pozostałymi systemami Zamawiającego zbudowanymi w oparciu o technologię Oracle, wdrożonymi u Zamawiającego, do których Zamawiający posiada prawa licencyjne oraz będzie zapewniać pracę tych systemów tak jak realizuje to technologia Oracle, bez konieczności zakupu dodatkowych licencji, wykonywania dodatkowych prac dostosowawczych czy migracji,
- 5) nie będzie powodować zakłóceń pracy oprogramowania z zakresu technologii Oracle, z którym będzie współdziałało,
- 6) zapewni pełną, równoległą pracę w czasie rzeczywistym oraz pełną funkcjonalną zamienną technologii równoważnej z technologią Oracle, umożliwi wskazanie miejsca przetwarzania danych na terenie Europejskiego Obszaru Gospodarczej (EOG, ang. European Economic Area) i uniemożliwi ich przekazanie przez procesora w jakiegokolwiek formie (np. backup, logi) poza ten obszar opisane pod linkiem: [Learn about the Oracle European Union Sovereign Cloud](#)



## V. Część nr 3

### Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, "Ekran dotykowy 13,3 " (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" oraz licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożenie oprogramowania oraz urządzeń mobilnych

Rozbudowa i integracja systemu szpitalnego o możliwość elektronicznego podpisu dokumentów za pomocą urządzeń do zbierania podpisu oraz czytników e-Dowodów – zakup systemu cyfryzacji dokumentacji wymagającej podpisu pacjenta w placówce medycznej **zintegrowanego z systemem HIS AMMS** wraz z dostawą urządzeń do cyfryzacji podpisu i wyświetlania treści, szkoleniem dla personelu oraz usługą wsparcia.

Ogólny opis

Przedmiotem zamówienia jest dostawa i wdrożenie systemu do automatycznej digitalizacji dokumentacji (dalej: System). System ma umożliwiać digitalizację pisma odręcznego.

Zakres prac

**W ramach zamówienia Wykonawca zobowiązany jest do:**

1. Dostawy sprzętu umożliwiającego wykonanie funkcjonalności Systemu – długopisy cyfrowe (2 sztuki), ekrany wraz z uchwytyami montowanymi do ściany (5 sztuk), tablety mobilne (12 sztuk).
2. Dostawy licencji na system w liczbie sztuk 19.
3. Instalacji i wdrożenia systemu automatycznej digitalizacji dokumentacji wraz z integracją z posiadanym środowiskiem systemu Medycznego HIS AMMS w jednostce Zamawiającego.
4. Przeprowadzenia odpowiednich szkoleń w zakresie administrowania i użytkowania Systemu.
5. Przygotowanie dokumentacji formularzowej.
6. Świadczenia opieki serwisowej wraz z nadzorem autorskim dla wszystkich przekazywanych licencji na System przez okres 36 miesięcy od daty zakończenia wdrożenia.

#### *1.8 Zakup urządzeń mobilnych*

1. Tablet mobilny powinien posiadać rozdzielczość min. WQXGA+ (2880x1800) i przekątną co najmniej 12 cali.
2. Tablet powinien działać na systemie operacyjnym Android.
3. Tablet nie powinien przekraczać wymiarów 31cmx20cmx0,7cm.
4. Tablet nie powinien przekraczać wagi 670g.
5. Tablet mobilny powinien być wyposażony w dedykowany rysik, jednocześnie, w razie awarii samego rysika, umożliwiając jego wymianę.
6. Rysik powinien posiadać czułość co najmniej 2000 poziomów nacisku.
7. Zamawiający wymaga 24 miesięcznej gwarancji na ekran liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu.

*1.9 Zakup czytników z podwójnym interfejsem. e-Dowody oraz stykowych kart procesorowych (np. podpis elektroniczny) Czytnik musi spełniać wymagania techniczne wskazane przez MSWiA dla czytników e-Dowodów bez PINPADu.*

Wymiary	120.5 mm (długość) x 72.0 mm (szerokość) x 20.4 mm (wysokość)
Waga	140.0 g
Interfejs USB	USB typu A 2.0 Full Speed
Długość przewodu	2.0 m
Interfejs kart stykowych	Format karty: Standardowy (ID-1) - 85.60 mm x 53.98 mm Standard: ISO 7816 Class A, B, C (5 V, 3 V, 1.8 V)

	Protokoły: T=0; T=1
Interfejs kart zbliżeniowych	Standard: ISO 14443 A & B Parts 1-4 lub równoważne Protokoły: ISO 14443-4 Compliant Card, T=CL MIFARE® Classic Card, T=CL
Zasięg	do 50 mm (zależy od typu znacznika)
Interfejs kart SAM	Standard: ISO 7816 Class A (5V) lub równoważne Protokoły: T=0; T=1
Certyfikaty / Zgodności	ISO 14443, ISO 7816, lub równoważne, PC/SC, CCID, CE, FCC, RoHS 2, REACH, USB Full Speed, Microsoft® WHQL
Obsługiwane systemy operacyjne	Windows® Linux® Mac OS® Android™ od wersji 3.1

*1.10 Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, "Ekran dotykowy 13,3 " (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" oraz licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożeniem oprogramowania.*

Zakup urządzeń do zbierania podpisów tj. Długopisów cyfrowych ze stacją dokującą, oraz podkładką, 2 szt.

Ekran 13,3" (niemobilne, dotykowy), wraz z akcesoriami i obudową enterprise" 5 szt.

Licencji oprogramowania do cyfryzacji zgód oraz oświadczeń woli pacjentów w sprawach związanych z leczeniem pacjenta wraz z wdrożeniem oprogramowania.

#### *1.10.1 Długopis cyfrowy*

1. Pamięć długopisu powinna wystarczyć na co najmniej 1000 wypełnionych stron A4 zanim będzie potrzeba jego synchronizacji i przesłania danych do Systemu.
2. Długopis cyfrowy musi posiadać czułość co najmniej 250 poziomów nacisku.
3. Długopis powinien mieć wbudowany akumulator litowo-jonowy lub litowo-polimerowy i umożliwiać ładowanie przez port USB.
4. Maksymalny czas pełnego ładowania nie może przekraczać 2,5 godziny.
5. Minimalny czas ciągłego pisania nie może być krótszy niż 5 godzin.
6. Waga długopisu cyfrowego nie może przekroczyć 35g.
7. Długopis powinien wytrzymać upadek na dowolną powierzchnię z wysokości maksimum 1,5m.
8. Długopis cyfrowy powinien zostać dostarczony ze stacją dokującą umożliwiającą ładowanie oraz komunikację ze stacją roboczą.
9. Przesłanie danych do Systemu powinno być możliwe za pomocą portu USB 2.0.
10. Zamawiający wymaga 24 miesięcznej gwarancji na długopis liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu. Serwis obejmuje wymianę sprzętu na nowy w razie zaistnienia takiej konieczności.

#### *1.10.2 Ekran do podpisu - dotykowy*

1. Ekran powinien posiadać rozdzielczość min. Full HD (1920x1080) i przekątną co najmniej 13 cali.
2. Ekran powinien być podłączany do komputera za pomocą portów USB-C.
3. Ekran nie powinien przekraczać wymiarów 34cmx23cmx1,5cm
4. Ekran nie powinien przekraczać wagi 950g.
5. Rysik dołączony do ekranu powinien posiadać czułość co najmniej 4000 poziomów nacisku

6. Dedykowany rysik do ekranu powinien mieć możliwość przymocowania go na stałe, jednocześnie, w razie awarii samego rysika, umożliwiając jego wymianę.
7. Zamawiający wymaga 36 miesięcznej gwarancji na ekran liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu.

#### *1.10.3 Minimalne warunki licencji na system*

1. Z chwilą dostarczenia danego rozwiązania lub jego części dla Zamawiającego, Wykonawca udzieli (z chwilą dostarczenia, bez konieczności składania dodatkowych oświadczeń woli) niewyłącznej licencji na takie rozwiązanie, na czas nieokreślony od daty podpisania przez Zamawiającego końcowego protokołu odbioru bez uwag i zastrzeżeń, na następujących polach eksploatacji:
  - a. wprowadzanie do pamięci komputera,
  - b. korzystanie,
  - c. sporządzanie kopii zapasowej,
  - d. przenoszenie pomiędzy stanowiskami.
2. Zamawiający w ramach udzielonej licencji uprawniony będzie do korzystania z wygenerowanych za pomocą danego rozwiązania dokumentów (np. raportów, analiz) w szczególności poprzez:
  - a. opracowanie, w tym zmianę, adaptację, tłumaczenie,
  - b. utrwalanie lub zwielokrotnianie w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu, w tym techniką drukarską, techniką reprograficzną, techniką cyfrową lub poprzez wprowadzanie do pamięci komputera,
  - c. publiczne rozpowszechnianie, w tym: wyświetlanie, odtwarzanie w dowolnym systemie lub standardzie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym,
  - d. wprowadzanie do sieci multimedialnych oraz Internetu,
  - e. umieszczanie w publikacjach drukowanych (w tym m.in. ulotki, foldery, plakaty),
  - f. umieszczanie w publikacjach elektronicznych oraz aplikacjach elektronicznych,
  - g. umieszczanie w prezentacjach i materiałach prasowych,
  - h. umieszczanie w spotach i filmach reklamowych.
3. Licencja, o której mowa w ust. 1 i 2 uprawnia Zamawiającego do korzystania z rozwiązania na terytorium Rzeczypospolitej Polskiej.
4. Zamawiający może wykonywać wszelkie prawa przyznane w ramach licencji również przy udziale, za pośrednictwem lub przy pomocy osób trzecich świadczących usługi na rzecz Zamawiającego, w tym w szczególności profesjonalnych doradców, konsultantów, zleceńbiorców oraz innych osób współpracujących z Zamawiającym.
5. Zamawiający nie będzie mieć prawa przenosić licencji na inne osoby, przy czym wyjątkiem jest zmiana formy prawnej lub zmiany struktury właścicielskiej Zamawiającego, która wyłączona jest spod zapisów tego ustępu.
6. Wykonawcy składając ofertę oświadcza, iż:
  - 1) przysługują mu wszelkie prawa do przedmiotów własności intelektualnej oferowanych w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; lub
  - 2) przysługują mu prawa do sprzedaży sublicencji na przedmiot własności intelektualnej oferowanej w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; oraz
  - 3) udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowiło naruszenia praw osób trzecich.
7. Zamawiający gwarantuje parametry ujęte w postępowaniu, a Wykonawca zobowiązany jest do dostarczenia pozostałych elementów niezbędnych do poprawnego wdrożenia rozwiązania.
  1. W ramach realizacji przedmiotu zamówienie Wykonawca zobowiązany jest do przeprowadzenia wdrożenia systemu w następującym zakresie:
    - a) instalacja oprogramowania na maszynie wirtualnej w infrastrukturze sieciowej Zamawiającego;
    - b) rozmieszczenie dostarczanych sprzętów na stanowiskach roboczych wskazanych przez Zamawiającego;

- c) instalacja na wskazanych stanowiskach, o których mowa w podpunkcie b, oprogramowania niezbędnego do poprawnej pracy systemu lub dostarczenie zestawu instalatorów wymaganych do przeprowadzenia instalacji domenowej;
  - d) konfiguracja i parametryzacja dostarczonego oprogramowania do współpracy z dostarczonym sprzętem;
  - e) w porozumieniu z dostawcą systemu dziedzinowego HIS uruchomienie integracji między systemem HIS a dostarczonym systemem;
  - f) przekazanie Zamawiającemu zestawu zmiennych i parametrów wymaganych do poprawnego działania integracji między systemem HIS a dostarczonym systemem;
  - g) przeprowadzenie szkoleń z zakresu działania systemu dla użytkowników systemu (personelu medycznego);
  - h) przeprowadzenie szkoleń z zakresu administrowania infrastrukturą i konfiguracją systemu dla administratorów szpitala;
  - i) dostarczenie dokumentacji powdrożeniowej.
2. Zamawiający zastrzega sobie prawo do wskazania Wykonawcy w trakcie trwania wdrożenia mniejszej liczby stanowisk do instalacji i konfiguracji niż liczba dostarczonego przez Wykonawcę sprzętu i przeprowadzenia odbioru końcowego z uwzględnieniem powyższej zmiany. Wykonawca będzie zobowiązany do przeprowadzenia instalacji i konfiguracji pozostałych stanowisk w ramach świadczenia opieki serwisowej. Zamawiający uzgodni z Wykonawcą szczegółowy harmonogram instalacji i konfiguracji poza okresem wdrożenia, przy czym czas wykonania instalacji i konfiguracji nie może być dłuższy niż 20 dni roboczych od przekazania Wykonawcy informacji o zleceniu realizacji zadania.
3. Szkolenia dla użytkowników systemu zostaną przeprowadzone w trybie:
- 1) szkoleń audytoryjnych przeprowadzonych w grupach; i/lub
  - 2) szkoleń stanowiskowych - na każdym z zainstalowanych i skonfigurowanych stanowisk Wykonawca przeprowadzi szkolenie dla personelu szpitala obsługującego dane stanowisko w dwóch różnych terminach;
  - 3) szkoleń dla administratorów szpitala z zakresu administrowania infrastrukturą i konfiguracją;
  - 4) zamawiający przewiduje konieczność przeszkolenia około 60 osób; dokładna liczba osób do przeszkolenia zostanie przekazana Wykonawcy w terminie do 10 dni od zawarcia umowy.
- a) Wykonawca jest zobowiązany do umożliwienia każdemu uczestnikowi szkolenia aktywnego uczestnictwa w szkoleniu polegającego na indywidualnym przejściu całego procesu związanego z wygenerowaniem dokumentu z systemu, podpisaniem dokumentu i zapisaniem dokumentu w systemie.
  - b) Wykonawca jest zobowiązany do uzyskania i udostępnienia Zamawiającemu potwierdzenia uczestnictwa od każdego z uczestników szkoleń.
  - c) Szkolenia mają być przeprowadzone w placówce Zamawiającego w dni robocze w godzinach od 8:00 do 15:00. Zamawiający zastrzega sobie prawo do zmiany trybu przeprowadzania szkoleń na formę zdalną za pośrednictwem telekonferencji w przypadku występowania w placówce sytuacji epidemiologicznej uniemożliwiającej przeprowadzenie szkoleń stacjonarnych.
  - d) Wykonawca przekaze Zamawiającemu materiały instruktażowe w postaci filmów instruktażowych lub instrukcji stanowiskowych, umożliwiających wykonanie samodzielnego szkolenia dla personelu szpitala.
  - e) Zamawiający zastrzega sobie prawo do zorganizowania szkoleń dla części personelu szpitala w terminie wykraczającym poza okres trwania prac wdrożeniowych i przeprowadzenia odbioru końcowego z uwzględnieniem powyższej zmiany. Wykonawca będzie zobowiązany do przeprowadzenia pozostałych szkoleń w ramach świadczenia opieki serwisowej. Zamawiający uzgodni z Wykonawcą szczegółowy harmonogram szkoleń poza okresem wdrożenia, przy czym czas przeprowadzenia szkoleń nie może być dłuższy niż 30 dni roboczych od przekazania Wykonawcy informacji o zleceniu realizacji zadania.
  - f) Wykonawca jest zobowiązany przedstawić Zamawiającemu propozycję szczegółowego harmonogramu szkoleń nie później niż na 3 dni robocze przed planowanym rozpoczęciem szkoleń.
  - g) Wykonawca jest zobowiązany do uwzględnienia uwag przekazanych przez Zamawiającego, a w przypadku braku takiej możliwości, do przedstawienia nowej propozycji harmonogramu szkoleń w terminie maksymalnie 2 dni roboczych od przekazania uwag.
4. Wykonawca przekaze Zamawiającemu Dokumentację powdrożeniową po zakończeniu wszystkich prac wdrożeniowych aktualną na dzień odbioru końcowego. Dokumentacja powdrożeniowa ma obejmować:
- 1) raport z wykonanych prac wdrożeniowych

- 2) zestawienie personelu uczestniczącego w szkoleniach
- 3) instrukcję obsługi systemu
- 4) wykaz zmiennych i parametrów ustawionych dla systemu
- 5) informacje na temat dostępnego sposobu zgłaszania awarii i usterek w działaniu systemu
- 6) wykaz procedur wymaganych dla poprawnego działania systemu, które administrator systemu szpitalnego ma przeprowadzać na serwerze i dostarczonym systemie

#### *1.10.4 Integracja systemu z działającym w placówce systemem HIS AMMS*

1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest w porozumieniu z dostawcą systemu HIS AMMS do przeprowadzenia modyfikacji systemu w szczególności polegających na:
  - a) umożliwieniu dodawania szablonów dokumentów mających podlegać integracji za pomocą edytora będącego częścią dostarczanego systemu
  - b) umożliwieniu umieszczania w polach aktywnych dokumentu powstałego z szablonu opisanego w pkt. a) treści związanych z danymi pacjenta oraz danymi jednostki organizacyjnej szpitala pobieranych z systemu AMMS
  - c) umożliwieniu powiązania dowolnej klasy dokumentacji z systemem AMMS z szablonem opisanym w pkt. a)
  - d) umożliwieniu dostosowania istniejących szablonów pism w systemie AMMS do obsługi w systemie digitalizacji poprzez:
    - umieszczenie w pliku szablonu pisma znaczników pól aktywnych takich jak pola podpisu, pola tekstowe, pola wyboru
    - dodanie możliwości przekazania dokumentu generowanego z szablonu pisma do obsługi w systemie digitalizacji
  - e) w przypadku dokumentów opisanych w punkcie d) umożliwieniu uzupełnienia dokumentu o dodatkowe dane wpisywane w formularzu systemu AMMS podczas generowania dokumentu
  - f) umożliwieniu wygenerowania dokumentu z widoku Dokumentacji Medycznej w systemie HIS AMMS dla konkretnego pacjenta
  - g) wygenerowany dokument ma być jednoznacznie powiązany z pacjentem i kontekstem, w którym został utworzony
  - h) umożliwieniu wskazania (rodzaju) urządzenia, na które dokument ma zostać przesłany celem podpisania przez pacjenta:
    - na stacji roboczej, z której generowany jest dokument w HIS AMMS dla długopisów cyfrowych lub ekranów do podpisu,
    - na podstawie ręcznego wyboru urządzenia przez użytkownika z listy dla tabletów mobilnych. W tym celu System musi udostępnić HIS AMMS interfejs sieciowy umożliwiający pobranie listy dostępnych w systemie urządzeń.
  - i) Wskazanie urządzenia docelowego ma się odbywać za pośrednictwem słownika systemu AMMS
  - j) wypełniony w systemie digitalizacji dokument ma zostać automatycznie udostępniony w widoku Dokumentacji Medycznej i powiązany z klasą dokumentu i szablonem pisma, z którego został wygenerowany
  - k) umożliwieniu wskazania za pośrednictwem parametrów systemu AMMS, czy dokumenty tego samego typu generowane dla tego samego pacjenta mają być zapisywane jako nowy dokument czy kolejna wersja wcześniejszego dokumentu
  - l) umożliwieniu uwierzytelnienia się w Systemie za pośrednictwem danych autoryzacyjnych użytkownika systemu HIS – AMMS, a w przypadku uruchomienia w jednostce Zamawiającego logowania domenowego, umożliwieniu uwierzytelnienia za pomocą danych autoryzacyjnych użytkownika domenowego

#### *1.10.5 Wymagania w zakresie przygotowania dokumentacji formularzowej podpisywanej odręcznie przez pacjenta*

W celu realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia analizy i przygotowania dokumentacji formularzowej podpisywanej odręcznie przez pacjenta, wykorzystywanej obecnie przez Zamawiającego, w celu wprowadzenia jej do systemu digitalizacji, w pakiecie zawierającym maksymalnie 20 sztuk.

Po przekazaniu przez Zamawiającego dokumentacji formularzowej, Wykonawca ma obowiązek podjąć się jej analizy i przygotowania. W przypadku napotkania problemów z prawidłowym wprowadzeniem dokumentacji formularzowej do systemu wynikającej z typów dokumentów dostarczonych przez Zamawiającego, Wykonawca zobowiązany jest do zgłoszenia uwag w tym zakresie do Zamawiającego. W przypadku dokumentów

niemożliwych do przerobienia wg uwag Wykonawcy, Zamawiający przewiduje możliwość wymiany dostarczonego formularza na inny lub akceptację wykonania przez Wykonawcę mniejszej liczby sztuk dokumentacji formularzowej.

W przypadku wymiany dokumentu niemożliwego do wprowadzenia do systemu na inny, po dostarczeniu nowego typu formularza przez Zamawiającego, Wykonawca ma 5 dni roboczych na podjęcie się analizy nowego formularza.

W przypadku braku zgłoszenia uwag przez Wykonawcę do dokumentacji formularzowej dostarczonej przez Zamawiającego w ciągu 10 dni roboczych od ich dostarczenia Zamawiający przyjmuje, iż dostarczone formularze możliwe są do wprowadzenia do systemu.

Zamawiający zastrzega sobie prawo do dostarczenia w trakcie trwania wdrożenia mniejszej liczby formularzy niż wskazana w niniejszym opisie, w takiej sytuacji Wykonawca zobowiązany będzie do prawidłowego wprowadzenia dokumentacji formularzowej do systemu w trakcie trwania opieki serwisowej.

#### 1.10.6 Opieka na systemem

W ramach opieki serwisowej nad Systemem Wykonawca w okresie 36 miesięcy świadczyć będzie następujące usługi/ wykonywać będzie następujące prace:

- 1) udostępnianie nowych wersji oprogramowania ,
- 2) udostępnianie łatek i hotfixów zapewniających bezpieczeństwo działania Systemu,
- 3) wykonywanie wymaganych prac programistycznych oraz konfiguracyjnych w przypadku awarii lub nieprawidłowego działania Systemu,
- 4) świadczenie wsparcia technicznego w godzinach pracy serwisu,
- 5) naprawa awarii, wad i usterek oprogramowania opisanych w tabeli Warunki brzegowe realizacji usług serwisowych,
- 6) obsługa konsultacji opisanych w tabeli Warunki brzegowe realizacji usług serwisowych.

#### Warunki brzegowe realizacji usług serwisowych

Godziny Pracy Serwisu 8 <sup>00</sup> -16 <sup>00</sup>		Okres godzin w ciągu dnia roboczego od poniedziałku do piątku.
Minimalne warunki serwisu		Uwagi
Reakcja serwisu	do 2h roboczych	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.
Usunięcie Awarii (błąd krytycznego)*	do 8h	Czas liczony w godzinach roboczych od upływu czasu reakcji. Możliwe jest zaproponowanie tymczasowego obejścia błędu w wymaganym czasie 8h, pod warunkiem kontynuowania prac nad usunięciem awarii.
Usunięcie Wady Aplikacji **	5 dni	Czas liczony w dniach roboczych od upływu czasu reakcji
Usunięcie wady Programistycznej ***	10 dni	Czas liczony w dniach roboczych od upływu czasu reakcji
Obsługi Konsultacji ****	10 dni	Czas liczony w dniach roboczych od upływu czasu reakcji.

- \* - przez awarię (błąd krytyczny) rozumiany jest błąd natury technicznej uniemożliwiający korzystanie z aplikacji i realizację procesu dla niej przewidzianego w pierwotnych założeniach aplikacji, wynikający z nieprawidłowego działania Wykonawcy w zakresie tworzenia lub konfiguracji i występujący w odosobnieniu od okoliczności, na które Wykonawca nie ma wpływu.
- \*\* - przez wadę rozumiana jest niezgodność z pierwotnymi założeniami aplikacji, która nie mogła zostać wykryta w trakcie testów akceptacyjnych.



- \*\*\* - przez usterkę rozumiany jest błąd w aplikacji wynikający z nieprawidłowego stworzenia kodu programistycznego w odniesieniu do pierwotnych założeń aplikacji, ale nie powodujący przerwania pracy, a stanowiący utrudnienie korzystania z aplikacji.
- \*\*\*\* - dotyczy zgłoszeń i zapytań nie związanych z wystąpieniem błędu, a dotyczących zastosowania dodatkowych lub alternatywnych możliwości wykorzystania istniejących funkcji.

### 1.10.7 Wymagania dla oprogramowania

#### 1. Ogólne – System do digitalizacji (dalej: System)

- System musi umożliwiać pracę w odizolowanym środowisku na infrastrukturze Zamawiającego, bez dostępu do Internetu lub jakichkolwiek połączeń sieciowych poza infrastrukturę teleinformatyczną Zamawiającego
- System musi umożliwiać współpracę z różnymi urządzeniami do digitalizacji dokumentów dostępnymi na rynku – ekranami piórkowymi dedykowanymi do składania podpisów kontekstowych, tabletami mobilnymi, długopisami cyfrowymi, skanerami dokumentacji. W ramach Systemu, Zamawiający ma mieć możliwość doboru kompatybilnych urządzeń dobranych do aktualnych potrzeb, bez wprowadzania przez Wykonawcę zmian w oprogramowaniu (z wyłączeniem niezbędnych aktualizacji).
- System musi posiadać Aplikację Centralną, dostępną z poziomu przeglądarki Internetowej, wymagającą logowania na konto użytkownika.
- System ma umożliwiać implementację nowych formularzy do Systemu poprzez import do aplikacji edytora (będącej elementem Systemu) tła dokumentu w postaci PDF (tzn. obrazu niezmiennych części dokumentu), a następnie naniesienie na tło regionów aktywnych, które mogą być edytowalne w celu personalizacji powstających dokumentów. Utworzone w ten sposób regiony powinny znaleźć się w wynikowym pliku PDF i być zgodne ze specyfikacją formatu PDF (w szczególności umożliwiać kompatybilność z popularnymi przeglądarkami plików PDF, np. Adobe Reader).
- System musi umożliwiać obsługę innych plików PDF niezdefiniowanych wcześniej w Systemie.
- System musi umożliwiać zarządzanie wersjami formularzy w celu umożliwienia modyfikacji szablonu bez zmian konfiguracji powiązanych systemów lub narzędzi. System musi umożliwiać tworzenie dowolnej liczby wersji danego formularza z oznaczeniem aktualnie obowiązującej wersji.
- Repozytorium dokumentów:
  - System musi posiadać wbudowane mechanizmy zapisywania, przechowywania i katalogowania dokumentów w ramach Systemu,
  - System musi umożliwiać samodzielne tworzenie, usuwanie i zmianę nazwy katalogów i podkatalogów możliwych do przeglądania z poziomu Aplikacji Centralnej.
  - System musi umożliwiać przenoszenie dokumentów pomiędzy katalogami oraz definiowanie domyślnych katalogów zapisu dokumentów.
  - System musi umożliwiać samodzielną konfigurację struktury danych, która prezentuje dokumenty w postaci rekordów zbudowanych na podstawie danych zawartych w dokumentach. To znaczy, że jeżeli w określonych polach dokumentów znajdują się określone wartości, to System automatycznie utworzy nowy rekord i zapisze w nim dokumenty lub przypisze dokumenty do istniejącego rekordu zawierającego te dane.
- System musi umożliwiać zarządzanie podłączonymi do Systemu stanowiskami, w podziale na typ urządzenia, aktualny status komunikacji. Aplikacja Centralna musi ponadto umożliwiać przegląd ostatnich zdarzeń na stanowisku oraz możliwość zdalnej zmiany konfiguracji w celu zarządzania stanowiskami.
- System musi umożliwiać śledzenie statusu podpisywania poszczególnych dokumentów.
- System musi umożliwiać nakładanie w polach podpisu pieczętek konfigurowalnych w Systemie.
- System musi udostępniać panel administracyjny dostępny z poziomu Aplikacji Centralnej.
- System musi umożliwiać tworzenie kont użytkowników i zarządzanie nimi z poziomu panelu administracyjnego.
- Integracje
  - System musi umożliwiać otwartą integrację z systemami zewnętrznymi za pomocą API w technologii REST.
  - System umożliwia wysłanie do podpisu dokumentu za pośrednictwem funkcjonalności wirtualnej drukarki. W przypadku braku dostosowania dokumentów do pracy z systemem, aplikacja obsługująca wirtualną drukarkę powinna umożliwiać ręczne wskazanie lokalizacji pól podpisu.
  - System musi pozwalać na przesłanie do podpisu dowolnego dokumentu w formacie PDF oraz ukrycie niezbędnych informacji o dokumencie, w szczególności o polach podpisu, w samej treści dokumentu – bez konieczności obsługi tych informacji w zapytaniu integracyjnym.

- System musi umożliwiać cofnięcie autoryzacji dla danej integracji w celu zabezpieczenia przed wyciekiem.
- System musi posiadać funkcjonalność ustawiania automatycznych powiadomień o podpisaniu dokumentu na wskazany webservice w celu umożliwienia integracji bez konieczności wykonania prac po stronie Wykonawcy.

n. Podpisy:

- System zapewnia użytkownikowi zrozumiały proces składania podpisu odręcznego, tzn. podpis składany jest zawsze w kontekście dokumentu „tak jak na papierze”. Podpis odręczny nie może być składany na odrębnym urządzeniu, które nie wyświetla jednocześnie dokumentu, ani w odrębnym wyskakującym oknie aplikacji.
- System umożliwia składanie pisma odręcznego na dokumentach również poza polami podpisu, w celu umożliwienia digitalizacji dowolnej treści, również takiej, która nie została wcześniej zdefiniowana na poziomie wzoru formularza.
- System powinien umożliwiać opatrzenie dokumentów elektronicznym podpisem odręcznym (biometrycznym). System powinien gromadzić informacje takie jak siła nacisku czy znaczniki czasowe umożliwiające weryfikację autentyczności podpisu.
- System niezależnie powinien umożliwiać opatrzenie dokumentów podpisem osobistym z e-Dowodu.

## 2. Wymagania związane z urządzeniami

### A. Ekran do podpisu

- Możliwość uruchomienia aplikacji Systemu na dowolnym komputerze z systemem operacyjnym Windows 10/11, wersja 64-bitowa
- Dedykowany ekran powinien być na stałe połączony z komputerem, aby umożliwiać digitalizację dokumentu w czasie rzeczywistym.
- System umożliwia prezentację na ekranie treści multimedialnych, gdy ten nie jest wykorzystywany do wyświetlania i podpisywania dokumentu. Konfiguracja wyświetlanych treści powinna odbywać się z poziomu panelu administracyjnego w Aplikacji Centralnej.
- System umożliwia uzupełnianie, zaznaczanie, wypełnianie i edycję pól aktywnych (tekstowych, zaznaczalnych, wyboru) w trakcie podpisywania dokumentu.
- System umożliwia utrzymywanie aktywnego połączenia aplikacji obsługującej ekran z serwerem, tak aby wywołanie dokumentu do podpisu nie wymagało aktywności użytkownika w aplikacji.
- System powinien mieć funkcję powiększania, zmniejszania i przesuwania wyświetlanego formularza, gdyby ten był nieczytelny.
- System powinien zapewniać operatorowi Systemu możliwość podglądu i kontroli przebiegu podpisywania na własnym monitorze (synchronizacja widoków).
- System musi umożliwiać zalogowanie wielu użytkowników do jednej aplikacji z możliwością przełączania się pomiędzy ich kontami.

### B. Tablet mobilny

- System powinien umożliwiać uruchomienie aplikacji na urządzeniu z systemem operacyjnym Android.
- System powinien mieć funkcję powiększania, zmniejszania i przesuwania wyświetlanego formularza, gdyby ten był nieczytelny.
- System umożliwia uzupełnianie, zaznaczanie, wypełnianie i edycję pól aktywnych (tekstowych, zaznaczalnych, wyboru) w trakcie podpisywania dokumentu.
- System musi posiadać możliwość podpisywania dokumentów bez stałego dostępu sieciowego do serwera poprzez zapisanie dokumentu w pamięci.
- System musi umożliwiać zalogowanie wielu użytkowników do jednej aplikacji z możliwością przełączania się pomiędzy ich kontami.

### C. Długopis cyfrowy

- System powinien umożliwiać uruchomienie aplikacji do obsługi długopisu cyfrowego na dowolnym komputerze z systemem operacyjnym Windows 10/11, wersja 64-bitowa

- System powinien umożliwiać odwzorowanie formularza papierowego w wersji elektronicznej w wersji 1:1.
- System powinien umożliwiać wygenerowanie formularza w taki sposób, aby każdy wydrukowany formularz był unikatowy. Oznacza to, że wypełnienie papierowego formularza długopisem cyfrowym, tworzy wzajemnie jednoznacznie przyporządkowaną do niego wersję elektroniczną dokumentu.
- System powinien umożliwiać podgląd danych pochodzących bezpośrednio z urządzeń przez wysłaniem dokumentu do repozytorium.
- System powinien umożliwiać automatyczny wydruk dokumentów przeznaczonych do obsługi długopisem cyfrowym, bez konieczności ingerencji ze strony użytkownika Systemu.
- System powinien umożliwiać zbieranie danych na formularzach papierowych niezależnie od infrastruktury informatycznej (zbieranie danych off-line)
- System nie może pozwalać na odtworzenie danych z długopisu cyfrowego bez zgrania danych i załadowania się do systemu.
- Odręczny podpis wykonany długopisem cyfrowym powinien być przechowywany w Systemie jako grafika oraz informacje zawierające cechy biometryczne.
- Wydruk formularza dopasowanego do długopisu cyfrowego musi umożliwiać standardowa drukarka laserowa o parametrach minimalnych:
  - Minimalna rozdzielczość wydruku: 600 x 600 DPI

## **VI. Część nr 4**

### **2.1 Zakup oprogramowania do integracji urządzeń z system AMMS w zakresie skanowanej dokumentacji papierowej w tym kart informacyjnych**

Wykonanie integracji na bazie standardowej dokumentacji integracyjnej HIS. dotyczącej integracji z urządzeniami do skanowania dokumentacji

**System HIS udostępnia dane:**

- Pobytu pacjenta ; numer pobytu pod który ma być podłączony skanowany dokument.
- Dane personelu wykorzystywane do identyfikacji osoby skanującej i autoryzującej kopię elektroniczną.
- Dane pacjenta (PESEL, identyfikator w systemie medycznym, imię, nazwisko).

**System skanowania przekazuje:**

- zeskanowany dokument do systemu HIS przypisaniem go do wybranego typu dokumentu oraz pacjenta i jego wizyty/pobytu.

W ramach prac produkcyjnych zaplanowana jest rozbudowa obsługi powiązania dokumentu z pobytem przekazywanego z systemu zewnętrznego, tj. systemu skanowania. W sytuacji, gdy system zewnętrzny, w przekazanych danych indeksowych dokumentu, posłuży się identyfikatorami pobytów zgodnymi z systemem HIS, system HIS wyświetli taki dokument we właściwym kontekście.

#### **Scenariusz integracji**

Po zalogowaniu się na maszynie skanującej do systemu, osoba chcąc wprowadzić dokumenty papierowe pacjenta wyszukuje i wybiera kartotekę pacjenta, korzystając z danych takich jak nazwisko bądź numer PESEL. Możliwe jest wyszukiwanie po fragmencie nazwiska bądź numeru PESEL. W dalszej części operator pracuje już na wybranym pacjencie, wybierając na panelu kategorię główną dokumentów. W kategorii głównej dostępne są kolejne podkategorie dokumentów, zgodnie z odwzorowaniem struktury dokumentów w bazie HIS. W momencie wyboru na panelu urządzenia rodzaju dokumentu, jaki ma być wprowadzony do bazy, użytkownik umieszcza papierowy dokument (lub dokumenty) na podajniku. Użytkownik ma możliwość wypełnienia dodatkowych informacji dotyczących wprowadzanego dokumentu, zgodnie z wymogami bazy HIS. System winien umożliwiać również zmianę domyślnych ustawień skanowania w przypadku niestandardowych oryginałów. Zmiana parametrów skanowania powinna być dostępna pod przyciskiem „Ustawienia”. Po wprowadzeniu danych dotyczących skanowanego oryginału użytkownik naciska przycisk SKANUJ w celu uruchomienia procesu pobierania obrazów z oryginałów umieszczonych na podajniku urządzenia. Po zeskanowaniu wszystkich oryginałów umieszczonych w podajniku, jakie mają być wprowadzone do bazy AMMS, należy nacisnąć przycisk ZAPISZ, aby obrazy dokumentów zostały wprowadzone do bazy HIS. Ostatecznie dokument jest dostępny w systemie HIS, podpięty do odpowiedniego pacjenta oraz pod wybrany typ dokumentacji. Dodatkowo, na dokumencie powinna być dodana stopka z informacjami na temat tego, kto skanował dokument, w jakim dniu i o jakiej godzinie, oraz jakiego pacjenta on dotyczy.

### ***2.2 Zakup oprogramowania do zarządzania medyczną dokumentacją elektroniczną wraz z kosztami nadzorów przez okres 3 letni***

**Wymagania funkcjonalne**

Opis wszystkich funkcjonalności oraz zależności w ramach modułu, w podziale:

#### **2.1 Wymagania funkcjonalne**

1. System umożliwia rejestrację indywidualnej dokumentacji medycznej, zbiorczej dokumentacji medycznej oraz dokumentacji niemedycznej.
2. System umożliwia podział dokumentacji niemedycznej według rodzajów oraz jednostek organizacyjnych z wykorzystaniem słownika konfigurowanego przez dedykowanego użytkownika.

3. System umożliwia zdefiniowanie słownika typów dokumentów dla dokumentacji niemedycznej. Słownik powinien uwzględniać podział typów dokumentów według rodzaju: przychodzące, wewnętrzne, wychodzące.
4. System umożliwia automatyczne zakładanie teczek pacjentów w module Archiwum na podstawie pobytów pacjentów zarejestrowanych w HIS Ruch Chorych/Przychodnia wraz z wykazem dokumentów (metryczka dokumentu).
5. Parametryzacja systemu umożliwia organizację dokumentacji medycznej dla automatycznie założonych teczek pacjentów dla poszczególnych jednostek organizacyjnych szpitala wg rodzajów:
  - 1) teczki zawierające dokumentację medyczną w zakresie jednej hospitalizacji,
  - 2) teczki zawierające dokumentację medyczną z wielu hospitalizacji,
  - 3) teczki zawierające dokumentację medyczną dla każdego pobytu na oddziale szpitalnym,
  - 4) teczki zawierające dokumentację medyczną wielu pacjentów,
  - 5) teczki zawierające dokumentację medyczną w zakresie gabinetów, pracowni,
  - 6) teczki zawierające dokumentację medyczną w zakresie gabinetów pogrupowane wg jednostki nadrzędnej.
6. System umożliwia organizację rejestrowanej dokumentacji w postaci teczek oraz spraw w teczce.
7. System umożliwia grupowanie teczek w zbiory (segregatory), w ramach wybranych jednostek organizacyjnych szpitala, w celu połączenia w jeden zestaw grupy teczek dowolnego pacjenta lub wielu wybranych pacjentów.
8. System umożliwia automatyczne wyszukiwanie teczek pacjentów z poradni do przekazania do Archiwum.
9. System umożliwia automatyczne blokowanie edycji teczek pacjentów przyjętych do zasobów archiwalnych.
10. System umożliwia „śledzenie” teczek w zakresie aktualnego miejsca ich przechowywania
  - 1) System automatycznie aktualizuje miejsce przechowywania teczki pacjenta na podstawie danych z HIS w zakresie ruchu międzyoddziałowego,
  - 2) Miejsce przechowywania teczek jest aktualizowane na podstawie danych wynikających z obiegu dokumentacji papierowej.
11. System umożliwia potwierdzenie przyjęcia dokumentacji pacjenta przez JOS na podstawie obiegu dokumentacji w formie papierowej.
12. Potwierdzenie odbioru dokumentacji przyjęcia dokumentacji pacjenta przez JOS dostępne jest z modułu Archiwum oraz w modułach HIS tj. Izba przyjęć, Oddział, Gabinet, Pracownia.
13. System umożliwia przekazanie dokumentacji medycznej pacjenta do wybranego JOS na podstawie obiegu papierowego dokumentacji.
14. System umożliwia przypisanie zarchiwizowanych teczek pacjenta do wybranego magazynu, pomieszczenia, regału, półki.
15. System umożliwia grupowe przenoszenie teczek pomiędzy magazynami, pomieszczeniami, regałami, półkami.
16. System umożliwia zdefiniowanie wielu archiwów oraz magazynów w ramach archiwum.
17. Opis teczki musi obejmować przynajmniej:
  - 1) numer teczki nadany wg zdefiniowanego szablonu,
  - 2) symbol klasyfikacyjny wraz z tytułem oraz kategorię archiwalną,
  - 3) miejsce utworzenia,
  - 4) miejsce przechowywania.
18. Opis sprawy w przypadku indywidualnej dokumentacji medycznej musi obejmować przynajmniej:
  - 1) dane pacjenta,
  - 2) dane zdarzenia medycznego (hospitalizacja/pobyt/kartoteka w poradni).
19. System umożliwia rejestrowanie metadanych archiwizowanych dokumentów. W szczególności informację o formie dokumentu (papierowy/elektroniczny) oraz miejscu jego przechowywania.
20. System umożliwia wyświetlanie oraz pobieranie treści elektronicznej dokumentacji medycznej oraz dokumentacji medycznej zmaterializowanej.
21. System umożliwia zarejestrowanie kopii dokumentu.
22. System umożliwia stworzenie systemu klasyfikacyjnego przechowywanej w teczce dokumentacji. System klasyfikacyjny musi umożliwiać rozróżnienie dokumentacji medycznej od dokumentacji niemedycznej.
23. System umożliwia zdefiniowanie Jednolitego Rzeczowego Wykazu Akt wraz z kategorią archiwalną.
24. System umożliwia automatyczne przypisanie oraz wyszukiwanie teczek pacjentów na podstawie pozycji zdefiniowanych w JRWA (Jednolitym Rzeczowym Wykazie Akt) co najmniej dla:
  - 1) historii chorób pacjentów wypisanych,
  - 2) historii chorób pacjentów zmarłych,

- 3) historii chorób pacjentów zmarłych na skutek uszkodzenia ciała lub zatrucia,
  - 4) historii chorób osób leczonych krwią i preparatami krwiopochodnymi,
  - 5) historii chorób dzieci do 2 roku życia,
  - 6) historia leczenia ambulatoryjnego.
25. System umożliwia zdefiniowanie (workflow) procesu archiwizacji dokumentacji medycznej i niemedyceynej w podziale na podprocesy z możliwością włączania i wyłączania podprocesu. Wykaz zdefiniowanych podprocesów:
    - 1) akceptacja przełożonego/Brak akceptacji,
    - 2) przyjęcie do weryfikacji przez jednostkę weryfikującą,
    - 3) akceptacja w jednostce weryfikującej/Brak akceptacji,
    - 4) przyjęcie do weryfikacji przez jednostkę archiwizującą,
    - 5) akceptacja w jednostce archiwizującej/Brak akceptacji,
  26. System umożliwia wycofanie wykonanego podprocesu tj. wycofanie akceptacji przełożonego, wycofanie akceptacji jednostki weryfikującej, wycofanie akceptacji w jednostce archiwizującej.
  27. W przypadku protokołu przeniesienia/spisu zdawczo-odbiorczego system umożliwia wykonywanie poszczególnych funkcji (przełącz, przyjmij do weryfikacji, zaakceptuj w statystyce, odrzuć) zarówno na całym protokole/spisie (wszystkich teczkach) jak i na wybranych pozycjach (wskazanych teczkach).
  28. System umożliwia wydruk etykiet teczek, spraw oraz dokumentów wg zdefiniowanych szablonów. Etykieta może zawierać kod kreskowy identyfikujący teczkę, sprawę lub dokument.
  29. System umożliwia utworzenie i wydruk protokołów przeniesienia dokumentacji.
  30. System umożliwia utworzenie i wydruk spisów zdawczo-odbiorczych.
  31. System umożliwia utworzenie i wydruk protokołu zniszczenia/zagubienia dokumentacji.
  32. System umożliwia utworzenie i wydruk protokołu odnalezienia dokumentacji.
  33. System umożliwia wydruk wykazu dokumentów znajdujących się w teczce pacjenta.
  34. System umożliwia zmianę miejsca przechowywania dokumentacji oraz wygenerowanie i wydruk protokołu zdawczo-odbiorczego.
  35. System umożliwia utworzenie i wydruk wykazów teczek przekazanych i nieprzekazanych do Jednostki Organizacyjnej Szpitala.
  36. System umożliwia wyszukanie teczek wg zadanych kryteriów:
    - 1) klasa dokumentacji,
    - 2) numerteczki lub sprawy,
    - 3) Jednolitego Rzeczowego Wykazu Akt,
    - 4) status dokumentacji: wypożyczona/przekroczony termin zwrotu/zniszczona/zagubiona,
    - 5) jednostka organizacyjna w której dokumentacja została utworzona,
    - 6) zakres dat w których dokumentacja została utworzona,
    - 7) dane pacjenta oraz zdarzenia, którego dokumentacja dotyczy,
    - 8) historia choroby: daty przyjęcia, wypisu, miejsca pobytu, tryb wypisu z oddziału,
    - 9) rozpoznanie według rodzaju (końcowe, ze skierowania, wstępne, po wypisowe) i pozycja w wykazie klasyfikacji chorób według ICD10,
    - 10) klasyfikacjateczki określona wg kategorii archiwalnej nadanej automatycznie dlateczki oraz poprzez wskazanie parametrów opisujących teczkę, dane historii choroby lub wizyty oraz datę utworzenia (od-do),
    - 11) przekroczony termin zwrotu,
    - 12) zwrot potwierdzony,
    - 13) odbiór potwierdzony,
    - 14) lekarz prowadzący/wypisujący,
    - 15) dokumentacja niemedyceynej,
  37. System umożliwia podgląd danychteczki, spraw oraz dokumentów.
  38. System umożliwia podgląd historiiteczki oraz sprawy, zawierającej:
    - 1) informację o modyfikacji danychteczki oraz spraw i dokumentów w teczce,
    - 2) informację o wypożyczeniach/zwrotach dokumentacji medycznej,
    - 3) informację o zagubieniu/zniszczeniu/planowym zniszczeniu dokumentacji.
  39. System umożliwia obsługę kodów kreskowych utworzonych w HIS Ruch Chorych i nadrukowywanych na historiach chorób pacjentów oraz obsługę kodów wygenerowanych w systemie Archiwum.
  40. System umożliwia dowolną konfigurację numeratora dla teczek, protokołów przeniesienia, spisów zdawczo-odbiorczych.
  41. System umożliwia wykonanie zestawienia zdawalności teczek pacjentów z oddziałów do Statystyki medycznej lub Archiwum.
  42. System umożliwia utworzenie i wydruk Księgi Archiwum w formie analitycznej i syntetycznej. Raport może być generowany dla wskazanych jednostek odbierających i przekazujących poradni, oddziałów



- oraz dla określonych zakresów dat leczenia pacjenta i przekazania do archiwum. System umożliwia wydrukowanie raportu w formacie dokumentu pdf oraz arkusza xls.
43. System umożliwia utworzenie i wydruk Listy dokumentacji przechowywanej w określonej jednostce w formie analitycznej i syntetycznej. Raport może być generowany dla wskazanych jednostek oraz dla określonego zakresu dat przyjęcia i wypisu pacjenta ze szpitala. System umożliwia wydrukowanie raportu w formacie dokumentu pdf oraz arkusza xls.
  44. System umożliwia obsługę udostępnienia dokumentacji na wewnętrzne potrzeby podmiotu.
  45. System umożliwia obsługę udostępnienia dokumentacji do celów naukowo-badawczych.
  46. System umożliwia obsługę udostępniania dokumentacji medycznej pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta.
  47. System umożliwia obsługę udostępniania dokumentacji organowi upoważnionemu.
  48. System udostępnia dokumentację w postaci teczki lub sprawy.
  49. Udostępnienie dokumentacji odbywa się na podstawie wniosku o udostępnienie, który zawiera przynajmniej:
    - 1) dane wnioskującego,
    - 2) dane jednostki przechowującej dokumentację,
    - 3) listę teczek/spraw lub opis dokumentacji, która ma zostać udostępniona,
    - 4) termin realizacji udostępnienia,
    - 5) podstawę prawną dla udostępnienia dokumentacji organowi upoważnionemu.
  50. System umożliwia wyszukanie wniosków o udostępnienie wg zadanych kryteriów:
    - 1) dane wnioskującego,
    - 2) dane udostępniającego,
    - 3) dane identyfikujące teczkę/sprawę,
    - 4) dane pacjenta w przypadku udostępniania indywidualnej dokumentacji medycznej,
    - 5) termin realizacji,
    - 6) stan realizacji udostępnienia,
    - 7) przekroczony termin zwrotu,
  51. System umożliwia wspomaganie realizacji wniosku o udostępnienie dokumentacji poprzez oznaczenie stanu realizacji zamówienia.
  52. System umożliwia kontrolę liczby udostępnień dokumentacji medycznej pacjentowi lub osobie przez niego upoważnionej, a co za tym idzie wspomaga proces pobierania obowiązkowych opłat dotyczących kolejnych udostępnień dokumentów.
  53. System umożliwia obsługę potwierdzenia przekazania udostępnianej dokumentacji.
  54. System umożliwia obsługę potwierdzenia zwrotu udostępnianej dokumentacji.
  55. System posiada (workflow) procesu udostępniania dokumentacji medycznej. Wykaz podprocesów:
    - 1) akceptacja przełożonego
    - 2) przyjęcie do realizacji przez jednostkę archiwizującą
    - 3) oznaczenie dokumentacja gotowa do odbioru
    - 4) potwierdzenie odbioru dokumentacji
    - 5) zwrot dokumentacji
  56. System umożliwia zaczytanie listy teczek pacjenta z pliku .xls do karty udostępnienia na cele naukowo-badawcze.
  57. System integruje się z portalem pacjenta w zakresie realizacji wniosków o udostępnienie elektronicznej dokumentacji medycznej, wystawianych za pośrednictwem konta użytkownika założonego na portalu. W ramach realizacji wniosku system umożliwia utworzenie paczki zawierającej elektroniczną dokumentację medyczną, określenie wysokości opłaty za udostępnienie dokumentacji oraz automatycznie generuje potwierdzenie odbioru dokumentacji po jej pobraniu przez pacjenta.
  58. System posiada wbudowany słownik instytucji dla modułu. Słownik powinien być zintegrowany ze słownikiem instytucji w systemie HIS, a jednocześnie powinien umożliwiać rejestrowanie nowych instytucji nieewidencjonowanych w słowniku HIS.
  59. System musi umożliwiać utworzenie i wydruk w formacie dokumentu pdf oraz w formacie arkusza xls następujących parametryzowanych raportów:
    - 1) Lista dokumentacji zgubionej.
    - 2) Lista dokumentacji wypożyczonej w określonym czasie do wskazanych innych jednostek organizacyjnych podmiotu lub organów upoważnionych,.
    - 3) Lista dokumentacji medycznej przechowywanej w określonej jednostce organizacyjnej z możliwością wskazania okresu hospitalizacji.
    - 4) Lista dokumentacji wypożyczonej do wskazanych jednostek organizacyjnych podmiotu lub instytucji zewnętrznych oraz organów upoważnionych, dla której czas zwrotu upłynął.

- 5) Lista dokumentacji medycznej pacjenta nieprzekazanej do jednostki archiwizującej podmiotu oraz lista dokumentacji medycznej zwróconej przez jednostkę archiwizującą do jednostek przekazujących podmiotu.
- 6) Lista dokumentacji medycznej przyjętej na stan jednostki archiwizującej podmiotu z jednostek organizacyjnych.
- 7) Lista dokumentacji określonego pacjenta z możliwością wyboru okresu, wskazania hospitalizacji lub wizyty pacjenta oraz określenia zakresu dokumentacji (opieka, pobyt, pacjent).
- 8) Sumaryczne sprawozdanie roczne z działalności jednostki archiwizującej podmiotu.
- 9) Rejestr udostępnień umożliwiający wygenerowanie wydruku dla udostępnień wewnętrznych, udostępnień do celów naukowo-badawczych, udostępnień pacjentowi lub organowi upoważnionemu.
- 10) Lista teczek pacjenta wg jednostki wypisującej. Raport powinien prezentować dane w zakresie hospitalizacji pacjentów. Dane powinny być pogrupowane wg jednostki wypisującej pacjenta. Dodatkowo raport musi zawierać informacje dotyczące lekarza wypisującego, lekarza prowadzącego oraz jednostki przechowującej dokumentację w momencie generowania raportu.
- 11) Zestawienie liczby zwrotów medycznych teczek pacjentów. Zwrot z jednostek odbierających do jednostek przekazujących. Zestawienie powinno prezentować dane w formie analitycznej i sumarycznej.
60. System umożliwia wydruk kodu kreskowego na drukarce typu Zebra bezpośrednio z teczki pacjenta.
61. System umożliwia automatyczną weryfikację kompletności teczek pod kątem dokumentacji medycznej pacjenta.
62. System umożliwia utworzenie elektronicznej paczki (.zip) zawierającej wybraną dokumentację medyczną pacjenta z wielu hospitalizacji / pobytów w celu udostępnienia jej pacjentowi oraz organowi upoważnionemu.
63. System umożliwia pobranie i podpisanie elektronicznej paczki dokumentów (.zip) podpisem Xades w celu udostępnienia jej pacjentowi.
64. System musi umożliwiać trwałe usunięcie elektronicznej dokumentacji, która podlega brakowaniu, przechowywanej w repozytorium EDM.
65. System musi umożliwiać obsługę powiadamiania pacjentów o dokumentacji do odbioru poprzez możliwość wprowadzenia informacji o sposobie, dacie i statusie powiadomienia.
66. System musi dawać możliwość oznaczenia teczek przeznaczonych do brakowania, które zostały odebrane przez pacjentów.
67. System musi dawać możliwość wprowadzenia danych do Protokołu z posiedzenia komisji oraz jego wydruku.
68. System musi umożliwiać wygenerowanie spisu dokumentacji niearchiwalnej podlegającej brakowaniu.
69. System musi umożliwiać wygenerowanie pisma ze zgodą do Archiwum Państwowego na zbrakowanie dokumentacji.

## **2.2 Wewnętrzne integracje:**

1. HIS – co najmniej jeden z wymienionych modułów: Oddział, Pracownia, Poradnia lub Izba Przyjęć,
2. EDM

## **2.3 Zależności między modułami:**

1. HIS (Oddział, Pracownia, Poradnia, Izba Przyjęć) - przynajmniej jeden z wymienionych modułów musi być uruchomiony przed uruchomieniem ZDM.
2. ZDM korzysta ze wspólnej bazy HIS.
3. Aktualizacja HIS wpływa na działanie ZDM i odwrotnie.

## **2.4 Kryteria odbioru produktu**

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru

Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

1. Umożliwia rejestrację indywidualnej i zbiorczej dokumentacji medycznej oraz dokumentacji niemedyceynej.

2. Pozwala na podział dokumentacji niemedycznej według rodzajów oraz jednostek organizacyjnych z wykorzystaniem słownika konfigurowanego przez dedykowanego użytkownika.
3. Umożliwia automatyczne zakładanie teczek pacjentów w module Archiwum na podstawie pobytów pacjentów zarejestrowanych w HIS Ruch Chorych/Przychodnia wraz z wykazem dokumentów.
4. Parametryzacja systemu umożliwia organizację dokumentacji medycznej w ramach automatycznie założonych teczek pacjentów dla poszczególnych jednostek organizacyjnych szpitala wg rodzajów.
5. Automatycznie aktualizuje miejsce przechowywania teczek pacjenta na podstawie danych z HIS w zakresie ruchu międzyoddziałowego.
6. Umożliwia potwierdzenie przyjęcia dokumentacji pacjenta przez JOS na podstawie obiegu dokumentacji w formie papierowej.
7. Wyświetla oraz pobiera treści elektronicznej dokumentacji medycznej oraz dokumentacji medycznej zmaterializowanej.
8. Umożliwia zdefiniowanie Jednolitego Rzeczowego Wykazu Akt wraz z kategorią archiwalną.
9. Umożliwia zdefiniowanie procesu archiwizacji dokumentacji medycznej i niemedycznej w podziale na podprocesy z możliwością włączania i wyłączania podprocesu
10. W ramach obsługi protokołu przeniesienia / spisu zdawczo-odbiorczego pozwala na wykonywanie czynności zarówno w ramach całego protokołu/spisu jak i na wybranych pozycjach.
11. Umożliwia wydruk etykiet teczek, spraw oraz dokumentów wg zdefiniowanych szablonów.
12. Pozwala na utworzenie i wydruk: protokołów przeniesienia dokumentacji, spisów zdawczo-odbiorczych, protokołów zniszczenia/zgubienia/odnalezienia dokumentacji, wykazu dokumentów w teście, protokołów zdawczo-odbiorczych.
13. Umożliwia wyszukiwanie, przeglądanie i modyfikowanie teczek pacjentów.
14. Umożliwia konfigurację numeratorów teczek, protokołów i spisów.
15. Pozwala na obsługę procesu udostępniania dokumentacji.
16. Umożliwia automatyczną weryfikację kompletności teczek pod kątem dokumentacji medycznej pacjenta.
17. Umożliwia utworzenie, pobranie i podpisanie elektronicznej paczki dokumentów. Warunki startowe – HIS
18. Licencja
19. Skonfigurowana komunikacja z HIS.
20. Skonfigurowane systemy zewnętrzne.
21. Wdrożony jeden z modułów HIS.
22. Skonfigurowany ZDM w zakresie: numeratory teczek, rodzaje teczek.

## 2.5 Wymagania do uruchomienia produktu

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

1. Wymagania techniczne: Serwer aplikacyjny:
  - 1) CPU 2x4core
  - 2) RAM 16GB
  - 3) HDD 100GB
  - 4) oprogramowanie Apache Tomcat 8, Java SE RE 1.7.0.U80
2. Serwer bazodanowy:
  - 1) CPU 2x4core
  - 2) RAM 24GB
  - 3) HDD 500GB
  - 4) oprogramowanie Oracle 12g

### Wymagania organizacyjne:

Konfiguracja systemu ZDM zgodnie z analizą przedwdrożeniową przeprowadzoną u klienta

### Opis wdrożenia

1. Analiza przedwdrożeniowa.
2. Instalacja systemu.
3. Konfiguracja ZDM (zgodnie z analizą przedwdrożeniową).
4. Uruchomienie adaptera.
5. Wczytywanie teczek historycznych (zakres zgodny z analizą przedwdrożeniową).

6. Szkolenie użytkowników: pracownicy archiwum, statystyka, sekretarka medyczna / pielęgniarka oddziału, sekretarka medyczna / pielęgniarka pracowni, sekretarka medyczna / pielęgniarka poradni, dział informatyki.
7. Asysta stanowiskowa (ok. pół godziny na stanowisko).

## *2.3 Zakup oprogramowania do integracji z CeZ w zakresie digitalizacji karty leczenia - Ucyfrowienie oraz indeksacja*

### **3.1. Wymagania funkcjonalne**

- 1) Możliwość monitorowania poziomu zaindeksowania dokumentów (karty informacyjne) - z uwzględnieniem kart przekazanych do centralnego repozytorium Centrum e-Zdrowia dla zdigitalizowanej papierowej dokumentacji medycznej z podziałem na jednostki organizacyjne (możliwość monitorowania wskaźnika na poziomie kierowników poszczególnych jednostek org.), z dokładnością do miesiąca.
- 2) Możliwość ponownej wysyłki indeksów do P1 i przeglądu błędów indeksacji z poziomu GUI HIS.
- 3) Funkcjonalność tworzenia dokumentów elektronicznych zgodnych z szablonem PIK HL7 CDA dla dokumentów zdigitalizowanych na bazie zarejestrowanych w systemie dokumentów zeskanowanych.
- 4) Możliwość poświadczenia zgodności dokumentu z oryginałem przez złożenie podpisu elektronicznego.
- 5) Integracja z platformą P1 zgodnie z udostępnioną specyfikacją usług dla dokumentów zdigitalizowanych.

### **3.2. Zewnętrzne integracje:**

- 1) Rozwiązanie obejmuje integrację z systemem P1 w zakresie związanym z obsługą dokumentów zdigitalizowanych.

### **3.3. Zależności między modułami:**

- 1) Funkcjonalność opiera się na systemie HIS zintegrowanym z repozytorium EDM oraz komponentem odpowiedzialnym za komunikację z P1.

## *2.4 Wdrożenie oprogramowania*

### **Wymagania do uruchomienia produktu**

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

Warunki startowe:

- 1) Licencja: Licencja na funkcjonalność.
- 2) Działająca integracja z systemem P1 w zakresie wymiany EDM.

Wymagania techniczne:

- 1) Rozwiązanie opiera się o istniejące komponenty.
- 2) Jako wsparcie/usprawnienie w digitalizacji mogą być wykorzystywane urządzenia skanujące dostawców zewnętrznych
- 3) zapewnienie zasobów zgodnie z ich wymaganiami.

Wymagania organizacyjne:

- 1) Podmiot zintegrowany z platformą P1 (w szczególności aktywne konto podmiotu w P1 i aktualne certyfikaty dostępowe).
- 2) W przypadku wykorzystania systemów zewnętrznych, licencja na integrację.

### **Opis wdrożenia**

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

- 1) Uzupełnienie konfiguracji
- 2) Ewentualna konfiguracja w zakresie integracji z urządzeniami skanującymi.

## Kryteria odbioru produktu

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru:

Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

- 1) Umożliwia monitorowanie poziomu zaindeksowania dokumentów (karty informacyjne) z uwzględnieniem kart przekazanych do centralnego repozytorium Centrum e-Zdrowia dla zdigitalizowanej papierowej dokumentacji medycznej – prezentuje poprawne wartości statystyk zgodnie z liczbą przekazanych dokumentów lub indeksów.
- 2) Umożliwia tworzenie dokumentów elektronicznych zgodnych z szablonem PIK HL7 CDA dla dokumentów zdigitalizowanych i ich utrwalenie w repozytorium EDM.
- 3) Umożliwia przekazanie dokumentów zdigitalizowanych do platformy P1 zgodnie z udostępnioną specyfikacją usług.
- 4) Umożliwia wymuszenie wysyłki indeksu dokumentu EDM do systemu P1 z poziomu GUI.

### 2.5 Zakup urządzeń do skanowania dokumentacji papierowej do postaci cyfrowej Urządzenie umożliwiające integrację z systemem szpitalnym

Skaner typ 1 – 2 szt.

Lp.	Parametr	Wymagane minimalne parametry techniczne
1.	<b>Typ urządzenia</b>	Urządzenie skanujące z integracją do systemu AMMS Asseco z opcją drukowania i kopiowania
2.	<b>Automatyczny podajnik dokumentów</b>	Wymagany, o pojemności nie mniejszej niż 300 arkuszy, obsługujący formaty A6-A3; w gramaturze 35-210 g/m <sup>2</sup> - Jednoprzebiegowy.
3.	<b>Prędkość skanowania</b>	Min. 280 oryginałów/min. (300 dpi) zarówno w kolorze jak i w mono
4.	<b>Panel dotykowy / rozdzielczość</b>	Panel dotykowy o minimalnej przekątnej 10,1” oraz rozdzielczości 1024 x 600 personalizowany w języku polskim, z możliwością wyświetlania interfejsów zewnętrznych aplikacji np. do zarządzania wydrukiem, systemów OCR.
5.	<b>Tryby skanera</b>	Kolorowy sieciowy z możliwością skanowania 1) Skanowania na adres e-mail (Scan-to-Me) 2) Skanowanie do SMB (Scan-to-Home) 3) Skanowanie do FTP 4) Skanowanie do skrzynki (HDD) 5) Skanowanie do USB 6) Skanowanie do WebDAV 7) Skanowanie do DPWS 8) Skanowanie sieciowe TWAIN
6.	<b>Wyjściowe formaty plików skanera</b>	JPEG; TIFF; PDF; PDF/A; kompaktowy PDF; szyfrowany PDF; opcjonalnie: przeszukiwany PDF ; XPS; kompaktowy XPS; PPTX; DOCX, XLSX, RTF,TXT,
7.	<b>Funkcja zoom</b>	Co najmniej w zakresie od 25-400% w odstępach 0.1% ; automatyczne powiększenie zarówno z szyby ekspozycji jak i Automatycznego podajnika dokumentów.
8.	<b>Zużycie Energii</b>	220–240 V / 50/60 Hz; o mocy: 1,58 kW TEC max. 0,57kWh / Tydzień
9.	<b>Kopiowanie wielokrotne</b>	Co najmniej w zakresie 1 - 9,999
10.	<b>Zainstalowana pamięć</b>	Min. 7,0 GB RAM oraz twardy dysk SSD o pojemności min. 256 GB z możliwością rozbudowy do 1 TB
11.	<b>Wydajność wyjściowa</b>	Min. dwie tace o łącznej pojemności 2200 arkuszy
12.	<b>Protokoły sieciowe</b>	TCP/IP (IPv4/IPv6); SMB; LPD; IPP; SNMP; HTTP(S); Bonjour
13.	<b>Rozdzielczość kopiowania i skanowania</b>	Nie mniejsza niż 600 x 600 dpi
14.	<b>Maksymalny format papieru</b>	Nie mniejszy niż SRA3, możliwość wydruku banderowego długości 1,2m
15.	<b>Rozdzielczość drukowania</b>	Nie mniejsza niż 1,800 x 600 - 1,200 x 1,200
16.	<b>Interfejsy</b>	USB 2.0, 10/100/1000BaseTX

17.	<b>Funkcje drukarki</b>	Bezpośredni druk PDF, bezpośredni druk z pamięci USB
18.	<b>Funkcje monitorujące i raportujące</b>	Aplikacja umożliwiająca poprzez przeglądarkę internetową, dodawanie użytkowników (do 1000 kont użytkowników; obsługa również Active Directory (login + hasło + e-mail + katalog SMB)) z możliwością definiowania uprawnień do danych funkcji urządzenia np. Wydruk: mono / kolor, Kopia Mono / Kolor Skanowanie. Rozwiązanie winno umożliwiać również możliwość raportowania ilości wykonanych wydruków / kopii / skanów, poszczególnych użytkowników wpisanych do systemu. System musi posiadać autoryzację użytkownika na maszynie za pomocą: Identyfikatora, login / hasło lub <b>karty zbliżeniowej typu Unique 125 khz</b> , za pomocą której można zwalniać wydruki z serwera urządzenia.
19.	<b>Wymagane funkcje bezpieczeństwa</b>	ISO 15408 Common Criteria lub równoważny Filtrowanie IP i blokowanie portów; Komunikacja sieciowa SSL2; SSL3 i TLS1.0/1.1/1.2; Obsługa IPsec; Obsługa IEEE 802.1x; Uwierzytelnianie użytkowników; Dziennik uwierzytelniania; Bezpieczny wydruk; Kerberos; Nadpisywanie dysku twardego (min. 8 standardowych metod); Szyfrowanie danych na twardym dysku (AES 256); Automatyczne usuwanie danych z pamięci; Odbiór faksów poufnych; Szyfrowanie danych użytkownika drukarki; Skanowanie antywirusowe w czasie rzeczywistym, Ochrona przed kopiowaniem ( <b>Copy Guard, Password Copy</b> )
20.	<b>Wymagane oprogramowanie</b>	Aplikacja umożliwiająca zgłaszanie przez użytkowników problemów z urządzeniem – możliwość zgłoszenia problemów z działaniem urządzenia bezpośrednio z panelu urządzenia na zdefiniowany wcześniej e-mail. W przypadku problemów z wydrukiem istnieje możliwość załączenia skanu dokumentu oraz wpisania komentarza bezpośrednio z panelu urządzenia. Aplikacja musi mieć możliwość zgłaszania następujących predefiniowanych problemów: Uszkodzenie mechaniczne, Problem z kaseta papieru, Problem z podajnikiem ADF, Głośna praca urządzenia, Zacinanie papieru, Nie pobiera papieru, Zła jakość wydruku, Zabrudzenia na wydruku, Pogniczony wydruk, Nie można odebrać wydruku, Wdruk niepoprawny
21.	<b>Zawansowane funkcje bezpieczeństwa</b>	1) Zmiana Hasła Administratora (Indywidualne 16 znakowe hasło alfanumeryczne). 2) Szyfrowanie całej zawartości dysku twardego (Indywidualny 20-znakowy klucz szyfrujący). 3) Zabezpieczenie hasłem dysku twardego (Indywidualne 20-znakowe hasło alfanumeryczne). 4) Tymczasowe nadpisywanie danych w celu wyeliminowania wszelkich śladów danych (Klient może wybrać pomiędzy pojedynczym lub potrójnym nadpisywaniem). 5) Automatyczne usuwanie prac i związanych materiałów znajdujących się w elektronicznych folderach (Klient może wybrać żądane ustawienie czasu).
22.	<b>Wymagane certyfikaty dołączone do oferty.</b>	<b>Certyfikat ISO 27001</b> lub równoważny - System Zarządzania Bezpieczeństwem Informacji w Organizacji - Sprzedaż urządzeń wielofunkcyjnych i biurowych, projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania procesem druku, obiegiem dokumentacji. Dostarczanie usług serwisowych do urządzeń wielofunkcyjnych, biurowych, drukarek, urządzeń poligraficznych oraz rozwiązań informatycznych. Certyfikat wydany przez Jednostkę zrzeszoną w IAF - International Accreditation Forum. <b>Certyfikat ISO 20000</b> lub równoważny - System Zarządzania Usługami IT w Organizacji - Sprzedaż urządzeń wielofunkcyjnych i biurowych, projektowanie, sprzedaż i wdrażanie rozwiązań informatycznych do zarządzania procesem druku, obiegiem dokumentacji. Dostarczanie usług serwisowych do urządzeń wielofunkcyjnych, biurowych, drukarek, urządzeń poligraficznych oraz rozwiązań informatycznych. Certyfikat



		wydany przez Jednostkę zrzeszoną w IAF - International Accreditation Forum.
23.	<b>Wymagania gwarancji.</b>	Urządzenie winno mieć wykupiony min 36 miesięcznym pakiet gwarancji producenta sprzętu z dostępem do portalu zgłoszeń serwisowych.. Zamawiający nie dopuszcza gwarancji wystawionej przez subdystrybutora, dealera czy też brokera. Całość świadczeń instalacji i gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu i oprogramowania

Skaner typ 2 – 10 szt.

Skaner do długich dokumentów:

Lp.	Parametr	Wymagane parametry techniczne
1.	Typ skanera:	Szczelinowy
2.	Typ sensora:	CIS
3.	Zastosowanie:	Stacjonarne
4.	Interfejs:	LAN, USB, Wi-Fi
5.	Rozdzielczość optyczna [dpi]:	600 x 600
6.	Maksymalny format skanowania:	215.9 x 6096 mm
7.	Skanowanie w pionie:	Nie
8.	Skanowanie do e-maila:	Tak
9.	Wyświetlacz:	Tak
10.	Tryby skanowania:	Czarno-biały, Kolor, Odcienie szarości
11.	Źródło światła:	LED
12.	Prędkość skanowania w czerni [str./min]:	40
13.	Prędkość skanowania w kolorze [str./min]:	40
14.	Zalecany dzienny tryb pracy [str.]:	6500
15.	Podajnik dokumentów [ADF]:	Tak
16.	Pojemność podajnika dokumentów [ADF]:	100 stron
17.	Obsługiwane formaty plików:	BMP, DOCX, JPEG, PDF, PDF/A, PNG, PPTX, TIFF, XLSX
18.	Obsługiwane formaty nośników:	A4, A5, A6, B4, B5, B6, DL (koperta), Legal, Letter, Plastikowa karta, Poczтівка, Wizytówka
19.	Głębia koloru [bit]:	24 (wyjście), 30 (wejście)
20.	Głębia szarości [bit]:	10 (wejście), 8 (wyjście)
21.	Skan dwustronny:	Tak
22.	Skanowanie bez komputera:	Tak
23.	Skanowanie w pionie:	Nie
24.	Skanowanie do e-maila:	Tak
25.	Skanowanie do chmury:	Tak
26.	Wyświetlacz:	Tak
27.	Przystawka do negatywów:	Nie
28.	Obsługiwane systemy:	macOS 10.6+, Windows 10, Windows 11, Windows Server 20016, Windows Server 20022, Windows Server 2025
29.	Pobór mocy [W]:	13 (USB), 14 (LAN)
30.	Temperatura pracy [st. C]:	Od +5 do +35
31.	Wilgotność pracy [%]:	Od 15 do 80
32.	Złącza:	RJ-45 - 1 szt., USB 2.0 - 1 szt., Złącze zasilania - 1 szt.

33.	Dodatkowe informacje:	Automatyczna korekta położenia ukośnego, Automatyczne rozpoznawanie dokumentów wielostronicowych, Automatyczny obrót obrazu, Blokada panelu z hasłem, Detektor podwójnych arkuszy, Funkcja Push Scan, Funkcje kompresji pliku, IPv6, Łączenie skanów A3, Obsługuje papier o gramaturze od 27 do 413 g/m <sup>2</sup> , Pomijanie pustych stron, Poprawa tekstu, Rozpoznawanie kodu kreskowego, Rozszerzona edycja obrazu, Scan to Cloud Storage, Separacja zadań, Skanowanie do SFTP, Skanowanie na FTP, Usuwanie otworów po dziurkaczu, Wstępnie zdefiniowane ustawienia, Wygładzenie krawędzi, Wykrywanie zabrudzeń Parametry
34.	Zasilanie:	Sieciowe
35.	Kolor obudowy:	Biało-czarny
36.	Wyposażenie:	Kabel USB, Kabel zasilający, Zasilacz
37.	Gwarancja:	12 miesięcy

## VII. Część nr 5

### Zakup rozwiązania integracyjnego PUI (Platformy Usług Inteligentnych)

Lp.	PUI Connector	
1.	<b>System umożliwia integrację z PUI (Platformą Usług Inteligentnych) dostarczaną przez CEZ (Centrum eZdrowie) w zakresie AI, minimum w zakresie zapewnienia funkcjonalności:</b>	
a)	System zapewnia bezpieczne podłączenia do PUI szyfrowanym kanałem z uwzględnieniem mechanizmów autoryzacji i autentykacji wymaganych w ramach PUI	Tak
b)	Mechanizmy integracyjne zapewniają komunikację bez konieczności dodatkowego logowania się do innych systemów niż RIS/PACS	Tak
c)	Przekazania do PUI wybranych badań do analizy za pomocą mechanizmów standardu DICOM	Tak
d)	Przyjęcia wyniku przetwarzania zadanego badania na PUI z wykorzystaniem formatu HL7CDA, Interoperacyjności zapewnianej przez standard FHIR	Tak
e)	Możliwość komunikacji z wykorzystaniem REST API oraz formatu JSON	Tak
f)	Możliwość wywołania interfejsu użytkownika platformy PUI, jeżeli taki interfejs będzie wymagany do pracy z PUI	Tak
2.	<b>W zakresie dostosowania systemu RIS/PACS do kooperacji z PUI:</b>	
a)	System umożliwia skonfigurowanie zasad automatyczne przekazywania obrazów przypisanych do konkretnych badań na podstawie wybranych kryteriów (minimum rodzaj badania, modalność)	Tak
b)	System prezentuje wyniki przetwarzania AI w interfejsie użytkownika, w formie zależnej od konkretnych algorytmów, przez które dane badanie zostało przetworzone	Tak
c)	System prezentuje ewentualne informacje techniczne, w tym informacje dotyczące błędów przetwarzania, jeżeli są dostępne za pomocą mechanizmów integracyjnych	Tak
d)	System zapewni repozytorium EDM utrzymujące dokumenty zgodnie z wymaganiami CEZ zgodnie HL7 CDA PIK lub alternatywnie zapewni możliwość integracji z działającym obecnie repozytorium EDM danego świadczeniodawcy w zakresie umożliwiającym indeksowanie i udostępnianie EDM.	Tak

## VIII. Część nr 6

### 1.14 System telekonsultacji dostarczony na zasadach SaaS lub Managed Service, umożliwiający zdalną ocenę badań obrazowych w chmurze oraz przekazywanie opisów w standardzie HL7 CDA.

Wymagania:

Lp.	Wymagania	
I.	<b>System telekonsultacji zintegrowany z posiadanym RIS/PACS</b>	
1.	System telekonsultacji dostarczony na zasadach SaaS lub Managed Service (usługa zarządzana), umożliwiający zdalną ocenę badań obrazowych w tym elastografii (2D/3D) z wbudowanym archiwum obrazów w chmurze o pojemności minimum 5 TB.	TAK
2.	Wbudowana chmurowa przeglądarka webowa diagnostyczna i referencyjna obrazów DICOM zapewniająca pogląd obrazów, bez konieczności instalacji dodatkowych komponentów na stacjach klienckich takich jak kontrolki ActiveX, applety JAVA, pluginy NPAPI czy pakiety JAVA webstart, umożliwiającą pracę w trybie diagnostycznym minimum 2 lekarzom równocześnie.	TAK
3.	Dostęp do zgromadzonych w systemie obrazów do celów telekonsultacji poprzez protokół DICOMweb (WADO-RS, QUIDO-RS, STOW-RS).	TAK
4.	Obsługa asynchronicznego C-MOVE i C-GET oraz możliwość konfiguracji przez użytkownika administracyjnego równoległego przesyłania obrazów w ramach operacji CMOVE dla wybranych węzłów DICOM dla zapewnienia optymalnego wykorzystania łącza internetowego.	TAK
5.	Obsługa asynchronicznych transferów DICOM DIMSE.	TAK
6.	Możliwość szybkiego pobrania i otwarcia obrazów DICOM za pomocą jednego kliknięcia z poziomu okna opisu badania na stacjach roboczych: OsiriX MD, RadiAnt, Tomocon, Weasis, eFilm, INFINITT, syngoVia, AW server, iQ VIEW, Carestream, OHIF.	TAK
7.	Funkcjonalność udostępniania obrazów - możliwość generowania, zabezpieczonego kodem PIN, linka HTTPS pozwalającego na dostęp do obrazów z dowolnego miejsca z użyciem wbudowanej webowej przeglądarki referencyjnej obrazów DICOM. Możliwość zarządzania wygenerowanymi linkami do obrazów, w tym możliwość ich dezaktywacji oraz śledzenia historii dostępu.	TAK
8.	Możliwość automatycznego umieszczania w szablonach opisów telekonsultacji fraz w oparciu o dane z tagów DICOM oraz dane wprowadzone w systemie, w tym minimum powiązane z badaniem dane dotyczące: użytych kontrastów i leków (ilość, rodzaj, droga podania), działań niepożądanych po dożylnym podaniu kontrastu (opis, data wystąpienia) poziom kreatyniny i GFR waga i wzrost pacjenta, BMI dla pacjentów >18 rż. dostarczonych przez pacjenta i dostępnych w systemie poprzednich badań obrazowych pacjenta (modalności, daty wykonania, nazwy) sumarycznej liczby serii i obrazów w badaniu, danych klinicznych podanych na zleceniu/e-skierowaniu, nazwy poszczególnych sekwencji (Series Description, Protocol Name), rozpoznań ICD10 wraz z opisem tekstowym kodów podanych na zleceniu/e-skierowaniu, celu badania określonego na zleceniu/e-skierowaniu	TAK
9.	Zgodność tworzenia opisów z HL7 CDA PIK i EDM (opisy badań diagnostycznych muszą być tworzone w wersji elektronicznej w HL7 CDA i podpisywane elektronicznie).	TAK
10.	Obsługa kwalifikowanego podpisu cyfrowego min. Certum, KIR, SimplySign w systemach Windows i MacOS.	TAK
11.	Obsługa podpisu cyfrowego ZUS z możliwością podpisywania PDF i EDM w systemach Windows i MacOS	TAK
12.	Możliwość zbiorczego podpisywania elektronicznego wyników telekonsultacji zarówno podpisem kwalifikowanym jak i podpisem ZUS.	TAK
13.	Uwierzytelnianie wieloskładnikowe 2FA/MFA z możliwością wygenerowania jednorazowych kodów zapasowych.	TAK
14.	Zarządzanie przez użytkowników własnym profilem z możliwością minimum zmiany hasła i włączenia logowania dwuskładnikowego.	TAK
15.	System zapewnia skanowanie antywirusowe wszystkich plików wczytywanych do systemu przez użytkownika, w tym skanów dokumentów, załączników do badań, plików HL7 CDA, obrazów, plików dźwiękowych z nagrań, a w przypadku wykrycia złośliwego oprogramowania uniemożliwić zapisanie pliku do systemu, poinformować o tym użytkownika końcowego i odnotować zdarzenie w logach dostępnych dla administratora.	TAK
16.	System zapewnia skanowanie antywirusowe „w locie” wszystkich plików DICOM wczytywanych do systemu, w tym danych obrazowych pochodzących z podłączonych aparatów diagnostycznych, wszelkich zewnętrznych węzłów DICOM oraz badań porównawczych, wczytywanych z	TAK

	nośników zewnętrznych. W przypadku wykrycia złośliwego oprogramowania, system musi uniemożliwić zapisanie pliku do systemu, poinformować o tym użytkownika końcowego i odnotować zdarzenie w logach dostępnych dla administratora.	
17.	Gwarancja: 36 - miesiące	TAK
<b>II. Moduł Importu zewnętrznej dokumentacji medycznej</b>		
1.	System posiada funkcję importu zewnętrznej dokumentacji medycznej.	TAK
2.	System posiada funkcję importu dokumentacji medycznej, w szczególności obrazów DICOM oraz dokumentów opisu badania.	TAK
3.	System posiada funkcję automatycznego wyszukiwania i identyfikacji badań na podstawie informacji zawartych w plikach DICOM DIR.	TAK
4.	System zapewnia obsługę zewnętrznych nośników danych (DVD, pamięci USB, etc.).	TAK
5.	System przeprowadza walidację tożsamości pacjenta, w kontekście którego dodawane jest badanie, w celu zapewnienia zgodności z danymi importowanej dokumentacji medycznej.	TAK
6.	System automatycznie wybiera dokument badania w formacie HL7 CDA.	TAK
7.	System umożliwia przesłanie obrazów na serwer PACS.	TAK
8.	System wspiera intuicyjną funkcję „przeciągnij i upuść” (Drag and Drop) w celu ułatwienia importu danych.	TAK
9.	System umożliwia podgląd zaimportowanych dokumentów zawierających wyniki badań.	TAK
10.	System umożliwia podgląd zaimportowanych obrazów w formacie DICOM.	TAK
11.	System umożliwia opisanie importowanych badań metadanymi, w tym co najmniej datą wykonania badania, modalnością i rodzajem badania.	TAK
12.	System zapewnia funkcję filtrowania wcześniej zaimportowanych badań.	TAK
13.	System zapewnia dostępność zaimportowanych badań bezpośrednio z poziomu wyszukiwarki w systemie RIS.	TAK
14.	System umożliwia przekazanie do systemów zewnętrznych danych zaimportowanego badania wraz z URL do obrazów za pomocą mechanizmów integracyjnych.	TAK

## IX. Część nr 7

### 3.5 Zakup platformy do kompleksowej ochrony z XDR zapobiegająca naruszeniom bezpieczeństwa oraz skanowanie podatności oraz Sandboxing

Przedmiotem zamówienia jest licencja systemu XDR zapobiegająca naruszeniom bezpieczeństwa oraz skanowanie podatności oraz Sandboxing liczba stanowisk: 200 z okresem wsparcia i aktualizacji 3 lata

Zamawiający posiada obecnie 150 licencji na ESET PROTECT Enterprise ON-PREM z okresem ważności licencji do 2028-02-13.

System musi spełniać następujące wymagania:

#### **Administracja zdalna.**

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
  - 1) pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
  - 2) pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
  - 3) puforowanie ruchu HTTPS.
6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej
  - 1) uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
    - a) Google Authenticator,
    - b) Microsoft Authenticator,
    - c) Authy,
    - d) Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania
8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
  - 1) grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
    - a) adresy sieciowe IP,
    - b) aktywne zagrożenia,
    - c) stan funkcjonowania oraz ochrony,
    - d) wersja systemu operacyjnego,
    - e) podzespoły komputera.
10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
  - 1) wyrażenie CRON,
  - 2) codziennie,
  - 3) cotygodniowo,
  - 4) co miesiąc,
  - 5) co rok,
  - 6) po wystąpieniu nowego zdarzenia,
  - 7) po automatycznym umieszczeniu hosta w grupie dynamicznej.
11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim
  - 1) język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
12. Rozwiązanie musi mieć możliwość tagowania obiektów.
13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
  - 1) Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.



14. Rozwiązanie musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w systemie centralnego zarządzania.

#### **Ochrona stacji roboczych - Windows**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - 1) wirus,
  - 2) trojan,
  - 3) robak,
  - 4) adware,
  - 5) spyware,
  - 6) dialer,
  - 7) phishing,
  - 8) backdoor.
4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware:
  - 1) technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
  - 2) technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
  - 3) technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - 1) całego dysku,
  - 2) wybranych katalogów,
  - 3) pojedynczych plików,
  - 4) plików spakowanych oraz skompresowanych,
  - 5) dysków sieciowych,
  - 6) dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - 1) wybranych plików,
  - 2) wybranych procesów,
  - 3) wybranych lokalizacji,
  - 4) wybranych rozszerzeń,
  - 5) nazwy wykrycia,
  - 6) sumy kontrolnej (SHA1).
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - 1) sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
  - 2) konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
  - 3) konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy

- sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 1) typ urządzenia:
    - a) pamięci masowe,
    - b) optyczne pamięci masowe,
    - c) pamięci masowe Firewire,
    - d) urządzenia do tworzenia obrazów,
    - e) drukarki USB,
    - f) urządzenia Bluetooth,
    - g) czytniki kart inteligentnych,
    - h) modemy,
    - i) porty LPT/COM,
    - j) urządzenia przenośne.
  - 2) parametry urządzenia:
    - a) numer seryjny,
    - b) producent,
    - c) model.
  - 3) typ dostępu:
    - a) brak możliwości zapisu,
    - b) pełen dostęp,
    - c) ostrzeżenie użytkownika,
    - d) brak dostępu.
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 1) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - 2) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  - 3) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  - 4) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
  - 5) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 1) Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
  - 2) Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
  - 3) Raport musi posiadać co najmniej:
    - a) Listę zainstalowanych aplikacji,
    - b) Listę usług systemowych,
    - c) Informacje o systemie operacyjnym i sprzęcie,
    - d) Listę aktywnych procesów i połączeń sieciowych,
    - e) Harmonogram systemu operacyjnego,
    - f) Szczegóły pliku hosts,
    - g) Informacje o sterownikach.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
- 1) antywirus,
  - 2) zaporę osobistą
  - 3) sandbox,
  - 4) antyspyware,
  - 5) metody heurystyczne.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- 1) Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.

- 2) Ochrona musi być realizowana w oparciu o co najmniej:
  - a) globalna czarna lista RBL,
  - b) czarna lista użytkownika,
  - c) biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
  - 1) Ochrona przed anomaliami sieciowymi, w tym co najmniej:
    - a) Skanowanie portów TCP oraz UDP,
    - b) Wykrywanie duplikacji adresu IP,
    - c) Atak zatrutowania ARP,
    - d) Nieprawidłowa długość pakietu TCP oraz UDP.
  - 2) Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
    - a) RDP,
    - b) SMB,
    - c) My SQL,
    - d) MS SQL.
  - 3) Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
  - 1) Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
  - 2) Zapora osobista musi posiadać co najmniej cztery tryby pracy:
    - a) tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - b) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - c) tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
    - d) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
  - d.1) administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
  - 1) Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
  - 2) Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
  - 3) W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
  - 1) Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
  - 2) Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
    - a) treść komunikatu,
    - b) obraz.

### **Ochrona stacji roboczych – MacOS**

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - 1) wirus,
  - 2) trojan,
  - 3) robak,
  - 4) adware,
  - 5) spyware,

- 6) dialer,
- 7) phishing,
- 8) backdoor.
- 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- 6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
  - 1) Sygnatur wirusów.
  - 2) Reputacji chmurowej.
- 7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- 8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - 1) sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
  - 2) konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
  - 3) konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- 9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - 1) całego dysku,
  - 2) wybranych katalogów,
  - 3) pojedynczych plików,
  - 4) plików spakowanych oraz skompresowanych,
  - 5) dysków sieciowych,
  - 6) dysków przenośnych.
- 10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - 1) wybranych plików,
  - 2) wybranych procesów,
  - 3) wybranych lokalizacji,
  - 4) wybranych rozszerzeń,
  - 5) nazwy wykrycia,
  - 6) sumy kontrolnej (SHA1).
- 11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
  - 1) zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
  - 2) zapora osobista musi posiadać co najmniej dwa tryby pracy:
    - a) tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - b) tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

### **Ochrona stacji roboczych – Linux**

- 1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
  - 1) Ubuntu Desktop,
  - 2) Red Hat Enterprise Linux
  - 3) Linux Mint.
- 2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
  - 1) Cinnamon,
  - 2) GNOME,
  - 3) KDE,
  - 4) MATE,
  - 5) XFCE.
- 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - 1) wirus,
  - 2) trojan,

- 3) robak,
  - 4) adware,
  - 5) spyware,
  - 6) dialer,
  - 7) phishing,
  - 8) backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
  5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
  6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    - 1) Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    - 2) Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
  7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    - 1) całego dysku,
    - 2) wybranych katalogów,
    - 3) pojedynczych plików,
    - 4) plików spakowanych oraz skompresowanych,
    - 5) dysków sieciowych,
    - 6) dysków przenośnych.
  8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - 1) wybranych plików,
    - 2) wybranych procesów,
    - 3) wybranych lokalizacji,
    - 4) wybranych rozszerzeń,
  9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    - 1) typ urządzenia:
      - a) pamięci masowe,
      - b) optyczne pamięci masowe,
    - 2) parametry urządzenia:
      - a) numer seryjny,
      - b) producent,
      - c) model.
    - 3) typ dostępu:
      - a) brak możliwości zapisu,
      - b) pełen dostęp,
      - c) brak dostępu.

### **Ochrona serwera – Windows Server**

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
  - 1) Microsoft Windows Server 2012 R2,
  - 2) Microsoft Windows Server 2016,
  - 3) Microsoft Windows Server 2019,
  - 4) Microsoft Windows Server 2022,
  - 5) Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - 1) wirus,
  - 2) trojan,
  - 3) robak,
  - 4) adware,
  - 5) spyware,
  - 6) dialer,

- 7) phishing,
- 8) backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - 1) sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
  - 2) konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
  - 3) konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - 1) całego dysku,
  - 2) wybranych katalogów,
  - 3) pojedynczych plików,
  - 4) plików spakowanych oraz skompresowanych,
  - 5) dysków sieciowych,
  - 6) dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - 1) wybranych plików,
  - 2) wybranych procesów,
  - 3) wybranych lokalizacji,
  - 4) wybranych rozszerzeń,
  - 5) nazwy wykrycia,
  - 6) sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  - 1) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - 2) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  - 3) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  - 4) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
  - 5) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
  - 1) Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
  - 2) Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
  - 3) Raport musi posiadać co najmniej:
    - a) Listę zainstalowanych aplikacji,
    - b) Listę usług systemowych,
    - c) informacje o systemie operacyjnym i sprzęcie,
    - d) Listę aktywnych procesów i połączeń sieciowych,
    - e) harmonogram systemu operacyjnego,
    - f) Szczegóły pliku hosts,
    - g) Informacje o sterownikach.
14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:



- 1) antywirus,
  - 2) zaporą osobistą
  - 3) sandbox,
  - 4) antyspyware,
  - 5) metody heurystyczne.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- 1) typ urządzenia:
    - a) pamięci masowe,
    - b) optyczne pamięci masowe,
    - c) pamięci masowe Firewire,
    - d) urządzenia do tworzenia obrazów,
    - e) drukarki USB,
    - f) urządzenia Bluetooth,
    - g) czytniki kart inteligentnych,
    - h) modemy,
    - i) porty LPT/COM,
    - j) urządzenia przenośne.
  - 2) parametry urządzenia:
    - a) numer seryjny,
    - b) producent,
    - c) model.
  - 3) typ dostępu:
    - a) brak możliwości zapisu,
    - b) pełen dostęp,
    - c) ostrzeżenie użytkownika,
    - d) brak dostępu.
18. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
- 1) MS SQL,
  - 2) Active Directory,
  - 3) IIS,
  - 4) Sysvol,
  - 5) DNS,
  - 6) DHCP,
  - 7) Hyper-V,
  - 8) Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 1) ochrona przed anomaliami sieciowymi, w tym co najmniej:
    - a) skanowanie portów TCP oraz UDP,
    - b) wykrywanie duplikacji adresu IP,
    - c) atak zatrutowania ARP,
    - d) nieprawidłowa długość pakietu TCP oraz UDP.
  - 2) Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
    - a) RDP,
    - b) SMB,
    - c) My SQL,
    - d) MS SQL.
  - 3) Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
- 1) Zapora osobista musi posiadać co najmniej cztery tryby pracy:
    - a) tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

- b) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  - c) tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
  - d) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- d.1) Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

## Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
  - 1) RedHat Enterprise Linux (RHEL),
  - 2) Rocky Linux,
  - 3) Ubuntu,
  - 4) Debian,
  - 5) SUSE Linux Enterprise Server (SLES),
  - 6) Oracle Linux,
  - 7) Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - 1) wirus,
  - 2) trojan,
  - 3) robak,
  - 4) adware,
  - 5) spyware,
  - 6) dialer,
  - 7) phishing,
  - 8) backdoor.
3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - 1) konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
  - 2) konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - 1) całego dysku,
  - 2) wybranych katalogów,
  - 3) pojedynczych plików,
  - 4) plików spakowanych oraz skompresowanych,
  - 5) dysków sieciowych,
  - 6) dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - 1) wybranych plików,
  - 2) wybranych procesów,
  - 3) wybranych lokalizacji,
  - 4) wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
  - 1) lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonych mikro-serwisu.

13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
- 1) proces budowania obrazu kontenera,
  - 2) wdrażanie obrazu kontenera.

### **Mobile Device Management**

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
  - 1) MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
    - a) Android,
    - b) iOS,
    - c) iPadOS.
  - 2) MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
    - a) Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
    - b) Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
    - c) VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
    - d) Apple Business Manager (ABM),
    - e) Android Enterprise (co najmniej w zakresie Device Owner).
3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
  - 1) usunięcie zawartości urządzenia,
  - 2) przywrócenie urządzenia do ustawień fabrycznych,
  - 3) zablokowanie urządzenia,
  - 4) uruchomienie sygnału dźwiękowego,
  - 5) lokalizację GPS,
  - 6) Resetowanie hasła blokady ekranu.
4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. MDM musi umożliwiać co najmniej:
  - 1) Dla systemów iOS oraz iPadOS:
    - a) konfigurację kont e-mail,
    - b) konfigurację połączeń VPN,
    - c) konfigurację połączeń Wi-Fi,
    - d) konfigurację listy certyfikatów,
    - e) możliwość uruchomienia trybu jednej aplikacji.
  - 2) Dla systemu Android:
    - a) blokadę wykonywania połączeń,
    - b) blokadę konfiguracji sieci Wi-Fi,
    - c) blokadę konfiguracji tuneli VPN,
    - d) zarządzanie aktualizacjami systemu operacyjnego,
    - e) blokadę zmiany tapety urządzenia.

### **Mobile Threat Defense (MTD) dla systemu Android**

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
  - 1) inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
  - 2) dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
  - 1) złożoność kodu blokady ekranu:
    - a) Wzór,
    - b) PIN,

- c) Hasło,
- 2) przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
- 3) zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
- 5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
  - 1) nazwę aplikacji,
  - 2) nazwę pakietu,
  - 3) kategorię sklepu Google Play,
  - 4) uprawnienia aplikacji,
  - 5) pochodzenie aplikacji z nieznanego źródła.
- 6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

### **Sandbox w chmurze**

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy w tym co najmniej:
  - 1) Microsoft Windows 10 oraz 11,
  - 2) Microsoft Windows Server,
  - 3) macOS 11 (Big Sur) oraz nowszych
  - 4) RedHat Enterprise Linux (RHEL),
  - 5) Rocky Linux,
  - 6) Ubuntu,
  - 7) Debian,
  - 8) SUSE Linux Enterprise Server (SLES),
  - 9) Oracle Linux,
  - 10) Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
  - 1) archiwa,
  - 2) skrypty,
  - 3) pliki wykonywalne,
  - 4) pliki rejestru systemowego (.reg),
  - 5) możliwy spam,
  - 6) dokumenty.
7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
  - 1) natychmiast po ich przeanalizowaniu,
  - 2) po upływie 30 dni,
  - 3) nigdy.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzania.
11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
  - 1) administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
  - 1) czysty,
  - 2) podejrzany,

- 3) bardzo podejrzany,
- 4) szkodliwy.
14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
  - 1) wstrzymania uruchamiania pobieranych plików z następujących źródeł:
    - a) przeglądarki internetowej,
    - b) programy poczty e-mail,
    - c) nośniki wymienne,
    - d) pliki wydzielone z archiwum.
15. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
16. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

## Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
  - 1) Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
  - 2) Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
  - 1) hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
  - 2) hasło odzyskiwania nie może być krótsze niż 8 znaków.
  - 3) hasło odzyskiwania nie może być dłuższe niż 20 znaków.
7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
10. Rozwiązanie musi wspierać dyski wykorzystujące funkcję OPAL w wersji co najmniej 2.0.
11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

## Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
  - 1) tworzenie procesów,
  - 2) uruchamianie, zatrzymanie i modyfikacja usług,
  - 3) utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,
  - 4) usuwanie oraz zmiana nazw plików,
  - 5) tworzenie i usuwanie kluczy rejestru systemowego,
  - 6) ładowanie bibliotek DLL,
  - 7) zalogowanie użytkowników,
  - 8) elementy sieciowe, w tym co najmniej:
    - a) pobranie plików wykonywalnych,
    - b) zestawienie połączeń TCP/IP,
    - c) zapytania HTTP,
    - d) zapytania DNS.

4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.
  - 1) Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
    - a) blokowanie pliku wykonywalnego,
    - b) blokowanie pliku wykonywalnego i poddanie go kwarantannie,
    - c) blokowanie podejrzanej biblioteki DLL,
    - d) zakończenie procesu,
    - e) skanowanie komputera w poszukiwaniu zagrożeń,
    - f) wyłączenie komputera,
    - g) izolacja sieciowa hosta,
    - h) wylogowanie użytkownika.
  - 2) Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.
5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
  - 1) Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
  - 2) Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:
    - a) proces,
    - b) proces nadrzędny (proces rodzica),
    - c) nazwę procesu,
    - d) ścieżkę procesu,
    - e) wiersz polecenia,
    - f) wydawcę,
    - g) typ podpisu,
    - h) SHA-1,
    - i) SHA-2,
    - j) użytkownika.
  - 3) Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
  - 1) W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
  - 2) Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):
    - a) SHA-1,
    - b) SHA-256.
7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
  - 1) hash pliku SHA-1,
  - 2) hash pliku SHA-256,
  - 3) hash pliku MD5,
  - 4) typ sygnatury podpisu cyfrowego,
  - 5) wydawcę certyfikatu,
  - 6) wersję pliku,
  - 7) oryginalną nazwę pliku,
  - 8) rozmiar pliku,
  - 9) reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,
  - 10) pierwsze uruchomienie pliku w środowisku,
  - 11) ostatnie uruchomienie pliku w środowisku,
8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
  - 1) oznaczania ich jako bezpieczne lub niebezpieczne,
  - 2) pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
  - 3) zablokowania wykonywania i wykorzystania pliku,
  - 4) wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.



9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
  - 1) administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
  - 2) pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
  - 3) wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
  - 4) administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
  - 1) Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.

### **Ochrona serwera pocztowego MS Exchange**

1. Rozwiązanie musi wspierać co najmniej następujące serwery poczty:
  - 1) Microsoft Exchange 2010 SP3,
  - 2) Microsoft Exchange 2013,
  - 3) Microsoft Exchange 2016,
  - 4) Microsoft Exchange 2019.
2. Rozwiązanie musi zapewniać wsparcie co najmniej dla następujących ról:
  - 1) Mailbox,
  - 2) Edge,
  - 3) Hub.
3. Rozwiązanie musi być instalowane na maszynie z serwerem pocztowym Exchange.
4. Wszystkie komponenty rozwiązania ochrony serwera pocztowego Exchange muszą pracować na tym samym serwerze, na którym zainstalowany jest Microsoft Exchange (Rozwiązanie nie może pracować jako rozwiązanie typu gateway).
5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
6. Rozwiązanie musi skanować pocztę wewnętrzną (ruch pocztowy w obrębie serwera Microsoft Exchange).
7. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
8. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.
  - 1) Rozwiązanie musi posiadać co najmniej następujące warunki:
    - a) nadawca,
    - b) odbiorca,
    - c) temacie wiadomości,
    - d) adres IP nadawcy,
    - e) nazwa, rozmiar i typ załącznika,
    - f) rozmiar wiadomości,
    - g) nagłówek wiadomości,
    - h) godzina odbioru,
    - i) obecność załącznika chronionego hasłem,
    - j) wynik SPF, DKIM i DMARC.
  - 2) Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
    - 1) poddaj wiadomość kwarantannie,
    - 2) odrzuć wiadomość,
    - 3) porzuć wiadomość w trybie dyskretnym,
    - 4) usuń załącznik,
    - 5) dodaj prefix tematu,
    - 6) wyślij powiadomienie e-mail,
    - 7) pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.
9. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.

10. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
11. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
12. Rozwiązanie musi posiadać mechanizm greylisting (szara lista).
13. Rozwiązanie musi umożliwiać podpisywanie wiadomości za pomocą DKIM.

### **Ochrona usług chmurowych**

1. Rozwiązanie musi posiadać odrębną konsolę centralnego zarządzania:
  - 1) konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS),
  - 2) konsola centralnego zarządzania musi być dostępna z poziomu interfejsu
  - 3) WWW,
  - 4) konsola centralnego zarządzania musi być zabezpieczona za pośrednictwem protokołu szyfrowanego SSL/TLS.
  - 5) konsola centralnego zarządzania musi być dostępna co najmniej w języku polskim oraz angielskim.
2. Rozwiązanie musi obejmować ochronę dla co najmniej następujących usług:
  - 1) Microsoft Exchange Online,
  - 2) Microsoft OneDrive,
  - 3) Microsoft Sharepoint,
  - 4) Microsoft Teams,
  - 5) Google Workspace, w tym co najmniej
    - a) Gmail,
    - b) Google Drive.
3. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.
4. Rozwiązanie musi umożliwiać:
  - 1) wybór ręczny kont użytkowników, które będą objęte ochroną,
  - 2) wybór automatyczny całego tenantu, gdzie nowo utworzone konta będą automatycznie chronione.
5. Rozwiązanie musi posiadać możliwość raportowania w tym co najmniej:
  - 1) kont użytkowników, otrzymujących najwięcej spamu,
  - 2) kont użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
  - 3) kont użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
  - 4) kont użytkowników, które mogą być podejrzan.
6. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty.
7. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.
  - 1) rozwiązanie musi posiadać co najmniej następujące warunki:
    - a) nadawca,
    - b) temacie wiadomości,
    - c) adres IP nadawcy,
    - d) nazwa, rozszerzenie i typ załącznika,
    - e) nagłówek wiadomości,
    - f) godzina odbioru,
    - g) wynik SPF, DKIM, DMARC i ARC.
  - 2) rozwiązanie musi posiadać co najmniej następujące akcje w regułach:
    - a) poddaj wiadomość kwarantannie,
    - b) usuń wiadomość,
    - c) usuń załącznik,
    - d) dodaj prefix tematu,
    - e) wyślij powiadomienie e-mail,
    - f) pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.
8. Rozwiązanie musi umożliwiać pobranie plików z kwarantanny co najmniej:
  - 1) w formie oryginalnego pliku,
  - 2) w formie pliku zabezpieczonego hasłem.
9. Rozwiązanie musi umożliwiać przypisanie polityk co najmniej na poziomie:
  - 1) całego tenantu,
  - 2) grupy,

- 3) grupy Teams,
- 4) lokacji Sharepoint,
- 5) pojedynczego użytkownika.
10. Rozwiązanie musi korzystać z chmury reputacji plików, pochodzącego od tego samego producenta rozwiązania antywirusowego:
  - 1) możliwość automatycznego wysłania sumy kontrolnej 10.2.      możliwość      automatycznego wysłania fragmentu pliku.
11. Rozwiązanie musi umożliwiać określenie czynności realizowanej po wykryciu zagrożenia, w tym co najmniej następujące czynności:
  - 1) brak czynności,
  - 2) przenieś do spamu,
  - 3) poddaj wiadomość kwarantannie,
  - 4) poddaj załącznik kwarantannie,
  - 5) przenieś do kosza,
  - 6) usuń załącznik,
  - 7) zastąp załącznik
  - 8) usuń wiadomość.
12. Rozwiązanie musi umożliwiać dodanie znacznika do tematu wiadomości zaklasyfikowanej co najmniej jako:
  - 1) SPAM,
  - 2) phishing.
13. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
  - 1) archiwa,
  - 2) skrypty,
  - 3) pliki wykonywalne,
  - 4) pliki rejestru systemowego (.reg),
  - 5) możliwy spam,
  - 6) dokumenty.
14. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
  - 1) natychmiast po ich przeanalizowaniu,
  - 2) po upływie 30 dni, 1
  - 3) nigdy.
15. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail.
  - 1) Powiadomienia muszą dotyczyć wykryć co najmniej:
    - a) zagrożeń w wiadomościach,
    - b) phishing w wiadomościach,
    - c) zagrożeń w plikach onedrive,
    - d) zagrożeń na dysku Google Drive,
  - 2) Powiadomienia muszą być możliwe do wysłania w co najmniej jednym z następujących języków:
    - a) Język polski,
    - b) Język angielski.

### **Vulnerability Assessment and Patch Management**

1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
2. Rozwiązanie musi mieć możliwości wykrywania podatności:
  - 1) w tym co najmniej następujących systemach operacyjnych:
    - a) Windows,
    - b) macOS,
    - c) Linux
  - 2) w aplikacjach zainstalowanych na zarządzanych stacjach.
3. Rozwiązanie musi posiadać bazę podatności zawierającą co najmniej 35000 CVE.
4. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych. Zarządzanie musi się odbywać z poziomu tej samej konsoli co rozwiązanie antywirusowe, pochodzące od tego samego producenta.
5. Rozwiązanie musi umożliwiać utworzenie harmonogramu automatycznego wykrywania podatności.
6. Rozwiązanie musi umożliwiać wyświetlanie szczegółów danej podatności zawierające co najmniej:

- 1) nazwę aplikacji lub systemu operacyjnego
- 2) punktację CVSS
- 3) opis wykrytej podatności
- 4) wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
7. Rozwiązanie musi wykrywać podatności w minimum 700 aplikacjach.
8. Rozwiązanie musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 300 popularnych aplikacji.
9. Rozwiązanie musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji.
  - 1) Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście.
  - 2) Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Rozwiązanie musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.
  - 1) Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.
  - 2) Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
11. Rozwiązanie musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
12. Rozwiązanie musi być zintegrowane bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
13. Rozwiązanie musi umożliwiać wyłączenie powiadomień dla wybranej podatności.

#### **Two-factor authentication / Multi-factor authentication**

1. Rozwiązanie musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi pozwalać na instalację oprogramowania na co najmniej następujących systemach operacyjnych:
  - 1) Systemy serwerowe:
    - a) Microsoft Windows Server 2012 R2,
    - b) Microsoft Windows Server 2016,
    - c) Microsoft Windows Server 2019,
    - d) Microsoft Windows Server 2022,
    - e) Microsoft Windows Server 2025.
  - 2) Systemy kliencie:
    - a) Windows 8.1,
    - b) Windows 10,
    - c) Windows 11.
5. Rozwiązanie musi posiadać integrację z następującymi rozwiązaniami:
  - 1) Microsoft Exchange,
  - 2) Microsoft Dynamics CRM,
  - 3) Microsoft Sharepoint,
  - 4) Microsoft Remote Desktop Web Access,
  - 5) Microsoft Terminal Services Web Access,
  - 6) Microsoft Remote Web Access,
  - 7) Active Directory Federation Services.
6. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników podczas logowania do co najmniej:
  - 1) klienta VPN,
  - 2) systemu macOS
  - 3) systemu Linux,
  - 4) połączenia SSH.
7. Rozwiązanie musi oferować dedykowaną bezpłatną aplikację mobilną pochodzącą od tego samego producenta rozwiązania 2FA/MFA.
  - 1) Aplikacja mobilna musi wspierać następujące systemy:
    - a) Android,
    - b) iOS.
  - 2) Aplikacja mobilna musi umożliwiać uwierzytelnienie użytkownika przy pomocy co najmniej:
    - a) Generowanego kodu OTP w tym co najmniej:

- a.1) HOTP,
  - a.2) TOTP.
- b) Powiadomienia PUSH.
- 3) Aplikacja mobilna musi posiadać możliwość zabezpieczenia jej przy pomocy kodu PIN oraz danych biometrycznych.
- 4) Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP musi odbywać się w trybie offline.
- 5) Aplikacja musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.
- 8. Rozwiązanie musi oferować alternatywne możliwości uwierzytelnienia użytkownika w tym co najmniej:
  - 1) OTP dostarczonego przy pomocy wiadomości SMS,
  - 2) OTP dostarczonego przy pomocy wiadomości e-mail,
  - 3) tokenu sprzętowego,
  - 4) FIDO,
  - 5) klucza odzyskiwania (MRK).

## **X. Część nr 8**

### **3.1 Podwójna autentykacja w logowaniu do głównych systemów szpitala w których przechowywane są dane osobowe oraz dane medyczne**

Wymagania funkcjonalne

Opis wszystkich funkcjonalności oraz zależności w ramach modułu, w podziale:

#### **1. Wymagania funkcjonalne**

- 1) System musi umożliwiać bezpieczne logowanie do systemu HIS przy użyciu autentykacji dwuskładnikowej (2FA) z wykorzystaniem urządzeń klasy smartfon/tablet z zainstalowaną aplikacją potwierdzającą (Microsoft Authenticator albo Google Authenticator).
- 2) System musi umożliwiać powiązanie konta użytkownika w HIS z instalacją wybranej aplikacji potwierdzającej, za pomocą zeskanowania QR-kodu generowanego w systemie.
- 3) System musi umożliwiać administratorowi regulowanie czasu ważności poświadczeń na danym urządzeniu, na którym użytkownik będzie się logował.
- 4) System musi umożliwiać autentykację użytkownika za pomocą zastępczych metod potwierdzenia kodu autentykacji dwuskładnikowej (wysłanie kodu na email i/lub SMS).

#### **2. Wewnętrzne integracje:**

- 1) Funkcjonalność stanowi integralną część usług systemowych HIS.
- 2) Funkcjonalność ze względów bezpieczeństwa nie integruje się z zewnętrznymi dostawcami usług autentykacyjnych.

Podwójna autentykacja w logowaniu do głównych systemów szpitala w których przechowywane są dane osobowe oraz dane medyczne- wdrożenie.

#### **2.1 Wymagania do uruchomienia produktu**

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

- Warunki startowe (minimalna wersja HIS)
  - Licencja
- Wymagania techniczne:
  - Uruchomiony system HIS
  - Aplikacja typu authenticator (np. Google, Microsoft lub inne kompatybilne) na urządzeniu użytkownika (smartphone)

#### **2.2 Opis wdrożenia**

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

- Elementy do uruchomienia:
  - HIS
- Parametryzacja środowiska:
  - Wgranie licencji
  - Ustawienie parametrów administracyjnych związanych z autentykacją
  - Reguły dostępu i uprawnienia użytkowników.

#### **1 Kryteria odbioru produktu**



Produkt zostanie uznany za zgodny funkcjonalnie, jeśli:

- Umożliwi administratorom taką konfigurację, która wymusi na wybranych użytkownikach lub grupach użytkowników skonfigurowanie aplikacji authenticator poprzez zeskanowanie kodu QR z ekranu monitora z HIS.
- Umożliwi administratorom taką konfigurację, która pozwala regulować czas ważności poświadczeń na danym urządzeniu (przeglądarka z HIS).
- Umożliwi użytkownikom autentykację za pomocą zastępczych metod (wysłanie kodu na email i/lub SMS).