Mazowiecki Szpital Onkologiczny Sp. z o.o.

Al. Solidarności 12, 03-411 Warszawa

tel.: 22 766 15 05 faks: 22 766 15 99

NIP: 524 28 52 488 REGON: 369482970

www.szpitalonkologiczny.pl

Mazowiecki Szpital Onkologiczny w ramach realizacji przedsięwzięcia pn. „Wzmocnienie dojrzałości cyfrowej Mazowieckiego Szpitala Onkologicznego sp. z o.o." w ramach Krajowego Planu Odbudowy i Zwiększania Odporności: Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia" Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" na podstawie umowy o objęcie przedsięwzięcia wsparciem z planu rozwojowego nr KPOD.07.03 IP.10-0030/25/KPO/3498/2025/599 poprawił funkcjonowanie m. in. następujących obszarów:

- Stworzono kompletny system tworzenia kopii zapasowych wszystkich kluczowych systemów (w tym poczty e-mail) wraz z regularnym testowaniem odtwarzania danych.

- Wdrożono i poprawnie skonfigurowano zapory sieciowe (firewalle) chroniące sieć szpitala wraz z zapewnieniem bieżącej aktualizacji ich mechanizmów bezpieczeństwa (sygnatur, firmware, itp.).

- Środowisko poczty e-mail zabezpieczono przed podszywaniem, spamem i phishingiem, a dostęp do skrzynek oraz odtwarzalność danych pocztowych zostały zapewnione. Wdrożono mechanizmy wielowarstwowej ochrony: poczta przeniesiona do Exchange Online (Microsoft 365) z wymuszonym uwierzytelnianiem MFA dla użytkowników i administratorów, konfigurację domen pocztowych zgodną z dobrymi praktykami (rekordy SPF i DKIM aktywne) oraz filtry antyspamowe i antyphishingowe (FortiMail i Microsoft Defender) chroniące przed niepożądanymi wiadomościami.

- Segmentacja sieci wewnętrznej – oddzielenie stref o różnym poziomie zaufania/ryzyka (np. sieć administracyjna, sieć medyczna, sieć gościnna, strefa DMZ) oraz wdrożenie mechanizmów ograniczających ruch pomiędzy segmentami zgodnie z zasadą minimalnych uprawnień.

- Wdrożono nowoczesne rozwiązanie klasy Endpoint Detection and Response (EDR) na stacjach roboczych i serwerach. System EDR (Bitdefender GravityZone) zapewnia mechanizmy zaawansowanej ochrony punktów końcowych, takie jak antymalware, behawioralną detekcję zagrożeń oraz funkcje reakcji (np. izolację zainfekowanych hostów).

- Identyfikacja i uwierzytelnianie użytkowników w systemach – wdrożenie centralnego systemu zarządzania tożsamością (np. Active Directory) zapewniającego unikalne konto dla każdego użytkownika, wymóg stosowania silnych haseł i mechanizmów uwierzytelniania oraz zasad zarządzania uprawnieniami.

- Opracowani kompletny zestaw dokumentacji polityki i procedur z zakresu bezpieczeństwa informacji m.in.: Politykę Bezpieczeństwa Informacji, procedury i instrukcje dotyczące reagowania na incydenty,

politykę tworzenia kopii zapasowych i przywracania danych, politykę zarządzania dostępami oraz inne wymagane regulacje wewnętrzne.

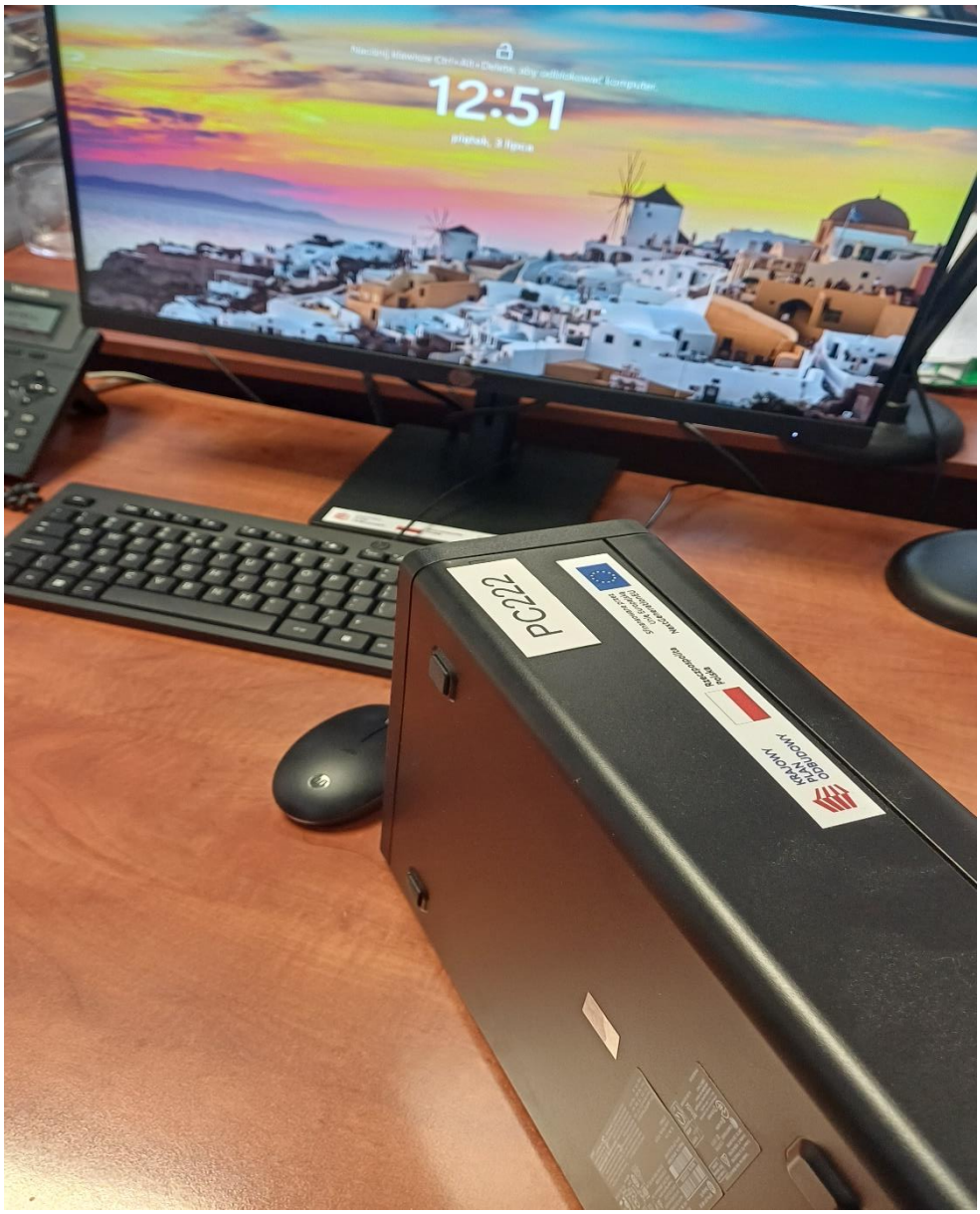
Audyt końcowy potwierdził wdrożenie kluczowych zabezpieczeń organizacyjnych, technicznych i dokumentacyjnych w Mazowieckim Szpitalu Onkologicznym, w szczególności w obszarach: systemu kopii zapasowych, zapór sieciowych, ochrony poczty e-mail, segmentacji sieci, ochrony stacji roboczych i serwerów, identyfikacji i uwierzytelniania, platformy wirtualizacyjnej, kontrolerów domeny, dokumentacji bezpieczeństwa oraz szkoleń z zakresu cyberbezpieczeństwa.

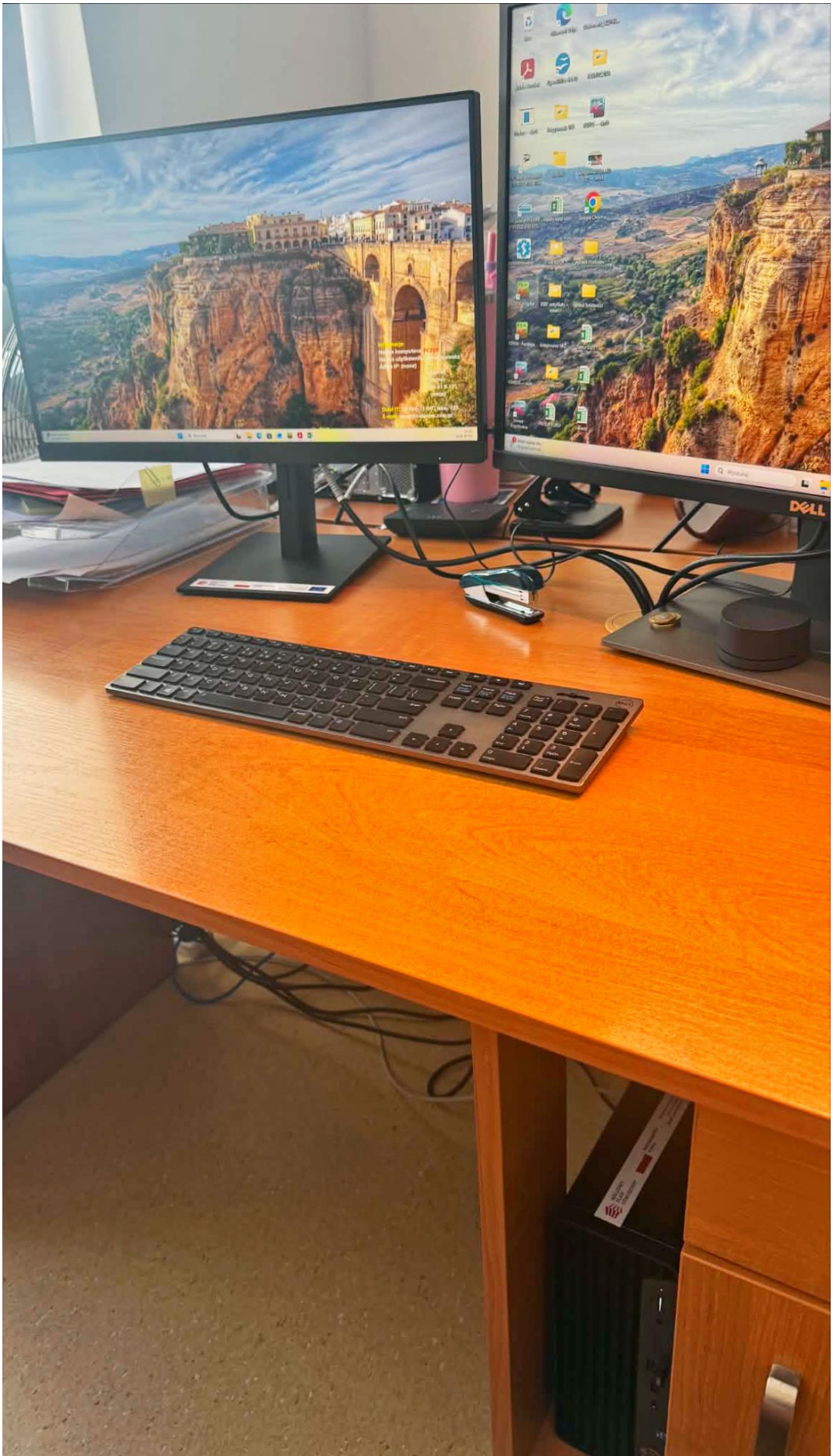
31 maja 2026 r.

Odbiór audytu końcowego potwierdzającego, że Szpital zrealizował projekt w pełni osiągając zakładany rezultat. **Wynik audytu pozytywny.**

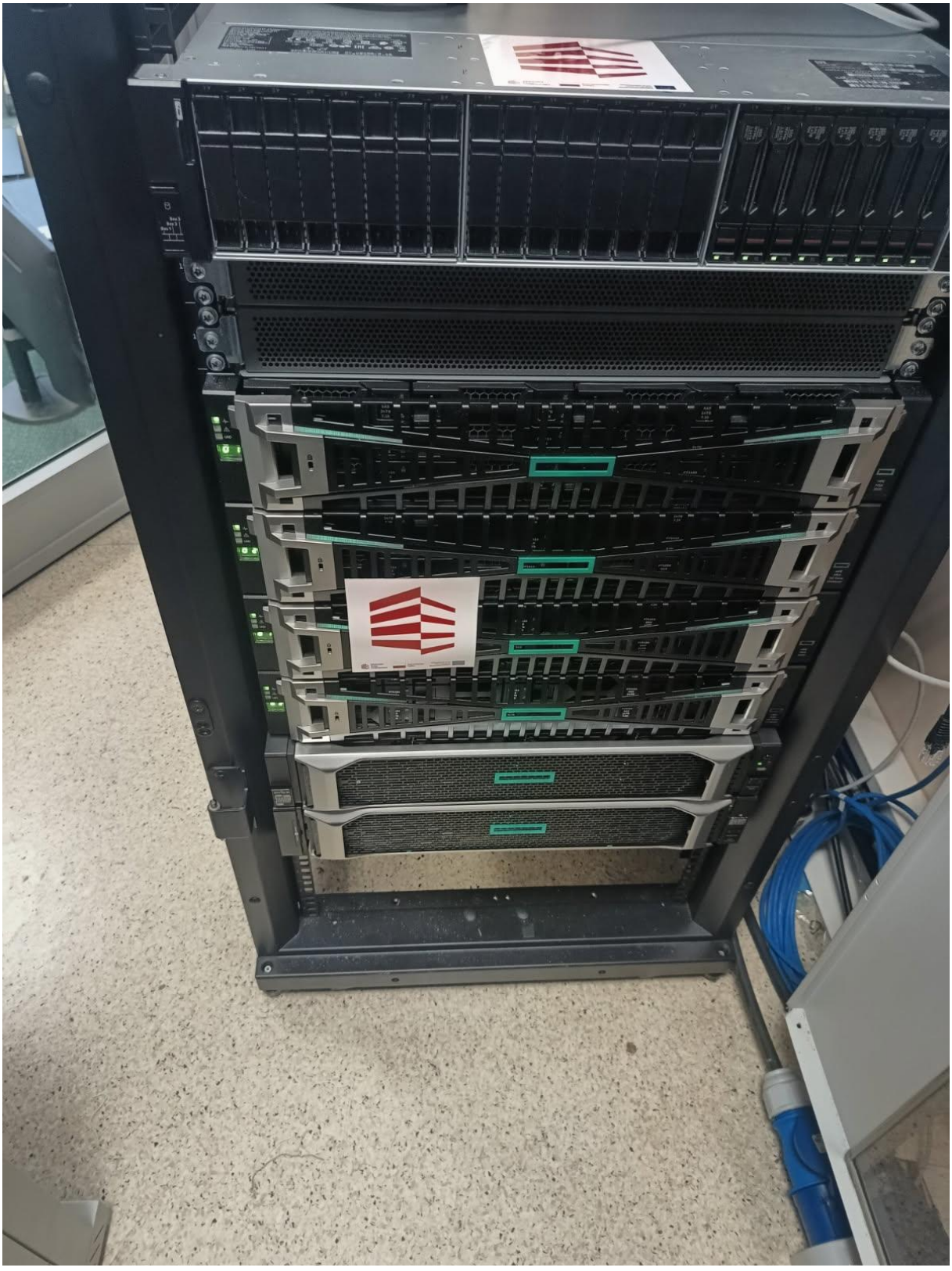
kwiecień 2026 r.

Realizacja umów – dostawy, instalacja sprzętu, oprogramowania, licencji




DELL

KRAJOWY
PLAN
ODBUDOWY
Rzeczpospolita
Polska
Sfinansowane przez
Unię Europejską
NextGenerationEU



18.02.2026 r. – 18.03.2026 r.

Zawieranie umów z wyłonionymi w postępowaniach Wykonawcami

27.02.2026 r. – 04.03.2026 r.

Opublikowanie w Bazie Konkurencyjności ostatniej grupy postępowań na wybór realizatorów Zadania nr 3 - Działania zwiększające poziom cyberbezpieczeństwa szpitala w pozostałym zakresie.

02.03.2026 r. – 09.03.2026 r.

Ocena zebranych ofert, rozstrzygnięcie kolejnych postępowań, zawieranie umów z wykonawcami.

05.02.2026 r. – 12.02.2026 r.

Opublikowanie w Bazie Konkurencyjności kolejnych postępowań między innymi na dostawę serwerów sterujących z biblioteką taśmową, serwerów z oprogramowanie, macierzy z dyskami oraz na wybór wykonawcy audytu końcowego.

06.02.2026 r. – 18.02.2026 r.

Ocena zebranych ofert, rozstrzygnięcie pierwszych postępowań, zawieranie umów z wykonawcami

22.01.2026 r. – 30.01.2026 r.

Opublikowanie w Bazie Konkurencyjności pierwszych postępowań między innymi na wybór realizatorów: Zadania nr 1 - Integracja i rozbudowa systemów informatycznych szpitala (w tym integracja z nowymi EDM) w zakresie dostawy serwera aplikacyjnego wraz ze stanowiskami opisowymi (6 stanowisk), rozszerzenie funkcjonalności systemu HIS; Zadania nr 2 - Digitalizacja dokumentacji medycznej; Zadania nr 3 - Działania zwiększające poziom cyberbezpieczeństwa szpitala w zakresie opracowania systemu zarządzania bezpieczeństwem informacji czy szkoleń z zakresu cyberbezpieczeństwa oraz Zadania nr 4 - Wdrożenie rozwiązań AI i podłączenie do centralnego repozytorium danych medycznych.

20.12.2025 r.

Podpisanie umowy nr KPOD.07.03-IP.10-0030/25/KPO/3498/2025/599 o objęcie wsparciem z planu rozwojowego Przedsięwzięcia „Wzmocnienie dojrzałości cyfrowej Mazowieckiego Szpitala Onkologicznego sp. z o.o.” w ramach Krajowego Planu Odbudowy i Zwiększania Odporności: Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia” Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”.

28.11.2025 r.

Ogłoszenie przez Ministerstwo Zdrowia wyników naboru w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” (nabór konkurencyjny - numer naboru: KPOD.07.03-IP.10-001/25) Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).