Załącznik nr 1 do pisma AW.173.1.2024 z dnia 19.09.2024 r.

ARKUSZ IDENTYFIKACJI, OCENY ORAZ OKREŚLENIA METODY PRZECIWDZIAŁANIA RYZYKU (ryzyko przewidywane) w 2025 r.

PRZEWIDYWANE RYZYKO				PRZECIWDZIAŁANIE RYZYKU PRZEWIDYWANEMU		
L. p.	Cel - zadanie	Ryzyko (wraz z podaniem kategorii)	Wpływ	Prawdopodobieństwo	Istotność ryzyka	Planowana metoda przeciwdziałania ryzyku
1.	Zabezpieczenie prawidłowej higieny w Ośrodku	Ryzyko działalności – zakażenia	niski	mało prawdopodobne	ryzyko nieznaczne	Przestrzeganie procedur i instrukcji oraz ich okresowa weryfikacja
2.	Podnoszenie standardu wykonywanych świadczeń	Ryzyko działalności - organizacji	niski	mało prawdopodobne	ryzyko nieznaczne	Analiza kwalifikacji i uprawnień personelu. Okresowe szkolenia wewnętrzne w celu podnoszenia standardu wykonywanych świadczeń.
3.	Zabezpieczenie przed awarią systemu informatycznego	Ryzyko działalności – systemów informatycznych	średni	średnio prawdopodobne	ryzyko umiarkowane	Współpraca z informatykiem. Zapewnienie dokumentacji w formie papierowej.
4.	Zapewnienie odpowiednio wyposażonych stanowisk pracy	Ryzyko działalności - organizacji	niski	mało prawdopodobne	ryzyko nieznaczne	Kontrola stanu gabinetów i sprzętu medycznego. Zgłaszanie usterek i braków w zakresie sprzętu medycznego. Wnioskowanie o doposażenia stanowisk.
5.	Zabezpieczenie środków publicznych poprzez właściwą ewidencję księgową.	Ryzyko finansowe- brak kompletności, terminowości informacji finansowych	Średni	Niskie	Umiarkowane	- opracowywanie i stosowanie zasady gromadzenia i przetwarzania danych finansowych, - stosowanie informatycznych systemów

						wspomagania ewidencji i sprawozdawczości finansowej, - prowadzenie merytorycznej, rachunkowej i formalnej weryfikacji dowodów źródłowych.
6.	Zapewnienie poprawnego naliczania wynagrodzeń z tytułu umów o pracę, umów zlecenia oraz umów o dzieło	Ryzyko finansowe: - awaria sprzętu - działania osób trzecich uniemożliwiające realizację zadania	Średni	Niskie	Umiarkowane	- stała ochrona danych dotyczących wynagrodzeń, - wprowadzenie stosownych zabezpieczeń systemów komputerowych, - stałe podnoszenie kwalifikacji przez pracowników
7.	Zapewnienie poprawności sporządzania i realizacji planu finansowego	Ryzyko finansowe: - błąd pracownika -brak wiedzy na temat konieczności opracowania planów finansowych	Średni	Niskie	Umiarkowane	-monitorowanie terminów sporządzenia planów finansowych -stałe monitorowanie realizacji planu budżetowego, dokonywanie niezbędnych korekt planu w ciągu roku.
8.	Jasny podział ról i odpowiedzialności	Ryzyko dotyczące zasobów ludzkich	Średni	Niskie	Umiarkowane	Jasny podział ról i odpowiedzialności Dobre praktyki w zakresie zarządzania komunikacją i współpracą. Systemy monitorowania postępu zadań i raportowania, aby zapewnić, że zadania są realizowane zgodnie z planem przez właściwe osoby.
W zakresie obszaru ochrony danych osobowych oraz związanych z zarządzaniem systemami IT:						
9.	Bezpieczeństwo danych i systemów informatycznych	Ryzyko dotyczące zasobów ludzkich	średni	średnie	ryzyko umiarkowane	Kontrola uprawnień dostępu do oprogramowania systemowego oraz programów zawierających dane wrażliwe zgodnie z przyjętą polityką RODO. Kontrola dostępu do urządzeń i nośników danych. Kontrola dostępu do systemów z

						sieci zewnętrznej za pomocą połączeń szyfrowanych.
10.	Sprawność i ciągłość działania systemów informatycznych	Absencja pracowników, ryzyko dotyczące zasobów ludzkich	wysoki	wysokie	ryzyko umiarkowane	Zapewnienie ciągłości działania systemów informatycznych poprzez: konserwację i aktualizację systemów informatycznych, instalację dostępnych aktualizacji, zapewnienie właściwej ochrony antywirusowej, zapewnienie kopii zapasowych zgodnie z obowiązującą polityką bezpieczeństwa.
11.	Sprawność i ciągłość działania sieci zewnętrznej oraz wewnętrznej	Absencja pracowników, ryzyko dotyczące zasobów ludzkich	wysoki	średnie	ryzyko umiarkowane	Zapewnienie ciągłości działania sieci wewnętrznej oraz zewnętrznej. Uruchomienie mechanizmów kontroli urządzeń sieciowych z sieci zewnętrznej.
12.	Zagubienie / kradzież nośników danych, komputerów przenośnych	Ryzyko finansowe oszustwa i kradzieży, podlegające ubezpieczeniu ryzyko działalności Systemów Informatycznych	wysoki	średnie	ryzyko umiarkowane	Zapewnienie szkoleń pracowników. Podnoszenie świadomości zagrożeń informatycznych pracownikom.
13.	Pożar / zalanie pomieszczeń technicznych (serwerownia)	Ryzyko finansowe podlegające ubezpieczeniu ryzyko działalności Systemów Informatycznych	wysoki	średnie	ryzyko nieznaczne	Zapewnienie sprawności działania systemów przeciwpożarowych. Przechowywanie kopii zapasowych w pomieszczeniu innego budynku.
14.	Odnowienie sprzętu komputerowego spowodowane zmianami technologicznymi	Ryzyko finansowe Ryzyko działalności Systemów Informatycznych	wysoki	wysokie	Ryzyko wysokie	Planowanie środków finansowych przeznaczonych na wymianę i odnowienie sprzętu komputerowego oraz systemów operacyjnych.

Ustala się następujące poziomy istotności ryzyka:

1) **Ryzyko poważne**, tj. ryzyko o wysokim wpływie i wysokim lub średnim prawdopodobieństwie oraz średnim wpływie i wysokim prawdopodobieństwie;
2) **Ryzyko umiarkowane**, tj. ryzyko o wysokim wpływie i niskim prawdopodobieństwie, ryzyko o średnim wpływie i niskim prawdopodobieństwie, a także ryzyko o niskim wpływie i wysokim prawdopodobieństwie;
3) **Ryzyko nieznaczne**, tj. ryzyko o niskim wpływie i średnim lub niskim prawdopodobieństwie oraz ryzyko o średnim wpływie i niskim prawdopodobieństwie.

.....

Podpis Kierownika Jednostki (podpisano elektronicznie)

Legenda:

1. Zidentyfikowane ryzyka powinny być przyporządkowane określonym celom i zadaniom wynikającym z działalności jednostki.
2. Proponowane kategorie (obszary ryzyka):ryzyko finansowe, ryzyko dotyczące zasobów ludzkich, ryzyko działalności, ryzyko zewnętrzne. Jeżeli w Pana/i jednostce zastosowana jest inna kategoryzacja (kategorii obszarów ryzyka) proszę o podanie tych ryzyk według własnych kategorii.