Załącznik nr 4 – Zakres realizacji przedsięwzięcia do wyboru przedsięwzięcia

(tryb konkurencyjny – I nabór – Inwestycja D.1.1.2)

SPIS TREŚCI

1. INTEGRACJA I ROZBUDOWA SYSTEMÓW INFORMATYCZNYCH ŚWIADCZENIODAWCY

W ramach 1 zakresu możliwe będzie uzyskanie wsparcia finansowego służącego spełnieniu obowiązku prowadzenia i wymiany elektronicznej dokumentacji medycznej, o której mowa w treści art. 2 pkt 6 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2023 r. poz. 2465 z późn.zm.) zarówno obowiązującej, jak i planowanej do wdrożenia przez Centrum e-Zdrowia.

W ramach naboru niekonkurencyjnego Centrum e-Zdrowia planuje rozszerzanie katalogu EDM o 9 nowych wzorów dokumentów do końca I kwartału 2026:

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)

Obszary możliwe do sfinansowania w ramach 1 zakresu:

a. Zakup lub rozbudowa lub integracja systemów szpitalnych;
b. Zakup lub rozbudowa lub integracja systemów dziedzinowych i peryferyjnych świadczeniodawcy np. LIS, RIS, PACKS, CIS, EHR z HIS;
c. Zakup lub rozbudowa systemów zbierania danych z urządzeń medycznych i ich integracja z systemem szpitalnym;
d. Integracja systemów szpitalnych z P1;
e. Zakup lub rozbudowa repozytoriów medycznych, w tym zakup usługi serwisowej w chmurze;
f. Budowa lub rozbudowa sieci lub hurtowni danych, z wyłączeniem prac budowlanych;
g. Zakup sprzętu ICT służącego informatyzacji lub cyfryzacji szpitali, w szczególności: serwerów, macierzy, przełączników sieciowych, stacji roboczych, urządzeń mobilnych, czytników e-dowodów, narzędzi do zbierania podpisów
h. Szkolenia pracowników z obsługi wdrażanych w ramach przedsięwzięcia systemów szpitalnych.

Zakres przedsięwzięcia obejmuje również 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.

<u>Informacje techniczne dotyczące 9 nowych wzorów EDM</u>

W przypadku standardu uwierzytelnienia użytkowników oraz systemów będą stosowane dwie metody:
1) oparte na standardzie OAuth 2.0 i metodzie zgodnej z “Client Credentials Grant” (analogicznie jak w przypadku obsługi zdarzeń medycznych);
2) bazującej na certyfikatach TLS i WSS wydanych z centrum certyfikacji P1.

Uwierzytelnienie Systemu wykonawcy wywołującego usługę systemu P1 będzie następowało w warstwie transportowej połączenia za pomocą protokołu TLS z obustronnym uwierzytelnieniem – oprócz uwierzytelnienia serwera przez system wykonawcy następuje uwierzytelnienie klienta (Systemu wykonawcy) przez serwer. Do nawiązania połączenia TLS system wykonawcy zobowiązany będzie użyć certyfikatu do uwierzytelnienia systemu wydanego przez Centrum Certyfikacji P1 (użycie przez klienta P1 klucza prywatnego powiązanego z certyfikatem do uwierzytelnienia systemu przekazanego przez Centrum e-Zdrowia). Użycie tego certyfikatu będzie niezbędne również do pobrania dodatkowych informacji o wykorzystaniu usług P1, w tym przykładów komunikatów.

Do poprawnego wykonania usługi wymagane będzie uwierzytelnienie pochodzenia komunikatu. System wykonawcy będzie zobowiązany do podpisania komunikatu SOAP z użyciem certyfikatu do uwierzytelnienia danych służącego do weryfikacji złożonego podpisu cyfrowego. Po poprawnej weryfikacji podpisu cyfrowego na podstawie certyfikatu do uwierzytelnienia danych identyfikowany i uwierzytelniany będzie System wykonawcy, w kontekście którego realizowana będzie usługa.

Bezpośrednio po uwierzytelnieniu będzie następowała autoryzacja, na którą składa się autoryzacja wykonania usługi oraz autoryzacja dostępu do danych. Autoryzacja wykonania usługi polega na sprawdzeniu przydzielenia do konta systemu wykonawcy (w P1) uprawnienia związanego z wywoływaną usługą. Autoryzacja dostępu do danych wykonywana jest w określonych przypadkach i weryfikuje możliwość dostępu do danych na podstawie parametrów wywołania usługi. System wykonawcy będzie uwierzytelniał użytkowników końcowych, a następnie przekazywał żądania do systemu P1, a tam gdzie jest to wymagane deklarował informacje o użytkowniku końcowym.

W komunikacji z systemem P1 wymagane jest użycie rozszerzenia Web Services Security i profilu Web Services Security X.509 Certificate Token Profile.

Poszczególne dokumenty różnić się mogą między sobą zastosowanym standardem komunikacji oraz danych, co wynikać będzie z charakteru ich zastosowania oraz oczekiwań dotyczących miejsca przechowywania informacji. W przypadku kart ratownictwa medycznego przewiduje się zastosowanie standardu HL7 CDA dla dokumentów, przechowywania w repozytorium podmiotu leczniczego oraz przekazania indeksu EDM do systemu e-zdrowie (P1). Dla karty e-DILO oraz planu leczenia onkologicznego zastosowany zostanie standard HL7 FHIR, w przypadku którego zasoby będą przekazywane usługami REST.

Karta opieki kardiologicznej będzie zgodna ze standardem HL7. Dokumenty związane z wynikami badań histopatologicznymi, cytologicznymi, medycyną pracy oraz Patient Summary będą dokumentami w standardzie HL7 CDA, a komunikacja będzie odbywała się wg interfejsów SOAP.

Dokument	Specyfikacja
Karta diagnostyki i leczenia onkologicznego (e-DILO)	2025-04-30
Plan leczenia onkologicznego	2025-04-30
Wyniki i opisy badań histopatologicznych	Udostępniona
Wyniki i opisy badań cytologicznych	Udostępniona
Patient Summary (Karta zdrowia pacjenta)	2025-05-31
Karta opieki kardiologicznej (e-KOK)	2025-07-31
Karta medycznych czynności ratunkowych	Udostępniona
Karta medyczna lotniczego zespołu ratownictwa medycznego	2025-04-11
Dokumenty medycyny pracy (dokument orzeczenia i dokument zaleceń)	2025-09-30

Wymagania techniczne dotyczące interoperacyjności teleinformatycznych systemów szpitalnych

Szpitale przy zakupie lub rozbudowie teleinformatycznych systemów szpitalnych powinny wymagać od dostawcy:

1. Interoperacyjności systemów teleinformatycznych, w ramach oferowanej ceny, zgodnie z:
   a) ustawą z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024 r. poz. 1557 z późn. zm.);
   b) Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 773);
   c) ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2023 r. poz. 2465 z późn.zm.);
   d) minimalnymi wymaganiami dla systemów określonych w treści art. 8a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. j.w.);

2. Zapewnienia możliwości eksportu i importu danych, w szczególności poprzez udostępnienie otwartych interfejsów oraz dokumentacji pozwalającej na przeprowadzenie procesu eksportu i importu danych, w tym specyfikację danych, które są przedmiotem wymiany, zgodnie z zapotrzebowaniem danego szpitala.

Wskaźnik D21G.R1:

Integracja systemów szpitalnych z systemem P1

- jednostka miary: liczba; wartość docelowa: 1

Sposób pomiaru: monitorowanie zwiększenia poziomu zaindeksowanej EDM w zakresie wyników badań laboratoryjnych lub opisów badań diagnostycznych w P1 w trakcie trwania realizacji przedsięwzięcia celem wykazania wzrostu procentowego lub liczbowego

Mechanizm weryfikacji: dokument wystawiony przez CeZ potwierdzający zaindeksowanie co najmniej 1 EDM w zakresie badań laboratoryjnych lub opisów badań diagnostycznych od dnia następującego po dniu ogłoszenia naboru.

2. DIGITALIZACJA DOKUMENTACJI MEDYCZNEJ ISTOTNEJ Z PUNKTU WIDZENIA LECZENIA I PROFILAKTYKI

W ramach 2 zakresu możliwe będzie uzyskanie wsparcie finansowe na:

a. wdrożenie rozwiązań umożliwiających zasilenie systemu P1 danymi medycznymi zgromadzonymi w systemie szpitalnym w zakresie digitalizacji karty informacyjnej z leczenia szpitalnego od 2023r.;
b. digitalizację papierowej dokumentacji medycznej przechowywanej w podmiocie obejmującej kartę informacyjną z leczenia szpitalnego od 2023 r., o której mowa w przepisach wydanych na podstawie art. 30 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2024r. poz.581) i przekazanie do centralnego repozytorium danych medycznych dla zdigitalizowanej dokumentacji medycznej,

- oraz utrzymanie ww. działań w okresie trwałości przedsięwzięcia.

W ramach przedsięwzięcia będzie możliwie sfinansowanie następujących czynności lub usług:

- koszt zakupu sprzętu służącego digitalizacji dokumentacji papierowej obejmującej co najmniej kartę informacyjną z leczenia szpitalnego od 2023 r.;
- koszt zakupu lub modyfikacji lub integracji systemów informatycznych szpitala, służących indeksacji EDM w systemie P1, w zakresie co najmniej karty informacyjnej z leczenia szpitalnego od 2023 r.

Informacje techniczne w zakresie digitalizacji dokumentacji papierowej

Dla dokumentacji w postaci papierowej można zakupić sprzęt umożliwiający co najmniej przeprowadzenie odwzorowania cyfrowego dokumentu oraz osadzenie w dokumencie XML (zgodnie ze standardem HL7 CDA), min. 300-600dpi (uzależnione od stanu dokumentacji w postaci papierowej), zapewniający obsługę plików wyjściowych PDF oraz, w zależności od opcji odwzorowania również kolorów, tryb skanowania i 24-bit kodowanie koloru.

Mając na uwadze, że digitalizacja dokumentacji papierowej prowadzona będzie z wykorzystaniem oprogramowania udostępnionego przez Centrum e-Zdrowia, **szczegółowe specyfikacje w zakresie digitalizacji karty informacyjnej z leczenia szpitalnego zostaną przekazane do 31.05.2025 r.**

Wskaźnik D18G.R1:

Karty informacyjne z leczenia szpitalnego w postaci elektronicznej dokumentacji medycznej od 1 stycznia 2023 r. do 31 grudnia 2025 r. zaindeksowane w systemie P1 lub umieszczone w centralnym repozytorium danych medycznych w Centrum e-Zdrowia

– jednostka miary: %, wartość docelowa: 95%;

Sposób pomiaru: monitorowanie zwiększenia poziomu zaindeksowanej EDM w zakresie kart informacyjnych z leczenia szpitalnego

Mechanizm weryfikacji; dokument wystawiony przez szpital potwierdzający, że 95% kart informacyjnych z leczenia szpitalnego za lata 2023-2025. zostało zaindeksowanych w systemie P1 lub umieszczonych w centralnym repozytorium Centrum e-Zdrowia dla zdigitalizowanej papierowej dokumentacji medycznej

3. DZIAŁANIA ZWIĘKSZAJĄCE POZIOM CYBERBEZPIECZEŃSTWA SZPITALA

W ramach 3 zakresu możliwe będzie uzyskanie wsparcia finansowego na działania zwiększające poziomu cyberbezpieczeństwa szpitali, co ma służyć bezpiecznemu przetwarzaniu elektronicznej dokumentacji medycznej.

W ramach przedsięwzięcia będzie możliwie sfinansowanie następujących kategorii kosztów (urządzenia, licencje, usługi) w zakresie:

a. systemu kopii zapasowych;
b. zapór sieciowych;
c. ochrony poczty e-mail;
d. segmentacji sieci;
e. ochrony stacji roboczych oraz serwerów (rozwiązania klasy EDR);
f. system zarządzania podatnościami;
g. system zarządzania bezpieczeństwem informacji;
h. szkolenia dla kadry kierowniczej oraz personelu medycznego i administracyjnego;
i. usługi zarządzane bezpieczeństwa;
j. uwierzytelnienie i autoryzacja do systemów;
k. audytu

Zakres przedsięwzięcia obejmuje również aktualizację i rozbudowę urządzeń i systemów, przedłużenia posiadanych już licencji, subskrypcji oraz wsparcia dla posiadanych urządzeń lub systemów, zarówno on-premise jak i w chmurze, w okresie trwałości przedsięwzięcia.

KATEGORIE WYDATKÓW KWALIFIKOWALNYCH ORAZ WARUNKI AKCEPTACJI

ZAŁOŻENIA OGÓLNE:

- Podmiot na etapie składania wniosku o objęcie przedsięwzięcia wsparciem dokonuje samooceny poziomu dojrzałości cyberbezpieczeństwa w swojej organizacji; podstawą do samooceny może być audyt cyberbezpieczeństwa szpitala, który jest wydatkiem kwalifikowalnym, przy czym wykonanie audytu przedwdrożeniowego nie jest obligatoryjne (w przypadku wykonania audytu przedwdrożeniowego, musi on obejmować obszary z *Ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa*, a audytor musi spełnić wymagania określone w art. 15 ust. 2 pkt 2 lit. a-c ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 z późn. zm.).
- Samoocena poziomu dojrzałości cyberbezpieczeństwa wykonywana jest na bazie *Ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa*
  Na etapie samooceny, w przypadku niespełnionego w całości kryterium, podmiot może uznać go za niespełniony.
  Na bazie wypełnionej ankiety podmiot wskazuje obszary do doskonalenia (uzasadnienie realizacji zakresu zadania w obszarze cyberbezpieczeństwa), które wykazuje w treści sekcji D wniosku o objęcie przedsięwzięcia wsparciem; Wniosek musi zawierać co najmniej wszystkie kryteria, które zostały wskazane jako obligatoryjne w Ankiecie weryfikacji dojrzałości w zakresie cyberbezpieczeństwa (załącznik 3 do Wniosku o objęcie przedsięwzięcia wsparciem), jeżeli podmiot zaznaczył je jako niespełnione; Wniosek o objęcie przedsięwzięcia wsparciem w zakresie cyberbezpieczeństwa musi zawierać Ankietę weryfikacji dojrzałości w zakresie cyberbezpieczeństwa.
- Warunkiem rozliczenia zakresu DZIAŁANIA ZWIĘKSZAJĄCE POZIOM CYBERBEZPIECZEŃSTWA SZPITALA będzie przedstawienie wyników *Audytukońcowego w obszarze cyberbezpieczeństwa*; wynik audytu musi wskazywać na co najmniej dokonanie pozytywnej lub warunkowo pozytywnej oceny podmiotu w oparciu o kryteria wskazane w *Ankiecie weryfikacji dojrzałości w zakresie cyberbezpieczeństwa* jako obligatoryjne, jak również nieobligatoryjne, jeśli podmiot wskazał je we wniosku o objęcie przedsięwzięcie wsparciem. .

ZAKRES FINANSOWANIA WYDATKÓW

SYSTEM KOPII ZAPASOWYCH

LISTA WYDATKÓW KWALIFIKOWALNYCH:

Zakup sprzętu i oprogramowania

Zakup lub modernizacja oprogramowania lub urządzeń oferujących co najmniej:

- Tworzenie kopii zapasowych:
  - Automatyczne tworzenie kopii zapasowych zgodnie z ustalonym harmonogramem (np. codziennie, tygodniowo).
  - Obsługa pełnych, przyrostowych i różnicowych kopii zapasowych.
  - Możliwość tworzenia kopii zapasowych plików, baz danych, maszyn wirtualnych, aplikacji i systemów operacyjnych.
  - Backup do lokalnych serwerów, urządzeń NAS, taśm, chmury publicznej i prywatnej.
- Przywracanie danych:
  - Możliwość przywracania pojedynczych plików, folderów, maszyn wirtualnych, lub całych systemów.
  - Opcja natychmiastowego odzyskania danych na żądanie użytkownika.
  - Możliwość przywrócenia całego systemu na nowe lub istniejące urządzenie.
  - Funkcja weryfikacji poprawności kopii zapasowej bez wpływu na system produkcyjny.
- Zarządzanie i konfiguracja:
  - Interfejs umożliwiający zarządzanie kopiami zapasowymi w jednej lokalizacji.
  - Możliwość definiowania okresu przechowywania kopii zapasowych i automatycznego usuwania przestarzałych kopii.
  - Zachowywanie wielu wersji plików umożliwiających przywrócenie do konkretnego punktu w czasie.
  - Automatyczne informowanie o sukcesie lub błędach w tworzeniu kopii zapasowych.
- Bezpieczeństwo:
  - Szyfrowanie kopii zapasowych zarówno w trakcie przesyłania, jak i przechowywania.
  - Mechanizmy blokujące nieautoryzowaną modyfikację kopii zapasowych.
- Monitoring i raportowanie
  - Informacje o stanie kopii zapasowych oraz bieżących procesach.
  - Generowanie raportów dotyczących skuteczności backupu, ilości przechowywanych danych, czy historii przywracania.
- Skalowalność i wydajność
  - Minimalizacja rozmiaru kopii zapasowych bez utraty jakości danych.
- Integracja z innymi systemami
  - Obsługa integracji z systemami Security Information and Event Management lub logiem centralnym.
- Dodatkowe wymagania:
  - Urządzenie dostarczone jest z oficjalnej dystrybucji producenta przeznaczonej na teren Unii Europejskiej.

Zakup usług wdrożeniowych, szkoleniowych

Zakup usług utrzymaniowych oraz usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia

Zakup usług testów bezpieczeństwa

- W zakresie potwierdzenia skuteczności wprowadzonych zabezpieczeń i potwierdzenia zgodność konfiguracji z dokumentacją oraz braku występowania podatności

ZAPORY SIECIOWE

LISTA WYDATKÓW KWALIFIKOWALNYCH

Zakup sprzętu i oprogramowania dla zapór sieciowych nowej generacji

Zakup lub modernizacja urządzeń typu firewall o ile zapewniają co najmniej usługi:

- Funkcje podstawowe:
  - Filtracja pakietów sieciowych oparta na regułach i protokołach.
  - Obsługa stateless i stateful inspection ruchu sieciowego.
- Zarządzanie ruchem sieciowym:
  - Kontrola dostępu do aplikacji na podstawie tożsamości użytkownika i/lub urządzenia.
  - Identyfikacja i kontrola ruchu na poziomie aplikacji (L7).
  - Analiza i kontrola szyfrowanego ruchu.
- Bezpieczeństwo zaawansowane:
  - Wykrywanie i zapobieganie włamaniom (Intrusion Detection and Prevention System - IDS/IPS).
  - Integracja z systemami antywirusowymi i anti-malware w celu skanowania ruchu w czasie rzeczywistym.
  - Podstawowe wykrywanie i blokowanie ataków DDoS.
- Integracja z innymi systemami:
  - Obsługa integracji z systemami Security Information and Event Management lub logiem centralnym.
- Monitoring i raportowanie:
  - Możliwość śledzenia ruchu sieciowego w czasie rzeczywistym.
  - Generowanie szczegółowych raportów i logów dotyczących ruchu sieciowego, naruszeń bezpieczeństwa i konfiguracji.
  - Wsparcie dla alertów w czasie rzeczywistym z możliwością integracji z zewnętrznymi systemami notyfikacji.
- Zarządzanie i konfiguracja:
  - Interfejs użytkownika dostępny przez przeglądarkę internetową.
  - Możliwość definiowania polityk bezpieczeństwa dla określonych grup użytkowników lub aplikacji.
  - Wsparcie dla centralnego zarządzania regułami.
- Funkcje dodatkowe:
  - Blokowanie treści niepożądanych na podstawie kategorii URL.
  - Możliwość tworzenia reguł ograniczających przepustowość dla określonych aplikacji lub użytkowników.
  - Możliwość wykonywania kopii zapasowych konfiguracji urządzenia.

- Obsługa VPN (np. IPsec, SSL) dla organizacji zewnętrznych i pracowników zdalnych.

- Pozostałe wymagania:
  - Urządzenie dostarczone jest z oficjalnej dystrybucji producenta przeznaczonej na teren Unii Europejskiej.

Zakup sprzętu, oprogramowania, usług dla zapór sieciowych w warstwie aplikacji (WAF)

Zakup lub modernizacja urządzeń lub oprogramowania lub usług typu firewall aplikacyjny (WAF), o ile zapewniają co najmniej usługi:

- Ochronę przed typowymi atakami na aplikacje webowe, które zostały wykazane w OWASP TOP 10 2021 lub nowszej wersji.
- Ochronę przed atakami DoS/DDoS w warstwie aplikacji.
- Ochronę przed sztucznym ruchem wygenerowanym przez boty.
- Możliwość konfiguracji i zarządzania indywidualnymi politykami bezpieczeństwa dla poszczególnych aplikacji.
- Obsługę integracji z systemami Security Information and Event Management lub logiem centralnym.
- W zakresie urządzeń - urządzenie dostarczone jest z oficjalnej dystrybucji producenta przeznaczonej na teren Unii Europejskiej.

Zakup sprzętu, oprogramowania, usług dla rozwiązań klasy Sandbox

Zakup lub modernizacja urządzeń lub oprogramowania lub usług klasy Sandbox, o ile zapewniają co najmniej usługi:

- Integrację z planowaną w projekcie lub posiadaną zaporą sieciową.
- Integrację z planowanym w projekcie lub posiadanym rozwiązaniem do ochrony poczty.
- Uruchamianie próbek plików w kontrolowanym, odizolowanym środowisku.
- Analizę zachowania środowiska po uruchomieniu próbki pliku.
- Wsparcie do uruchamiania próbek w różnych konfiguracjach emulowanego środowiska.
- Wsparcie do uruchamiania próbek plików różnego formatu (np. pliki pdf, pliki pakietów biurowych, pliki wykonywalne, skrypt/makra, pliki z archiwami).
- Możliwość konfiguracji polityk w zależności od przyznanego scoringu próbki pliku.

Zakup usług wdrożeniowych, szkoleniowych

Zakup usług utrzymaniowych oraz usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia

Zakup usług testów bezpieczeństwa

- W zakresie potwierdzenia skuteczności wprowadzonych zabezpieczeń i potwierdzenia zgodność konfiguracji z dokumentacją oraz braku występowania podatności.

OCHRONA POCZTY E-MAIL

LISTA WYDATKÓW KWALIFIKOWALNYCH

Zakup sprzętu, usługi lub oprogramowania

Zakup lub modernizacja oprogramowania lub usługi lub urządzeń oferujących co najmniej:

- Filtracja wiadomości e-mail
  - Wykrywanie i filtrowanie wiadomości oznaczonych jako niechciane (spam).
  - Identyfikacja i blokowanie wiadomości zawierających podejrzane linki lub fałszywe treści.
  - Możliwość analizy i blokowania wiadomości zawierających określone słowa kluczowe lub treści niepożądane.
  - Analiza typów plików i blokowanie załączników potencjalnie szkodliwych.
- Ochrona przed złośliwym oprogramowaniem
  - Skanowanie załączników i treści wiadomości w czasie rzeczywistym w poszukiwaniu oprogramowania złośliwego.
  - Bezpieczne uruchamianie załączników w odizolowanym środowisku w celu wykrycia złośliwego oprogramowania.
- Bezpieczeństwo i integralność wiadomości
  - Obsługa szyfrowania wiadomości wychodzących i przychodzących.
  - Implementacja standardów SPF, DKIM i DMARC w celu ochrony przed fałszywymi nadawcami.
  - Ochrona przed utratą danych (DLP): Blokowanie wysyłki poufnych danych zgodnie z politykami bezpieczeństwa organizacji.
- Zarządzanie i konfiguracja
  - Centralne zarządzanie politykami bezpieczeństwa.
  - Możliwość definiowania reguł dotyczących odbierania, filtrowania i wysyłania wiadomości.
  - Obsługa systemów/usług Active Directory lub LDAP w celu stosowania indywidualnych polityk bezpieczeństwa.
- Raportowanie i monitoring
  - Informacje o przychodzących i wychodzących wiadomościach oraz zagrożeniach.
  - Generowanie szczegółowych raportów dotyczących wykrytych zagrożeń, statystyk spamu, czy skuteczności polityk.
  - Automatyczne powiadamianie administratora o wykryciu zagrożeń.
- Integracja z innymi systemami
  - Obsługa integracji z systemami Security Information and Event Management lub logiem centralnym.
- Funkcje dla użytkowników końcowych
  - Dostęp użytkowników do wiadomości zatrzymanych przez filtr.
  - Powiadomienia o zablokowanych wiadomościach: Automatyczne informowanie użytkowników o wiadomościach zatrzymanych przez system.
  - Użytkownicy mogą oznaczać wiadomości jako spam lub fałszywie pozytywne.
- Dodatkowe wymagania (jeżeli dotyczą):
  - Urządzenie dostarczone jest z oficjalnej dystrybucji producenta przeznaczonej na teren Unii Europejskiej.

Zakup usług wdrożeniowych, szkoleniowych

Zakup usług utrzymaniowych oraz usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia

Zakup usług testów bezpieczeństwa

- W zakresie potwierdzenia skuteczności wprowadzonych zabezpieczeń i potwierdzenia zgodności konfiguracji z dokumentacją oraz braku występowania podatności.

SEGMENTACJA SIECI

LISTA WYDATKÓW KWALIFIKOWALNYCH:

Zakup sprzętu i oprogramowania:

Zakup lub modernizacja urządzeń i/lub oprogramowania:

- Przełączniki wielowarstwowe (ang. multilayer switch) wraz z niezbędnymi licencjami oraz oprogramowaniem do zarządzania, oferujące co najmniej:
  - Funkcje zaawansowanego zarządzania dla warstw L2/L3.
  - Możliwość zarządzania urządzeniem przez centralne oprogramowanie.
  - Przepustowość nie mniejszą niż 1 Gbps na każdym porcie.
  - Obsługę standardu PoE.
  - Obsługa list kontroli dostępu (ACL).
  - Obsługę standardu autoryzacji użytkowników/urządzeń w oparciu o IEEE 802.1X.
  - Obsługę protokołu autoryzacji RADIUS i TACACS+.
- Oprogramowanie klasy NAC (Network Access Control), oferujące co najmniej:
  - Centralne monitorowanie i zarządzanie sieciami przewodowymi i bezprzewodowymi.
  - Wsparcie dla wielu producentów sprzętu sieciowego.
  - Wsparcie dla identyfikacji i klasyfikacji urządzeń podłączanych do sieci.
  - Obsługę przypisywania polityk dla grup urządzeń oraz użytkowników.
  - Obsługę standardu autoryzacji użytkowników/urządzeń w oparciu o IEEE 802.1X.
  - Obsługę protokołu autoryzacji RADIUS i TACACS+.
  - Obsługę integracji z systemami Security Information and Event Management lub logiem centralnym.
- Dodatkowe wymagania (jeżeli dotyczą):
  - Urządzenie dostarczone jest z oficjalnej dystrybucji producenta przeznaczonej na teren Unii Europejskiej.

Zakup usług wdrożeniowych, doradczych, szkoleniowych

Zakup usług utrzymaniowych oraz usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia

Zakup usług testów bezpieczeństwa

- w zakresie potwierdzenia skuteczności wprowadzonych zabezpieczeń i potwierdzenia zgodność konfiguracji z dokumentacją.

OCHRONA STACJI ROBOCZYCH ORAZ SERWERÓW (ROZWIĄZANIA KLASY EDR)

LISTA WYDATKÓW KWALIFIKOWALNYCH

Zakup oprogramowania:

Zakup lub modernizacja oprogramowania oferującego co najmniej:

- Ochronę przed złośliwym oprogramowaniem wykorzystującym techniki ataków plikowych i bezplikowych.
- Możliwość wykrywania i zapobiegania zagrożeniom przy użyciu analizy behawioralnej punktów końcowych, aplikacji i aktywności użytkowników końcowych.
- Zdalną konfigurację zabezpieczeń systemu operacyjnego, takich jak systemowa zapora sieciowa, dostęp do portów USB i SD, szyfrowanie dysków.
- Skanowanie podatności stacji roboczej i raportowanie w oparciu o inwentaryzację, konfigurację, zainstalowane poprawki i politykę urządzeń końcowych.
- Wykrywanie i reagowanie (EDR lub XDR), gromadzenie nieprzetworzonych danych telemetrycznych, dostosowywanie wykrywania, badanie po incydencie i zdalna izolacja zainfekowanej stacji roboczej.

Usługi związane z wdrożeniem oraz utrzymaniem systemu ochrony stacji roboczych oraz usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia

Szkolenia pracowników w zakresie administrowania systemem ochrony stacji roboczych.

SYSTEM ZARZĄDZANIA PODATNOŚCIAMI

LISTA WYDATKÓW KWALIFIKOWALNYCH

Zakup oprogramowania

Zakup lub modernizacja systemu zarządzania podatnościami o ile zapewnia co najmniej:

- Automatyzację skanowania:
  - Regularne i cykliczne skanowanie infrastruktury IT.
  - Możliwość uruchamiania skanów po istotnej zmianie w systemie (np. aktualizacja, wdrożenie nowej funkcji).
- Identyfikację podatności:
  - Wykrywanie podatności w systemach operacyjnych, aplikacjach, bazach danych, urządzeniach sieciowych.
  - Klasyfikacja podatności według poziomu ryzyka.
- Raportowanie wyników:
  - Generowanie szczegółowych raportów z identyfikowanymi podatnościami oraz zaleceniami naprawczymi.
  - Możliwość eksportu wyników do formatów CSV, PDF
- Integrację z innymi systemami:
  - Możliwość komunikacji z systemami zarządzania poprawkami w celu automatycznego tworzenia zgłoszeń.
- Monitorowanie i śledzenie trendów:
  - Śledzenie liczby i rodzaju podatności w czasie.
  - Wizualizacja wyników za pomocą wykresów i dashboardów.
- Bezpieczeństwo:
  - Dostęp do wyników skanów ograniczony rolami i uprawnieniami.
  - Szyfrowanie danych związanych ze skanowaniem.

Zakup usług wdrożeniowych, szkoleniowych

Zakup usług utrzymaniowych oraz usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia

WDROŻENIE LUB MODYFIKACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

LISTA WYDATKÓW KWALIFIKOWALNYCH

- Usługi związane z opracowaniem lub modyfikacją udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji. W ramach Systemu Zarządzania Bezpieczeństwem Informacji należy opracować, zatwierdzić i stosować polityki, procedury oraz standardy.
- Usługi związane z opracowaniem dokumentacji bezpieczeństwa, wraz z przekazaniem praw autorskich do dokumentacji, która jest wymagana i regulowana przepisami prawa w zakresie: Krajowego Systemu Cyberbezpieczeństwa, Ochrony Danych Osobowych.
- Szkolenia związane z wdrożeniem oraz stosowaniem udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji
- Usługi w zakresie certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji przez akredytowaną jednostkę certyfikującą.

SZKOLENIA Z ZAKRESU PODNOSZENIA ŚWIADOMOŚCI W OBSZARZE CYBERBEZPIECZEŃSTWA (CYBERHIGIENY)

LISTA WYDATKÓW KWALIFIKOWALNYCH

Szkolenia kadry kierowniczej, co najmniej z:

- Podstaw prawnych w obszarze cyberbezpieczeństwa.
- Typów ataków wraz z przykładami
- Reagowania na incydenty.
- Wykonywania testów bezpieczeństwa.
- Roli kadry zarządzającej w procesach bezpieczeństwa.

Szkolenia pracowników administracji i pracowników medycznych, co najmniej z:

- Podstawowych zasad cyberhigieny.
- Typów ataków wraz z przykładami
- Reagowania na incydenty
- Odpowiedzialności prawnej

Zakup usług szkoleniowych w okresie trwałości przedsięwzięcia

USŁUGI ZARZĄDZANE BEZPIECZEŃSTWA

LISTA WYDATKÓW KWALIFIKOWALNYCH

1) **Usługi Centrum Operacji Bezpieczeństwa (Security Operations Center):**

Usługi muszą być realizowane przez profesjonalne podmioty świadczące usługi z zakresu cyberbezpieczeństwa, spełniające warunki organizacyjne oraz techniczne opisane w Ustawie o Krajowym Systemie Cyberbezpieczeństwa oraz aktach wykonawczych.

- Usługa Pierwszej Linii Wsparcia minimum w zakresie:
    - Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie 24/7, zgodnie z uzgodnionymi warunkami SLA.
    - Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
    - Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.
    - Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji.
    - Eskalowanie zdarzenia w ramach ustalonego Scenariusza Reakcji.
    - Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
    - Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.
    - Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.
    - Modyfikacja polityk bezpieczeństwa systemów, aplikacji, rozwiązań podmiotu celem dostosowania ich do skuteczniejszego wykrywania zagrożeń (tuning systemów bezpieczeństwa).
    - Monitorowaniem muszą zostać objęte kluczowe:
        - Stacje robocze oraz serwery,
        - Urządzenia sieciowe, w tym urządzenia brzegowe,
        - Systemy / aplikacje serwerowe, w tym systemy informacji medycznej,
        - Kontrolery domenowe,
        - Środowiska chmurowe wraz z aplikacjami – o ile są wykorzystywane.
    - Zakres monitorowanych zdarzeń powinien uwzględniać minimum:
        - Powiadomienia o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowane z narzędzi ochrony,
        - Powiadomienia o dezaktywacji narzędzi bezpieczeństwa na danym hoście,
        - Powiadomienia z modułów ochrony / bezpieczeństwa urządzeń brzegowych oraz wewnętrznych urządzeń sieciowych,
        - Zdarzenia dotyczące nieudanych, wielokrotnych prób logowania dla wszystkich monitorowanych aktywów,
        - Kluczowe zdarzenia (np. utworzenie konta, zmiana hasła, usunięcie konta, zmiana grupy) związane z kontami uprzywilejowanymi dla wszystkich monitorowanych aktywów,
        - Zdarzenia sieciowe oraz systemowe (np. enumeracja, skanowanie portów i adresacji) mogące świadczyć o rekonesansie infrastruktury,
        - Zdarzenia związane z modyfikacją mechanizmów harmonogramu w systemach operacyjnych,
        - Zdarzenia związane z modyfikacją audytu zdarzeń / dzienników systemowych,
        - Zdarzenia dotyczące integralności plików, w szczególności zasobów sieciowych mogące świadczyć o zainfekowaniu oprogramowaniem złośliwym
        - Zdarzenia związane z logowaniem zdalnym.
- Usługa Drugiej Linia Wsparcia minimum w zakresie:
    - Analiza zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych
    - Realizacja Scenariuszy Reakcji zgodnie z wymaganiami.
    - Przygotowanie miesięcznych raportów z realizacji prac.
    - Oczekiwana dostępność usługi Drugiej Linii Wsparcia - 8 godzin dziennie, 5 dni w tygodniu
- Usługa przygotowania i wdrożenia Scenariuszy Reakcji dla zidentyfikowanych zagrożeń (playbooki).

- Usługa udostępnienia, administrowania i utrzymania systemu Security Incident and Event Management oraz integracja ze źródłami logów podmiotu, takimi jak Active Directory, Serwery Windows i Linux, DNS, system antywirusowy, WAF, Firewall, IPS / IDS, VPN, Routery i przełączniki.

2) <u>Usługi w zakresie testów bezpieczeństwa</u>

- Usługa testowania bezpieczeństwa obejmująca automatyczne skanowanie podatności testowanego środowiska, przeprowadzona zgodnie z założeniem że zespół testujący przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy. Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności.
- Usługa testowania bezpieczeństwa obejmująca manualne testy penetracyjne aplikacji webowej, wykonane zgodnie ze standardem ASVS 4.x, przeprowadzona zgodnie z założeniem że zespół testujący przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy. Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności.
- Usługa manualnego testowania bezpieczeństwa (testy penetracyjne) oraz poprawności konfiguracji kluczowej infrastruktury teleinformatycznej, w tym infrastruktury sieciowej, usług katalogowych, platformy wirtualizacyjnej, poczty e-mail itp. – o ile testy te zostały nieuwzględnione w innych grupach kwalifikacyjnych.

3) <u>Usługi w zakresie ubezpieczeń od ryzyk cybernetycznych</u>

- Usługi ubezpieczeniowe od najpowszechniejszych ryzyk i następstw związanych z cyberbezpieczeństwem

UWIERZYTELNIANIE I AUTORYZACJA DO SYSTEMÓW

LISTA WYDATKÓW KWALIFIKOWALNYCH

- Zakup sprzętowych kluczy bezpieczeństwa wspierających uwierzytelnianie zgodne przynajmniej ze standardem FIDO2 oraz Smart Card (PIV).
- Usługi wdrożenia i konfiguracji wieloskładnikowego uwierzytelniania i/lub uwierzytelniania bezhasłowego.
- Szkolenia pracowników w zakresie korzystania z wieloskładnikowego uwierzytelniania lub uwierzytelniania bezhasłowego oraz administrowania systemem.
- Zakup lub modernizacja oprogramowania lub usługi oferujących co najmniej:
    - Wsparcie dla wieloskładnikowego uwierzytelniania oraz uwierzytelniania bezhasłowego do stacji roboczych oraz sesji pulpitu zdalnego.
    - Wsparcie dla systemu pojedynczego logowania (SSO).
    - Wsparcie dla uwierzytelniania za pomocą sprzętowych kluczy bezpieczeństwa.
    - Wsparcie dla wieloskładnikowego uwierzytelniania sesji zdalnych VPN.

  - Wsparcie dla uwierzytelniania adaptacyjnego w oparciu o kontekst użytkownika oraz urządzenie.
  - Integracje z repozytoriami/katalogami tożsamości oraz usługami federacyjnymi.
  - Wsparcie dla budowy indywidualnych lub grupowych polityk dostępu.
- Zakup lub modernizacja oprogramowania lub usługi rozwiązań klasy PAM/PIM oferujących co najmniej:
  - Zarządzanie kontami uprzywilejowanymi.
  - Sejf haseł.
  - Monitorowanie i nagrywanie sesji uprzywilejowanych.
- Usług wsparcia posiadanych rozwiązań w okresie trwałości przedsięwzięcia.

AUDYT KOŃCOWY W OBSZARZE CYBERBEZPIECZEŃSTWA

Audyt powinien obejmować przynajmniej obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi). Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

- Kanały komunikacji jak np. poczta
- Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
- Kontrolery domeny
- Platforma wirtualizacyjna
- System zarządzania kopiami zapasowymi
- Poprawność konfiguracji stacji roboczych oraz serwerów
- Sposoby uwierzytelniania się użytkowników

Zespół audytujący: co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu lub co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka oceniająca zgodność, akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych.

ANKIETA WERYFIKACJI DOJRZAŁOŚCI POD KĄTEM CYBERBEZPIECZEŃSTWA

1) System kopii zapasowych

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożony system tworzy odmiejscowione kopie zapasowe. System posiada aktualne wsparcie producenta oraz wykonuje kopie kluczowych systemów podmiotu.		**Tak**
2.	Infrastruktura systemu backupu jest odseparowana od systemu produkcyjnego		**Tak**
3.	Przeprowadzono testy odtworzenia systemu i potwierdzono skuteczność/poprawność odtworzenia		**Tak**
4.	Podmiot posiada dokumentację powdrożeniową systemu backupu.		**Tak**

5.	Administratorzy systemu backupu podmiotu odbyli instruktaż z obsługi systemu kopii zapasowych.		**Tak**
6.	Wdrożono procedury backupowe oraz odtworzeniowe i procedury te są stosowane.		**Nie**
7.	Tworzone są i weryfikowane raporty z cyklicznego wykonywania odmiejscowionej kopii zapasowej.		**Nie**
8.	Podmiot cyklicznie odtwarza dane z kopii zapasowych w celu weryfikacji poprawności. Odtworzenia testowe potwierdzone są protokołem.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Zestawienie wszystkich kluczowych i pomocniczych systemów objętych systemem kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Dokument zawierający wymagania dotyczące częstotliwości wykonywania kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Kompletna dokumentacja wdrożonego rozwiązania systemu kopii zapasowych w szczególności zestaw procedur wykonywania, odtworzenia (w tym cyklicznych testów), zabezpieczenia odmiejscowionej kopii, monitoringu i weryfikacji poprawności działania systemu, zarządzania uprawnieniami i dostępem do systemu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Raport z testów funkcjonalnych i niefunkcjonalnych działania systemu backupu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu kopii zapasowej – w zakresie usług szkoleniowych.
- Wyniki testu potwierdzającego skuteczności wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych

2) Zapory sieciowe

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono moduł ochrony przed złośliwym oprogramowaniem dla ruchu z/do Internetu, posiadający aktualne wsparcie.		**Tak**
2.	Wdrożono i włączono moduł IPS/IDS przynajmniej dla ruchu z/do Internetu, posiadający aktualne wsparcie.		**Tak**
3.	Wdrożono i włączono moduły filtrowania zawartości oraz reguły filtrowania po kategorii treści.		**Tak**
4	Na brzegu sieci zainstalowany Firewall, a sama sieć podzielona jest na podsieci.		**Tak**
5.	Kluczowe aplikacje/systemy, w szczególności dostępne publicznie chronione są za pomocą firewalla aplikacyjnego (WAF) z włączonymi modułami ochrony aplikacji, ochrony DoS/DDoS.		**Nie**
6.	Pliki pobierane z sieci Internet podlegają analizie w izolowanych środowiskach typu Sandbox.		**Nie**
7.	Domyślne hasła przekazane przy odbiorze zostały zmienione i objęte procedurą zarządzania hasłami w organizacji.		**Tak**
8.	Nieużywane porty, usługi oraz konta zostały wyłączone.		**Tak**
9.	Dostęp do panelu zarządzania zaporą sieciowy został ograniczony jedynie dla wyznaczonych osób zgodnie z obowiązującą procedurą nadawania uprawnień oraz dostępny jest wyłącznie z wybranej podsieci.		**Tak**

10.	Wdrożona została procedura cyklicznego wykonywania kopii zapasowych konfiguracji urządzenia (lub po każdej zmianie reguł i wersji) .Procedura ta jest stosowana.		**Tak**
11.	Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego i/lub odbytych szkoleń z obsługi dedykowanego systemu Firewall.		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonych zapór sieciowych wraz z zabezpieczeniami – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych zapór sieciowych – dla usług szkoleniowych.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.

3) Ochrona poczty e-mail

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono mechanizmy ochrony poczty SPF, DMARC, DKIM.		**Tak**
2.	Wdrożono ochronę antyspam oraz ochronę przed złośliwym oprogramowaniem, z aktualnym wsparciem producenta i aktualnymi sygnaturami.		**Tak**
3.	Przeprowadzono testy wdrożonych mechanizmów ochrony poczty, które potwierdziły poprawne ich działanie.		**Tak**
4.	Wdrożono obowiązkowy drugi składnik uwierzytelniający (2FA) dla poczty dostępnej z sieci publicznej.		**Tak**
5.	Uwierzytelnianie do poczty dostępnej publicznie jest zgodne ze standardem FIDO2.		**Nie**
6.	Wdrożono zasady bezpiecznego wykorzystania poczty w organizacji.		**Nie**
7.	Wiadomości przychodzące z zewnątrz oznaczane są dedykowanym banerem.		**Nie**
8.	Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego z obsługi dedykowanego systemu lub usługi.		**Tak**
9.	Kopia bezpieczeństwa poczty jest regularnie wykonywana.		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Opis sposobu ochrony poczty wraz z dokumentacją systemów ochrony poczty
- Protokół z testów, który opisuje wyniki testów wdrożonych polityk ochrony poczty w tym weryfikację mechanizmów (SPF, DMARC, DKIM) ochrony poczty elektronicznej przy pomocy portalu CERT Polska https://bezpiecznapoczta.cert.pl/
- Wynik testu potwierdzającego wdrożenie obowiązkowego drugiego składnika uwierzytelniającego (2FA) dla poczty elektronicznej dostępnej publicznie.
- Raport z wykonania backupu poczty elektronicznej wraz testowym odtworzeniem.
- Raport zawierający informacje o aktualizacji systemu pocztowego wraz z jego ochroną

4) Segmentacja sieci

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono segmentację sieciową (na poziomie VLANów) zapewniającą odseparowanie sieci biurowej, systemów serwerowych, systemu kopii zapasowych, urządzeń medycznych, sieci gościnnej.		**Tak**
2.	Wdrożono reguły bezpieczeństwa pomiędzy segmentami sieci oparte na zasadzie minimalnego niezbędnego dostępu.		**Tak**
3.	Dokumentacja architektury sieciowej jest sporządzona i aktualizowana.		**Nie**
4.	Wszystkie podłączane do sieci urządzenia są identyfikowane, uwierzytelniane oraz autoryzowane.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokument zawierający wymagania dotyczące podziału sieci wraz ze sposobem implementacji – dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
- Dokumentacja sposobu identyfikowania, uwierzytelniania i autoryzacji urządzeń podłączanych do sieci – dla zakupu oprogramowania.
- Wynik weryfikacji zgodności konfiguracji z dokumentacją– dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych systemów ochrony sieciowej – dla usług szkoleniowych
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.
- Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.

5) Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono rozwiązanie ochrony przed złośliwym oprogramowaniem z aktualnym wsparciem producenta.		**Tak**
2.	Wdrożono rozwiązanie klasy EDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze oraz serwery.		**Tak**
3.	Wdrożono rozwiązanie klasy XDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze i serwery oraz zbierające i analizujące dane również z innych źródeł.		**Nie**
4.	Dla serwerów oraz stacji roboczych nieobjętych ochroną została wykonana analiza ryzyka.		**Tak**

5.	Osoby administrujące systemami ochrony stacji i serwerów posiadają odpowiednie kompetencje potwierdzone odbytym szkoleniem.		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonego rozwiązania, potwierdzająca zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych oraz serwerach – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu – dla usług szkoleniowych.

6) Zarządzanie podatnościami

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono system automatycznego (sieciowego i/lub agentowego) skanowania i identyfikacji podatności.		**Nie**
2.	Skanowanie podatności obejmuje przynajmniej kluczowe stacje robocze, serwery oraz urządzenia sieciowe.		**Nie**
3.	Skanowanie podatności obejmuje proces uwierzytelnienia się do poziomu systemu operacyjnego skanowanego hostu.		**Nie**
4.	Skanowanie podatności obejmuje ocenę poprawności konfiguracji bezpieczeństwa skanowanego hostu.		**Nie**
5.	Ocena ryzyka podatności uwzględnia inne czynniki niż system klasyfikacji CVSS.		**Nie**
6.	Ustalono czasy reakcji na zidentyfikowane podatności.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonego i uruchomionego systemu, wskazująca na obszary objęte skanowaniem podatności – dla zakupu oprogramowania lub zakupu wsparcia oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.

7) System zarządzania bezpieczeństwem informacji

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono politykę zarządzania dostępem i uprawnieniami.		**Tak**
2.	Wdrożono politykę kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania.		**Tak**
3.	Wdrożono politykę zarządzania podatnościami		**Tak**
4.	Wdrożono politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa		**Tak**
5.	Wdrożono politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny.		**Tak**
6.	Wdrożono politykę kopii bezpieczeństwa.		**Tak**
7.	Wdrożono politykę zarządzania incydentami bezpieczeństwa.		**Tak**
8.	Wdrożono politykę zarządzania ciągłością działania.		**Tak**

9.	Wdrożono politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Oświadczenie osoby uprawnionej do reprezentacji podmiotu, że kierownictwo ustanowiło lub zmodyfikowało System Zarządzania Bezpieczeństwem Informacji, oraz że zostały alokowane zasoby ludzkie i finansowe, niezbędne do jej realizacji, monitorowania i okresowych przeglądów.
- Lista opracowanej dokumentacji wraz z opisem
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych

8) Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Odbycie szkolenia przez kadrę kierowniczą, w okresie ostatniego roku, minimum w zakresie: • Podstaw prawnych w obszarze cyberbezpieczeństwa • Typów ataków • Reagowania na incydenty • Wykonywania badań bezpieczeństwa • Roli kadry zarządzającej w procesach bezpieczeństwa		**Tak**
2.	Odbycie szkolenia przez kadrę biurową i medyczną – min. 75% pracowników pracujących na systemach informatycznych szpitala, w okresie ostatniego roku, minimum w zakresie: • Podstawowych zasad cyberhigieny • Typów ataków wraz z przykładami • Reagowania na incydenty		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Konspekt programu szkoleń
- Potwierdzenie uczestnictwa w szkoleniach co najmniej 75% pracowników szpitala, pracujących na stacjach roboczych – oświadczenie dyrektora szpitala

9) Usługi zarządzane bezpieczeństwa

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Systemy teleinformatyczne jak i infrastruktura teleinformatyczna monitorowana jest całodobowa pod kątem bezpieczeństwa		**Nie**
2.	Przygotowano i przetestowano indywidualne procedury reagowania na incydenty bezpieczeństwa dla najbardziej powszechnych i najczęściej pojawiających się zdarzeń		**Nie**
3.	Utrzymywany jest centralny system klasy SIEM lub system centralnej kolekcji zdarzeń/logów gromadzący istotne z punktu widzenia zdarzenia bezpieczeństwa z infrastruktury teleinformatycznej oraz aplikacji i systemów		**Nie**
4.	Kluczowe aplikacje, systemy oraz infrastruktura teleinformatyczna testowana jest pod kątem bezpieczeństwa		**Nie**

5.	Ubezpieczenie od ryzyk cybernetycznych stosowane jest jako element uzupełniający zarządzania ryzykiem.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Umowa o świadczenie usług Centrum Operacji Bezpieczeństwa – w zakresie usług SOC.
- Wykaz przygotowanych Scenariuszy Reakcji dla zidentyfikowanych zagrożeń – w zakresie usługi przygotowania i wdrożenia scenariuszy.
- Umowa o świadczenie usług udostępniania i zarządzania systemem SIEM – w zakresie tego systemu.
- Umowa o świadczenie usług testów bezpieczeństwa – w zakresie usług testów.

10) Uwierzytelnienie i autoryzacja do systemów

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wszystkie krytyczne systemy w organizacji wymagają użycia drugiego składnika uwierzytelniania lub uwierzytelniania bezhasłowego.		**Nie**
2.	Każda osoba w organizacji ma obowiązek korzystania z drugiego składnika uwierzytelniania lub uwierzytelniania bezhasłowego (jeżeli jest dostępny).		**Nie**
3.	W przypadku wykorzystywania systemu pojedynczego logowania dla dostępu do systemów i aplikacji, uwierzytelnienie użytkownika odbywa się z wykorzystaniem metod wieloskładnikowych lub uwierzytelniania bezhasłowego.		**Nie**
4.	Wyłączono możliwość używania SMS-ów jako metody uwierzytelniania.		**Nie**
5.	Uwierzytelnianie do krytycznych systemów i aplikacji w organizacji jest zgodne ze standardem FIDO2.		**Nie**
6.	Wszystkie połączenia zdalne wymagają wieloskładnikowego uwierzytelniania.		**Nie**
7.	Uwierzytelnianie użytkownika uwzględnia jego kontekst np. urządzenie z którego następuje logowanie.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonych rozwiązań uwierzytelniających wraz z zabezpieczeniami – dla zakupu urządzeń i oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych.

Wskaźnik D21G.R2:

Zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej potwierdzone audytem bezpieczeństwa

– jednostka miary: liczba, wartość docelowa: 1

Sposób pomiaru: monitorowanie wzrostu poziomu cyberbezpieczeństwa w stosunku do *Ankiety weryfikacji dojrzałości pod kątem cyberbezpieczeństwa*

Mechanizm weryfikacji: wykonanie audytu bezpieczeństwa zgodnie z wymaganiami określonymi w kryteriach akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa

4. WDROŻENIE ROZWIĄZAŃ AI I PODŁĄCZENIE DO CENTRALNEGO REPOZYTORIUM DANYCH MEDYCZNYCH

W ramach 4 zakresu możliwe będzie uzyskanie wsparcia finansowego na działania służące rozwoju usług AI, służących wsparciu diagnostyki pacjenta, a także optymalizujących świadczenie usług dla pacjentów w szpitalu.

W ramach przedsięwzięcia będzie możliwie sfinansowanie następujących czynności lub usług:

a. integracja i wymiana danych z opracowaną przez Centrum e-Zdrowia platformą usług inteligentnych (PUI) w zakresie AI, wspomagających proces podejmowania decyzji diagnostyczno - leczniczych przez lekarza **(warunek konieczny realizacji zakresu nr 4);**

b. zakup innych narzędzi lub systemów wykorzystujących algorytmy AI , służących optymalizacji procesów szpitalnych oraz organizacji pracy personelu medycznego lub niemedycznego, niebędących wyrobem medycznym klasy IIa lub wyższym

c. budowa lub rozbudowa lub zwiększenie przepustowości sieci LAN lub WLAN, z wyjątkiem prac budowlanych, a także zakup i utrzymanie alternatywnej łączności internetowej poprzez łącza satelitarne.

Finansowanie może objąć usługi utrzymaniowe w okresie trwałości przedsięwzięcia.

Opis platformy PUI

Platforma będzie umożliwiała podmiotom medycznym przekazywanie, czasowe przechowywanie oraz przetwarzanie dokumentów obrazowych za pomocą oferowanych usług.

Podmioty będą mogły skorzystać z usług diagnostyki cyfrowej w celu ustalenia priorytetów obsługi pacjenta oraz wzbogacenia procesu diagnostycznego o wyniki działania usługi AI.

Katalog może obejmować rozwiązania dedykowane poszczególnym częściom ciała, szczególnie w obrębie: głowy, klatki piersiowej oraz układu kostnego.

Wymagania techniczne w zakresie PUI

Centrum e-Zdrowia, w zakresie wymiany danych między podmiotami medycznymi a Platformą Usług Inteligentnych, zamierza posługiwać się standardami zapewniającymi interoperacyjność, między innymi:

HL7 CDA – bazuje na zdefiniowanym i kompletnym obiekcie informacyjnym, który może zawierać dane tekstowe, obrazy, dźwięki oraz inną zawartość multimedialną,

HL7 FHIR - powszechny standard umożliwiający interoperacyjną wymianę jednostkowych danych medycznych,

IHE XDS - standard w zakresie zarządzania udostępnianiem dokumentów w sektorze ochrony zdrowia,

DICOM – norma opracowana dla potrzeb ujednolicenia wymiany i interpretacji danych medycznych reprezentujących lub związanych z obrazami diagnostycznymi w medycynie

REST API - architektoniczny styl tworzenia usług www. Bazuje na idei reprezentowania zasobów za pomocą metod HTTP i URI. Dane przekazywane będą w oparciu o format JSON.

Integracja z platformą P1

Podmiot będzie zobowiązany do uzyskania zdolności korzystania z usług P1 zgodnie z dokumentacją integracyjną P1. Podmioty medyczne w ramach spełnienia tego kryterium będą zobowiązane do integracji z platformą P1 z wykorzystaniem interfejsów zgodnie z dostępną dokumentacją integracyjną.

Dane obrazowe

Podmiot będzie zobowiązany do uzyskania zdolności automatycznego przekazywania danych obrazowych z urządzeń diagnostycznych do Platformy Usług Inteligentnych oraz będzie przesyłał te dane. Podmioty medyczne w ramach spełnienia kryterium będą zobowiązane do przekazywania dokumentów obrazowych z wykorzystaniem dostarczonego interfejsu PUI. Jednocześnie podmiot będzie zobowiązany do odbierania wyników zleconych analiz wykonanych ze wsparciem AI.

Dane o udzielonych świadczeniach

Podmiot będzie zobowiązany do uzyskania zdolności automatycznego przekazywania danych jednostkowych o udzielonych świadczeniach oraz będzie przesyłał te dane. Szpital w ramach spełnienia kryterium będą zobowiązany do sprawozdawania do Centrum e-Zdrowia kompletu informacji o zdarzeniach medycznych, wykorzystując do tego specyfikację opublikowanego interfejsu FHIR P1.

Dane o dokumentacji medycznej

Szpital Uzyska zdolność techniczną do automatycznego przekazywania Dokumentacji Medycznej oraz będzie przesyłał te dane. Podmioty medyczne w ramach spełnienia kryterium będą zobowiązane do utrzymywania repozytoriów EDM, w których zgodnie z wymaganiami opublikowanymi przez Centrum e-Zdrowia będą trzymały dokumenty zgodne z Polską Implementacją Krajową HL7 CDA oraz do rejestracji indeksów tej dokumentacji w rejestrze XDS domeny krajowej.

Wymagania ogólne w zakresie integracji z PUI po stronie szpitali:

- szerokopasmowy, symetryczny dostęp do sieci internet;

- urządzenia diagnostyczne podłączone do sieci komputerowej, umożliwiające bieżące przesyłanie danych w obszarze integracji z PUI, w szczególności danych obrazowych;

- zdolność techniczna do automatycznego przekazywania danych obrazowych z urządzeń diagnostycznych do Platformy Usług Inteligentnych za pośrednictwem wdrożonych rozwiązań PACS/RIS oraz przesyłanie tych danych zgodnie z wytycznymi integracyjnymi;

- integracja z Platformą Usług Inteligentnych w taki sposób, aby Użytkownik mógł korzystać z Usług bez konieczności przełączania lub logowania się do innego systemu

- integracja z Platformą Usług Inteligentnych w taki sposób, aby Użytkownik mógł przekazywać informację zwrotną o jakości działania Usługi Inteligentnej;

- w przypadku braku możliwości integracji bezpośredniej - konta oraz zestaw danych uwierzytelniających dla pracowników korzystających z PUI w systemie e-Gabinet+.

Szczegółowe wytyczne integracyjne z platformą PUI zostaną przekazane do 30.04.2025 r. oraz opublikowane na stronie Centrum e-Zdrowia.gov.pl

Wskaźnik D21G.R3

Podłączenie do centralnego repozytorium danych medycznych w Centrum e-Zdrowia w zakresie AI

– jednostka miary: liczba, wartość docelowa: 1

Sposób pomiaru: monitorowanie procesu podłączenia szpitala do centralnego repozytorium danych medycznych w Centrum e-Zdrowia w zakresie AI

Mechanizm weryfikacji: dokument wystawiony przez CeZ, potwierdzający wysłanie co najmniej jednego badania obrazowego do PUI

WSKAŹNIKI DO ROZLICZENIA DOFINANSOWANIA I UTRZYMANIA W OKRESIE TRWAŁOŚCI PRZEDSIĘWZIĘCIA

Do rozliczenia dofinansowania przez szpital wymagane będzie przedstawienie dokumentu potwierdzającego osiągnięcie każdego z podwskaźników, określonych dla każdego zakresu przedsięwzięcia.

W okresie trwałości przedsięwzięcia, , określonym w treści Wytycznych dotyczących kwalifikowalności wydatków finansowanych ze środków instrumentu na rzecz Odbudowy i Zwiększania Odporności dla przedsięwzięć realizowanych w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” stanowiących załącznik 7 do Umowy, wymagane będzie co najmniej utrzymanie podwskaźników tj.:

a. D18G.R1: Karty informacyjne z leczenia szpitalnego za dany rok kalendarzowy w postaci elektronicznej dokumentacji medycznej zaindeksowane w systemie P1 lub umieszczone w centralnym repozytorium danych medycznych w Centrum e-Zdrowia; jednostka miary: %; wartość docelowa: 95%,
b. D21G.R1: Integracja systemów szpitalnych z systemem P1; jednostka miary: liczba; wartość docelowa: 1,
c. D21G.R2: Zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej potwierdzone audytem bezpieczeństwa; jednostka miary: liczba; wartość docelowa: 1,
d. D21G.R3: Podłączenie do centralnego repozytorium danych medycznych w Centrum e-Zdrowia w zakresie AI; jednostka miary: liczba; wartość docelowa: 1,

– co będzie podlegać kontroli co roku, do 6 miesięcy od zakończenia danego roku kalendarzowego, za rok poprzedni, np. rok 2026 powinien zostać wykazany do końca czerwca 2027 r.; w przypadku podwskaźnika D21G.R2 raz w 2028 r.

MINIMALNA I MAKSYMALNA WARTOŚĆ PRZEDSIĘWZIĘCIA

Minimalna wartość przedsięwzięcia łącznie dla 4 powyższych zakresów:

- 1 025 000 zł – dla szpitali I stopnia,
- 1 600 000 zł - dla szpitali II stopnia,
- 2 325 000 zł – dla szpitali III stopnia, ogólnopolskich lub pulmonologicznych lub onkologicznych lub pediatrycznych.

Maksymalna wartość przedsięwzięcia łącznie dla 4 powyższych zakresów:

- 6 mln zł - dla szpitali I stopnia,
- 9 mln zł– dla szpitali II stopnia,
- 12 mln zł - dla szpitali III stopnia, ogólnopolskich lub pulmonologicznych lub onkologicznych lub pediatrycznych.