

Znak sprawy: Z.II.260.027.Zp.2022

**ZAPROSZENIE DO ZŁOŻENIA OFERTY CENOWEJ
O WARTOŚCI PONIŻEJ 130 000 ZŁOTYCH**

Przedmiot zamówienia:

**WYKONANIE AUDYTU BEZPIECZEŃSTWA SYSTEMÓW
TELEINFORMATYCZNYCH ORAZ SPORZĄDZENIE RAPORTU Z AUDYTU
Z WYNIKAMI WYKONANYCH CZYNNOŚCI W SAMODZIELNYM PUBLICZNYM
ZESPOLE ZAKŁADÓW OPIEKI ZDROWOTNEJ W NISKU**

W trybie:

rozpoznania cenowego - postępowanie o wartości poniżej 130 000 zł.

Podstawa:

„Regulamin udzielania zamówień, których wartość nie przekracza wyrażonej w złotych równowartości kwoty 130 000 zł w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku” w sprawie zasad dokonywania zakupu dostaw, usług i robót budowlanych na potrzeby Szpitala Powiatowego im. PCK w Nisku.

Nisko, Sierpień 2022

Zaproszenie do złożenia oferty cenowej
Wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego
oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku

Znak sprawy: Z.II.260.027.Zp.2022

Nisko, dnia: 04/08/2022 r.

OGŁOSZENIE O ZAMÓWIENIU
KTÓREGO WARTOŚĆ NIE PRZEKRACZA WYRAŻONEJ W ZŁOTYCH
RÓWNOWARTOŚCI KWOTY 130.000 ZŁOTYCH

1) Zamawiający:

Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Nisku

ul. Kościuszki 1, 37-400 Nisko

NIP: 865-20-74-945, REGON: 000306680

Tel. (15) 8416 703, 8416 779, Fax. (15) 8416 704, www.szpital-nisko.pl, e-mail: przetargi@szpital-nisko.pl

1) Opis przedmiotu zamówienia: **Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku. (Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1 do zaproszenia do złożenia oferty cenowej).**

2) Wspólny Słownik Zamówień kod CPV:

72810000-1

3) Realizacja przedmiotu zamówienia: **W nieprzekraczalnym terminie do dnia 20 listopada 2022 r.**

4) Warunki udziału w postępowaniu:

Lp.	Warunki udziału w postępowaniu
1.	Zdolność do występowania w obrocie gospodarczym. O udzielenie zamówienia mogą ubiegać się Wykonawcy prowadzący działalność gospodarczą lub zawodową, którzy są wpisani do jednego z rejestrów zawodowych lub handlowych prowadzonych w kraju, w którym mają siedzibę lub miejsce zamieszkania. Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku. Ocena spełniania warunków udziału w postępowaniu będzie dokonana na zasadzie spełnia/nie spełnia.
2.	Uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki, dotyczące posiadania kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów. Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku. Ocena spełniania warunków udziału w postępowaniu będzie dokonana na zasadzie spełnia/nie spełnia.
3.	Sytuacja ekonomiczna lub finansowa. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki, dotyczące sytuacji ekonomicznej lub finansowej. Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku. Ocena spełniania warunków udziału w postępowaniu będzie dokonana na zasadzie spełnia/nie spełnia.
4.	Zdolności techniczna lub zawodowa. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki, dotyczące zdolności technicznej lub zawodowej. Zamawiający uzna warunek za spełniony jeżeli Wykonawca udowodni, że w okresie ostatnich trzech lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizował co najmniej dwie usługi odpowiadające swoim rodzajem i wielkością przedmiotowi zamówienia. Ocena spełniania warunków udziału w postępowaniu będzie dokonana na zasadzie spełnia/nie spełnia na podstawie dokumentów dołączonych do oferty.

5) Wykaz oświadczeń lub dokumentów, jakie mają dostarczyć wykonawcy wraz z ofertą:

Lp.	Wymagany dokument
1.	Formularz ofertowy. Wypełniony formularz ofertowy.
2.	Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału.
3.	Oświadczenie Wykonawcy. Oświadczenie Wykonawcy, że nie podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 poz. 835).

Zaproszenie do złożenia oferty cenowej
Wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego
oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku

Lp.	Wymagany dokument
4.	Pełnomocnictwo. W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę(-y) nie wymienioną(-e) w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne pełnomocnictwo w oryginale lub kopii poświadczonej notarialnie.
5.	Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej. Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.
6.	Wykaz dostaw lub usług. Wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, dostaw lub usług w zakresie niezbędnym do wykazania spełniania warunku wiedzy i doświadczenia w okresie ostatnich trzech lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców, oraz załączeniem dokumentu potwierdzającego, że te dostawy lub usługi zostały wykonane lub są wykonywane należycie.
7.	Wykaz osób. Wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia wraz z informacjami na temat ich kwalifikacji zawodowych i doświadczenia niezbędnych do wykonania zamówienia oraz informacją o podstawie do dysponowania tymi osobami.

- 6) Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami:
- **Tomasz Maluga** – Główny specjalista ds. Ekonomiczno - Administracyjnych, tel.: (15) 8416 701,
 - **Piotr Tabor** – Starszy specjalista ds. Zamówień Publicznych, tel. (15) 8416 779,
- 7) Termin związania ofertą: **30 dni**.
- 8) Opis sposobu przygotowywania ofert:
- Oferta musi być sporządzona w języku polski, w sposób czytelny,
 - Wykonawca może złożyć tylko jedną ofertę,
 - Dokumenty ofertowe muszą być podpisane przez osobę(-y) upoważnioną(-e) do reprezentowania Wykonawcy (zgodnie z formą reprezentacji określoną w odpowiednim rejestrze lub innym dokumencie właściwym dla formy organizacyjnej Wykonawcy) bądź posiadającą(-ce) stosowne pełnomocnictwo. Pełnomocnictwo w oryginale należy dołączyć do oferty,
 - Oferta musi być sporządzona zgodnie z opisem przedmiotu zamówienia,
 - Wykonawca jest obowiązany wskazać w ofercie części zamówienia, których wykonanie zamierza powierzyć Podwykonawcom,
 - Oferty otrzymane przez Zamawiającego po terminie składania ofert oraz oferty złożone w innej niż dopuszczalnej formie zostaną odrzucone,
 - Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać ofertę,
 - Wykonawca o wprowadzeniu zmian lub zamiarze wycofania oferty powiadamia Zamawiającego pisemnie,
 - Pismo informujące o zmianie lub wycofaniu oferty należy złożyć (przed terminem składania ofert), oznaczając dodatkowo „Zmiana oferty”, „Wycofanie oferty”,
 - Do pisma o zmianie lub wycofaniu oferty musi być załączony dokument potwierdzający prawo osoby podpisującej informację do reprezentowania Wykonawcy.
 - Oczywiste omyłki pisarskie lub rachunkowe w ofercie zostaną poprawione przez Zamawiającego, każdy inny błąd w ofercie, który nie zostanie przez Zamawiającego zakwalifikowany jako oczywista omyłka pisarska lub rachunkowa spowoduje odrzucenie oferty.
 - Ceny w ofercie muszą być wyrażone w złotych polskich i zaokrąglone do dwóch miejsc po przecinku,
 - Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich,
 - Zamawiający nie dopuszcza składania ofert częściowych,
 - Zamawiający nie dopuszcza składania ofert wariantowych.

Zaproszenie do złożenia oferty cenowej
Wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego
oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku

Ofertę opisaną w następujący sposób: „Oferta na wykonanie audytu bezpieczeństwa systemów teleinformatycznych oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku. **NIE OTWIERAĆ przed: 12/08/2022**” należy złożyć w zamkniętej kopercie w sekretariacie SPZZOZ w Nisku lub przesłać do Zamawiającego w formie elektronicznej na adres e-mail: przetargi@szpital-nisko.pl w nieprzekraczalnym terminie do dnia **16/08/2022 r. do godziny 09.00.**

Oferty przekazane drogą elektroniczną uważa się za złożone w terminie, jeżeli zostały przekazane przed upływem wyznaczonego terminu, a fakt jej przekazania został niezwłocznie potwierdzony przez Zamawiającego.

- 9) Miejsce oraz termin otwarcia ofert:

Siedziba Zamawiającego, pokój nr 17 w dniu: 16/08/2022 r. godzina 09.30.

- 10) Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert:

- zamawiający będzie oceniał oferty według następujących kryteriów:

Nr	Nazwa kryterium	Waga
1	Cena	100 %

- punkty przyznawane za powyższe kryteria będą liczone według następujących wzorów:

Nr kryterium	Wzór
1.	Cena (koszt) $\text{Liczba punktów} = (\text{Cmin}/\text{Cof}) * 100 * \text{waga}$ <p>gdzie:</p> <ul style="list-style-type: none">- Cmin – najniższa cena spośród wszystkich ofert,- Cof – cena podana w badanej ofercie
Całkowita liczba uzyskanych przez badaną ofertę punktów	
$= [(\text{Cmin}/\text{Cof}) * 100 * \text{waga}]$	

- 11) Pozostałe informacje:

1. Zamawiający zastrzega sobie prawo do unieważnienia postępowania na każdym etapie przed podpisaniem umowy bez podawania przyczyn.
2. Zamawiający unieważnia postępowanie w szczególności, jeżeli:
 - nie złożono co najmniej jednej oferty niepodlegającej odrzuceniu,
 - cena najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,
 - wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym Zamawiającego, czego nie można było wcześniej przewidzieć,
 - postępowanie jest obciążone niemożliwą do usunięcia wadą uniemożliwiającą prawidłową realizację zamówienia.
3. Zamawiający odrzuci złożoną przez Wykonawcę ofertę w szczególności, jeżeli:
 - jej treść nie odpowiada treści zapytania ofertowego,
 - jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, zawiera istotne błędy w obliczeniu ceny, tzn. takie, które uniemożliwiają ustalenie ceny ofertowej,

Zaproszenie do złożenia oferty cenowej
Wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego
oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku

- jest nieważna na podstawie odrębnych przepisów,
 - Zamawiający zastrzega sobie prawo odrzucenia oferty, która będzie zawierała rażąco niską cenę.
4. Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień dotyczących treści złożonej oferty (w tym zawartej w ofercie ceny) oraz do uzupełnienia wymaganych dokumentów, w przypadku uznania takiego działania za celowe,
 5. Zamawiający wykluczy Wykonawcę, który nie wykazał spełnienia warunków udziału w postępowaniu. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą,
 6. Wykonawca może powierzyć wykonanie przedmiotu zamówienia podwykonawcom, po uzyskaniu pisemnej zgody Zamawiającego,
 7. Zamawiający o wyborze najkorzystniejszej oferty poinformuje pisemnie,
 8. Zamawiający do powyższego postępowania nie przewiduje zastosowania procedury odwołań,
 9. Postępowanie prowadzone jest w języku polskim,
 10. Pytania, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują faksem na numer (15) 841 67 04 lub przy użyciu środków komunikacji elektronicznej na adres e-mail: przetargi@szpital-nisko.pl,
 11. Zamawiający podkreśla, że w celu zachowania reguł równego traktowania Wykonawców, nie będzie udzielał ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane do Zamawiającego pytania, w sprawach wymagających formy pisemnej. Wszelkie ewentualnie udzielone telefonicznie informacje nie będą wiążące dla Zamawiającego i Wykonawców, nie wywołują skutków prawnych dla toczącego się postępowania i nie mogą być podstawą jakichkolwiek roszczeń,
 12. W przypadku jeżeli dwie lub więcej ofert przedstawi taki sam bilans ceny / kosztu za realizację przedmiotu zamówienia, Zamawiający zastrzega sobie prawo do przeprowadzenia negocjacji z jednym lub z kilkoma Wykonawcami lub Zamawiający wezwie Wykonawcę do złożenia oferty dodatkowej w określonym przez Zamawiającego terminie. Zamawiający będzie pozyskiwał oferty dodatkowe do skutecznego wyboru oferty najkorzystniejszej,
 13. Wykonawca, którego oferta zostanie wybrana przez Zamawiającego zobowiązuje się podpisać umowę, której projekt stanowi załącznik do niniejszego zaproszenia do składania ofert i jest jego integralną częścią.
- 12) Ochrona danych osobowych:
1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „Rozporządzenie”, informuję, że:
 - Administratorem Państwa danych jest **Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej** 37-400 Nisko, ul. Kościuszki 1, tel.: 15 841 67 03, fax: 15 841 67 04, e-mail: info@szpital-nisko.pl,
 - Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu email: adam.zieminski@cbi24.pl lub pisemnie pod adresem Administratora.
 2. Dane osobowe będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego.
 3. Dane osobowe będą przetwarzane przez okres zgodnie z art. 78 ust. 1 i 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129), przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy.
 4. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia.

5. Odbiorcami Państwa danych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 4 ustawy Pzp.
6. Obowiązek podania przez Państwa danych osobowych bezpośrednio Państwa dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z Pzp.
7. Osoba, której dane dotyczą ma prawo do:
 - dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania,
 - w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów Rozporządzenia służy prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa,
8. Osobie, której dane dotyczą nie przysługuje:
 - w związku z art. 17 ust. 3 lit. b, d lub e Rozporządzenia - prawo do usunięcia danych osobowych,
 - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 Rozporządzenia,
 - na podstawie art. 21 Rozporządzenia - prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c Rozporządzenia.
9. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.
10. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 Rozporządzenia, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego lub konkursu ani zmianą postanowień umowy w zakresie niezgodnym z Pzp.
11. Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 Rozporządzenia, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.
12. W przypadku danych osobowych zamieszczonych przez Administratora w Biuletynie Zamówień Publicznych, prawa, o których mowa w art. 15 i art. 16 Rozporządzenia, są wykonywane w drodze żądania skierowanego do Administratora.
13. Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 ust. 1 Rozporządzenia, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, Administrator nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 Rozporządzenia.
14. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.
15. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 Rozporządzenia, nie może naruszać integralności protokołu oraz jego załączników.
16. Ponadto informujemy, że w związku z przetwarzaniem Państwa danych osobowych nie podlegają Państwo decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 Rozporządzenia.

Zaproszenie do złożenia oferty cenowej
Wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego
oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku

13) Załączniki:

- Załącznik nr 1 – opis przedmiotu zamówienia,
- Załącznik nr 2 – wzór formularza ofertowego,
- Załącznik nr 3 – wzór wykazu dostaw lub usług,
- Załącznik nr 4 – wzór wykazu osób,
- Załącznik nr 5 – wzór oświadczenia o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu,
- Załącznik nr 6 – wzór oświadczenia wykonawcy,
- Załącznik nr 7 – wzór / projekt umowy,

Postępowanie o udzielenie zamówienia jest prowadzone zgodnie z postanowieniami Regulaminu udzielania zamówień o wartości nie przekraczającej kwoty 130 000 zł, oraz przepisami ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. Nr 16, poz. 93, z późn. zm.).

Dyrektor
Samodzielnego Publicznego
Zespołu Zakładów Opieki Zdrowotnej
w Nisku

Paweł Tofil

Data: 05/08/2022

podpis Kierownika Zamawiającego

SAMODZIELNY PUBLICZNY
ZESPÓŁ ZAKŁADÓW OPIEKI ZDROWOTNEJ w Nisku
37-400 Nisko, ul. Kościuszki 1
tel. (15) 8416703, fax (15) 8416704
NIP 865-20-74-945, REGON 000306680

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Ogólna charakterystyka i warunki realizacji zamówienia:

Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa systemów teleinformatycznych oraz sporządzenie raportu z audytu z wynikami czynności w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku,

II. Zakres przedmiotowy:

1. Celem audytu jest dokonanie oceny poziomu bezpieczeństwa teleinformatycznego Zamawiającego po zrealizowaniu czynności, które mogą zostać objęte finansowaniem zgodnie z **ZARZĄDZENIEM NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA** z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców - (załącznik nr 2 do Opisu Przedmiotu Zamówienia), w odniesieniu do stanu bezpieczeństwa teleinformatycznego Zamawiającego istniejącego na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Zamawiającego w formie „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa” (załącznik nr 3 do Opisu Przedmiotu Zamówienia).
2. Z Przeprowadzonego Audytu Wykonawca sporządzi Raport, z którego będzie wynikać podniesienie poziomu bezpieczeństwa teleinformatycznego Zamawiającego w odniesieniu do poziomu wynikającego z „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa” lub jego brak.
3. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.
4. Zakres audytu obejmował będzie czynności, które mogą zostać objęte finansowaniem w przypadku wykazania przez Zamawiającego, wynikiem audytu bezpieczeństwa, zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej. Do czynności tych należą:
 - 1) zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa, w szczególności:
 - a) systemów kopii bezpieczeństwa, odniesienia kopii, segmentacji w celu odseparowania urządzeń backupu, zapewnienia mechanizmów weryfikacji poprawności i odtwarzalności kopii i backupu,
 - b) systemów kontroli dostępu administracyjnego, zarządzania uprawnieniami (IAM/IDM),
 - c) urządzeń i oprogramowania typu firewall - zaporą sieciową z wbudowanym IPS oraz systemem antywirusowym oraz platform niezbędnymi do ich uruchomienia,
 - d) systemów zapewniających bezpieczny system poczty elektronicznej, włączając w to systemy weryfikacji załączników i treści korespondencji oraz systemy wieloskładnikowego uwierzytelniania,
 - e) rozwiązań zapewniających ochronę DNS (DNS Protection) z użyciem systemów lokalnych (licencja oraz wsparcie w okresie do dnia 31 grudnia 2022 r.),
 - f) systemu typu SIEM,
 - g) systemu typu NAC – jako system lokalny;
 - 2) zakup usługi wdrożenia i konfiguracji urządzeń i oprogramowania, o których mowa w pkt 1, oraz wsparcia eksperckiego w zakresie cyberbezpieczeństwa przez okres do dnia 31 grudnia 2022 r.;
 - 3) zakup i wdrożenie systemu (usługi) typu SOC – przez okres do dnia 31 grudnia 2022 r.;
 - 4) zakup usługi skanów podatności, w zakresie sprecyzowanym w materiale referencyjnym „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia”, opublikowanym na stronie internetowej Centrum e-Zdrowia), przez okres do dnia 31 grudnia 2022 r.;
 - 5) zakup opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych

wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) - jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii;

- 6) zakup szkolenia lub szkoleń w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT, w tym:
 - a) ochrony przed zaawansowanymi atakami przez pocztę i WWW,
 - b) tworzenia i zarządzania polityką hasel i tożsamości,
 - c) zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
 - d) wykonywania kopii zapasowych oraz tworzenia i utrzymania polityki ciągłości działania.

III. Ramowy harmonogram wykonania usługi:

1. Spotkanie koordynacyjne i szczegółowe planowanie realizacji usługi: do 7 dni roboczych od dnia zawarcia Umowy,
2. Wnikliwa analiza poziomu bezpieczeństwa teleinformatycznego Zamawiającego ze stanu początkowego z uwzględnieniem Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa. Głównym aspektem analizy powinny być elementy możliwe do finansowania opisane w pkt. 4 Opisu przedmiotu Zamówienia (odpowiednio Rozdziale 2 Zarządzenia prezesa NFZ) - do 14 dni roboczych od dnia zawarcia Umowy,
3. Przeprowadzenie Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po wdrożeniu przez Zamawiającego czynności podnoszących poziom bezpieczeństwa systemów teleinformatycznych - do 7 dni roboczych od dnia powiadomienia przez Zamawiającego Wykonawcy o gotowości do poddania się Audytowi. Powiadomienie Wykonawcy przez Zamawiającego o gotowości do poddania się Audytowi powinno nastąpić **nie później niż do dnia 10 listopada 2022 r.**
4. Sporządzenie pisemnego Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i doręczenie go Zamawiającemu - do 7 dni roboczych od dnia zakończenia Audytu.

IV. Dodatkowe wymagania:

1. Audyt poziomu bezpieczeństwa, o którym mowa w Opisie Przedmiotu Zamówienia może być przeprowadzony przez:
 - 1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
 - 2) co najmniej dwóch audytorów posiadających:
 - a) certyfikaty określone w poniższym wykazie certyfikatów uprawniających do przeprowadzenia audytu lub
 - b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
 - c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.
2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:
 - 1) Certified Internal Auditor (CIA);
 - Certified Information System Auditor (CISA);
 - Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami

Zaproszenie do złożenia oferty cenowej
Wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego
oraz sporządzenie raportu z audytu z wynikami wykonanych czynności w Szpitalu Powiatowym im. PCK w Nisku

ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

- Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami *ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;*
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

V. Załączniki:

1. Załącznik nr 1 - Zakres Raportu.
2. Załącznik nr 2 ZARZĄDZENIE NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.
3. Załącznik nr 3 - Ankieta weryfikacji dojrzałości pod kątem bezpieczeństwa.

SZCZEGÓŁOWY ZAKRES RAPORTU		
Lp.	Nazwa obszaru	Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców
1.	Skuteczność działania infrastruktury	<ul style="list-style-type: none"> – Urządzenia i konfiguracja w zakresie ochrony poczty, – Urządzenia i konfiguracja w zakresie ochrony sieci, – Urządzenia i konfiguracja w zakresie systemów serwerowych, – Urządzenia i konfiguracja w zakresie stacji roboczych, – Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa.
2.	Procesy zarządzania bezpieczeństwem informacji	<ul style="list-style-type: none"> – Nośniki wymienne – udokumentowany sposób postępowania, – Zarządzanie tożsamością / dostęp do systemów w zakresie: <ul style="list-style-type: none"> - przydzielania dostępu, - odbierania dostępu, - pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o której mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.
3.	Monitorowanie i reagowanie na incydenty bezpieczeństwa	<ul style="list-style-type: none"> – Procedury zarządzania incydentami, – Raportowanie poziomów pokrycia scenariuszami znanych incydentów, – Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego / sektorowego zespołu cyberbezpieczeństwa, – Monitorowanie i wykrycie incydentów bezpieczeństwa, – Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.
4.	Zarządzanie ciągłością działania	<ul style="list-style-type: none"> – Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa, – Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa, – Procedury wykonywania i przechowywania kopii zapasowych, – Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP), – Procedury utrzymaniowe.
5.	Utrzymanie systemów informacyjnych	<ul style="list-style-type: none"> – Harmonogramy skanowania podatności, – Aktualny status realizacja postępowania z podatnościami, – Procedury związane z identyfikowaniem (wykryciem) podatności, – Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.
6.	Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	<ul style="list-style-type: none"> – Polityka bezpieczeństwa w relacjach z dostawcami, – Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa, – Metody uwierzytelniania.

**ZARZĄDZENIE NR 68/2022/BBICD
PREZESA NARODOWEGO FUNDUSZU ZDROWIA**

z dnia 20 maja 2022 r.

**w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów
teleinformatycznych świadczeniodawców**

Na podstawie art. 102 ust. 5 pkt 21 i 25 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2021 r. poz. 1285, z późn. zm.¹⁾) oraz polecenia Ministra Zdrowia z dnia 29 kwietnia 2022 r., znak: DIWP.07.5.2022.KW, wydanego na podstawie 11h ust. 2 pkt 2 i ust. 4 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID- 19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2021 r. poz. 2095, z późn. zm.²⁾), zarządza się, co następuje:

Rozdział 1.

Postanowienia ogólne

§ 1. Zarządzenie określa warunki przyznawania i rozliczania środków na finansowanie działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców.

2. Finansowanie, o którym mowa w ust. 1, przyznawane jest świadczeniodawcom, będącym podmiotami leczniczymi, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2022 r. poz. 633, 655 i 974) prowadzącymi szpital i posiadającymi umowę o udzielanie świadczeń opieki zdrowotnej zawartą z Narodowym Funduszem Zdrowia obowiązującą w 2021 r. oraz 2022 r., w rodzaju:

- 1) leczenie szpitalne lub
- 2) rehabilitacja lecznicza, lub
- 3) opieka psychiatryczna i leczenie uzależnień, lub
- 4) lecznictwo uzdrowiskowe.

3. Finansowanie, o którym mowa w ust. 1, obejmuje wydatki świadczeniodawców ponoszone od dnia 29 kwietnia 2022 r. do dnia 31 grudnia 2022 r.

§ 2. Użyte w zarządzeniu określenia oznaczają:

- 1) dyrektor właściwego oddziału Funduszu - dyrektora oddziału wojewódzkiego Narodowego Funduszu Zdrowia, właściwy w zakresie realizacji umowy o udzielanie świadczeń opieki zdrowotnej, o której mowa w § 1 ust. 2;
- 2) Fundusz – Narodowy Fundusz Zdrowia;
- 3) oddział Funduszu - oddział wojewódzki Funduszu.

Rozdział 2.

Warunki udzielania finansowania

§ 3. 1. Finansowaniem, o którym mowa w § 1, w okresie do dnia 31 grudnia 2022 r., są objęte działania podnoszące poziom bezpieczeństwa systemów teleinformatycznych świadczeniodawców, z zastrzeżeniem ust. 2, i polegające na wykonaniu co najmniej jednej z następujących czynności:

- 1) zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa, w szczególności:
 - a) systemów kopii bezpieczeństwa, odmięscowienia kopii, segmentacji w celu odseparowania urządzeń backupu, zapewnienia mechanizmów weryfikacji poprawności i odtwarzalności kopii i backupu,

¹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 1292, 1559, 1773, 1834, 1981, 2120, 2232 i 2270 oraz z 2022 r. poz. 64, 91, 526, 583, 655, 807, 974 i 1002.

²⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 2120, 2133, 2262, 2269, 2317, 2368 i 2459 oraz z 2022 r. poz. 202, 218, 655 i 830

- b) systemów antywirusowych dla stacji roboczych i serwerów - centralnie zarządzanych, systemów klasy Endpoint Detection and Response (EDR),
 - c) systemów kontroli dostępu administracyjnego, zarządzania uprawnieniami (IAM/IDM),
 - d) urządzeń i oprogramowania typu firewall - zaporą sieciową z wbudowanym IPS oraz systemem antywirusowym oraz platform niezbędnymi do ich uruchomienia,
 - e) systemów zapewniających bezpieczny system poczty elektronicznej, włączając w to systemy weryfikacji załączników i treści korespondencji oraz systemy wieloskładnikowego uwierzytelniania,
 - f) rozwiązań zapewniających ochronę DNS (DNS Protection) z użyciem systemów lokalnych (licencja oraz wsparcie w okresie do dnia 31 grudnia 2022 r.),
 - g) systemu typu SIEM,
 - h) systemu typu NAC – jako system lokalny;
- 2) zakup usługi wdrożenia i konfiguracji urządzeń i oprogramowania, o których mowa w pkt 1, oraz wsparcia eksperckiego w zakresie cyberbezpieczeństwa przez okres do dnia 31 grudnia 2022 r.;
- 3) zakup i wdrożenie systemu (usługi) typu SOC – przez okres do dnia 31 grudnia 2022 r.;
- 4) zakup usługi skanów podatności, w zakresie sprecyzowanym w materiale referencyjnym „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia”, opublikowanym na stronie internetowej Centrum e-Zdrowia³⁾, przez okres do dnia 31 grudnia 2022 r.;
- 5) zakup opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) - jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii;
- 6) zakup szkolenia lub szkoleń w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT, w tym:
- a) ochrony przed zaawansowanymi atakami przez pocztę i WWW,
 - b) tworzenia i zarządzania polityką haseł i tożsamości,
 - c) zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
 - d) wykonywania kopii zapasowych oraz tworzenia i utrzymania polityki ciągłości działania.
2. Czynności, o których mowa w ust. 1, mogą zostać objęte finansowaniem wyłącznie w przypadku wykazania przez świadczeniodawcę, wynikiem audytu bezpieczeństwa, zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej.
3. Fundusz dokona weryfikacji zmian poziomu bezpieczeństwa teleinformatycznego świadczeniodawcy na podstawie wypełnionej i złożonej przez niego, przed przystąpieniem do czynności, o których mowa w ust. 1, wynikających z niniejszego zarządzenia, ankiety badającej poziom bezpieczeństwa systemów teleinformatycznych tego świadczeniodawcy, o której mowa w ust. 5, oraz wyniku audytu bezpieczeństwa potwierdzającego zwiększenie poziomu bezpieczeństwa teleinformatycznego u świadczeniodawcy. Ankieta powinna być złożona wraz z wnioskiem o zawarcie umowy zgodnie z ust. 8.

³⁾ <https://cez.gov.pl/pl/page/o-nas/aktualnosci/plan-dzialania-w-zakresie-cyberbezpieczenstwa-w-ochronie-zdrowia>

4. Finansowanie mogą otrzymać świadczeniodawcy spełniający określone w niniejszym zarządzeniu warunki, zgodnie z kolejnością składania spełniających wymogi formalne wniosków, do wyczerpania środków publicznych, o których mowa w ust. 6, którzy złożą oświadczenia o braku finansowania tych samych czynności (w tym zakupów urządzeń, oprogramowania, licencji, usług IT) z jakichkolwiek innych środków publicznych zewnętrznych, w tym krajowych bądź europejskich (wykluczenie podwójnego finansowania).

5. Warunkiem ubiegania się przez świadczeniodawcę o finansowanie jest przeprowadzenie badania poziomu dojrzałości cyberbezpieczeństwa, w formie ankiety w Systemie Statystyki Ochrony Zdrowia przed przystąpieniem do działań mających na celu podniesienie poziomu bezpieczeństwa, finansowych w ramach niniejszego zarządzenia oraz przeprowadzenie audytu bezpieczeństwa zgodnie załącznikiem nr 2 do umowy.

6. Kwota finansowania dla jednego świadczeniodawcy nie może przekroczyć:

1) w przypadku złożenia przez świadczeniodawcę oświadczenia o możliwości odliczenia podatku VAT:

- a) 243 902 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest nie większa niż 10 000 000 zł,
- b) 325 203 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 10 000 000 zł i nie większa niż 100 000 000 zł,
- c) 487 804 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 100 000 000 zł i nie większa niż 500 000 000 zł,
- d) 731 707 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 500 000 000 zł;

2) w przypadku złożenia przez świadczeniodawcę oświadczenia o braku możliwości odliczenia podatku VAT:

- a) 300 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest nie większa niż 10 000 000 zł,
- b) 400 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 10 000 000 zł i nie większa niż 100 000 000 zł,
- c) 600 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 100 000 000 zł i nie większa niż 500 000 000 zł,
- d) 900 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 500 000 000 zł.

7. Koszty audytu bezpieczeństwa nie mogą przekroczyć 10 % wartości faktycznie udzielonego świadczeniodawcy finansowania.

8. W celu uzyskania finansowania, o którym mowa ust. 1, uprawniony świadczeniodawca, składa w terminie do 30 listopada 2022 r. do dyrektora właściwego oddziału Funduszu:

- 1) wniosek o zawarcie umowy na finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, zwany dalej „wnioskiem”, którego wzór określony jest w załączniku nr 1 do zarządzenia;
- 2) wypełnioną ankietę, o której mowa w ust. 3, badającą poziom bezpieczeństwa systemów teleinformatycznych w postaci raportu z Systemu Statystyki Ochrony Zdrowia, o którym mowa w ust. 6, sporządzonego w formacie pdf.

9. W przypadku, gdy świadczeniodawca posiada umowy o udzielanie świadczeń opieki zdrowotnej, o których mowa w § 1 ust. 2, realizowane na obszarze właściwości kilku oddziałów Funduszu, wniosek składa się dyrektora właściwego oddziału Funduszu, z którym została zawarta umowa o najwyższej wartości.

10. Dyrektor właściwego oddziału Funduszu w terminie 7 dni od dnia złożenia wniosku spełniającego warunki formalne, o których mowa w ust. 8, zawiera ze świadczeniodawcą umowę na finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, zwaną dalej „umową”, której wzór określony jest w załącznik nr 2 do zarządzenia.

11. Informacja o wyniku rozpatrzenia wniosku o zawarcie umowy przekazywana jest świadczeniodawcy przez dyrektora właściwego oddziału Funduszu.

12. Wnioski złożone po terminie określonym w ust. 8 pozostawia się bez rozpatrzenia.

13. Warunkiem uzyskania przez świadczeniodawcę środków na finansowanie w wysokości maksymalnej określonej w ust. 6, jest zawarcie umowy i złożenie w siedzibie właściwego oddziału Funduszu nie później niż do 16 grudnia 2022 r. poniższych dokumentów:

- 1) wniosku o wypłatę finansowania, którego wzór określony jest w załączniku nr 3 do zarządzenia;
- 2) specyfikacji finansowania, której wzór określony jest w załączniku nr 4 do zarządzenia;
- 3) potwierdzonych za zgodność z oryginałem kopii dokumentów potwierdzających nabycie i sfinansowanie w okresie od dnia 29 kwietnia 2022 r. do dnia 31 grudnia 2022 roku przedmiotu finansowania, o którym mowa w ust. 1;
- 4) wynik audytu bezpieczeństwa, o którym mowa w ust. 3 i 5.

14. Środki, o których mowa w ust. 6, przekazywane są świadczeniodawcy, na rachunek wskazany w umowie, w terminie 14 dni od dnia złożenia w siedzibie właściwego oddziału Funduszu dokumentów, o których mowa w ust. 12, jednak nie później niż do 31 grudnia 2022 r. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego oddziału Funduszu.

Rozdział 3.

Rozliczenie środków na finansowanie

§ 4. 1. Dyrektor właściwego oddziału Funduszu w terminie do 10. dnia miesiąca następującego po miesiącu, w którym udzielono finansowania świadczeniodawcom na podstawie dokumentów, o których mowa w § 3 ust. 14, przekazuje do Centrali sprawozdanie miesięczne oraz narastająco, od pierwszego miesiąca do końca miesiąca, którego sprawozdanie dotyczy. Wzór sprawozdania określa załącznik nr 6 do zarządzenia.

2. Do sprawozdania, o którym mowa w ust. 1, za październik 2022 r., oddział Funduszu sporządza i przekazuje do Centrali prognozę wydatków na finansowanie działań, o których mowa w § 3 ust. 1 na okres listopad – grudzień 2022 r., sporządzoną na podstawie przewidywanych do poniesienia wydatków według wzoru określonego w załączniku nr 5 do zarządzenia.

3. Centrala Funduszu do 20. dnia miesiąca następującego po miesiącu, którego dotyczy sprawozdanie, o którym mowa w ust. 1, i prognoza, o której mowa w ust. 2, przekazuje na rachunek bankowy oddziału Funduszu środki finansowe w wysokości wynikającej ze złożonych sprawozdań i prognoz.

4. W terminie do dnia 6 stycznia 2023 r. oddział Funduszu sporządza i przekazuje do Centrali sprawozdanie za grudzień 2022 roku.

5. W przypadku niewykorzystania środków, o których mowa w ust. 3, oddział Funduszu dokonuje ich zwrotu w terminie do 6 stycznia 2023 r.

6. W przypadku konieczności dokonania korekty sprawozdania za miesiąc, za który sprawozdanie zostało uznane za sporządzone prawidłowo, korekty dokonuje się w sprawozdaniu sporządzanym w okresie stwierdzenia konieczności dokonania korekty, w części przedstawiającej dane narastające od pierwszego miesiąca do końca miesiąca, którego sprawozdanie dotyczy.

7. Oddział Funduszu zobowiązany jest do prowadzenia wyodrębnionej ewidencji księgowej dla zadania, o którym mowa w zarządzeniu, zgodnie z ustawą z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, z późn. zm.), w sposób umożliwiający identyfikację poszczególnych operacji księgowych w ramach realizacji zadania.

8. Sprawozdania oraz prognozy:

- 1) sprawdza pod względem merytorycznym i podpisuje kierownik Zespołu Bezpieczeństwa Informacji i Ciągłości Działania oddziału Funduszu albo osoba upoważniona przez dyrektora oddziału Funduszu;
- 2) sprawdza pod względem formalno – rachunkowym i podpisuje naczelnik Wydziału Księgowości – główny księgowy oddziału Funduszu albo osoba upoważniona przez dyrektora oddziału Funduszu;
- 3) zatwierdza dyrektor oddziału Funduszu albo osoba przez niego upoważniona

§ 5. 1. Centrala Funduszu, na podstawie sprawozdań oddziałów Funduszu, sporządza sprawozdania łączne, których wzór stanowi załącznik nr 6 do zarządzenia.

2. Informacje zawarte w sprawozdaniach, o którym mowa w ust. 1, wykazuje się odrębnie za miesiąc oraz narastająco.

3. Sprawozdanie, o którym mowa w ust. 1, sporządzone na podstawie danych otrzymanych z oddziałów Funduszu:

- 1) sprawdza pod względem zgodności z danymi przesłanymi z oddziałów wojewódzkich Funduszu i podpisuje kierownik Działu Rozliczeń Międzyoddziałowych i Dotacji Pozyskiwanych z Unii Europejskiej oraz Budżetu Państwa w Biurze Księgowości lub osoba zastępująca;
- 2) sprawdza pod względem merytorycznym i podpisuje dyrektor Biura Bezpieczeństwa Informacji i Ciągłości Działania Centrali Funduszu lub osoba zastępująca;
- 3) sprawdza pod względem formalno–rachunkowym i podpisuje dyrektor Biura Księgowości – Główny Księgowy Centrali Funduszu lub osoba zastępująca;
- 4) zatwierdza Prezes Funduszu lub osoba przez niego upoważniona.

4. Prezes Funduszu przekazuje ministrowi właściwemu do spraw zdrowia sprawozdanie, o którym mowa w ust. 1, w terminie do 20. dnia każdego miesiąca za miesiąc poprzedni.

5. W przypadku konieczności dokonania korekty sprawozdania za miesiąc, za który sprawozdanie zostało uznane za sporządzone prawidłowo, korekty dokonuje się w sprawozdaniu sporządzanym w okresie stwierdzenia konieczności dokonania korekty, w części przedstawiającej dane narastające od pierwszego miesiąca do końca miesiąca, którego sprawozdanie dotyczy.

6. Prezes Funduszu w terminie do 13 stycznia 2023 r. przekazuje ministrowi właściwemu do spraw zdrowia końcowe rozliczenie otrzymanych i wykorzystanych w 2022 r. środków.

7. W przypadku niewykorzystania otrzymanych środków do 31 grudnia 2022 r., Prezes Funduszu zwraca niewykorzystane środki ministrowi właściwemu do spraw zdrowia, w terminie do 13 stycznia 2023 r. Bernar

8. Za datę zwrotu środków, o których mowa w ust. 7, przyjmuje się dzień uznania rachunku ministra właściwego do spraw zdrowia.

§ 6. Zarządzenie wchodzi w życie z dniem następującym po dniu podpisania.

PREZES
NARODOWEGO FUNDUSZU ZDROWIA
Bernard Waśko

wz. Prezesa Narodowego Funduszu Zdrowia
/Dokument podpisano elektronicznie/

Formularz: Ankieta weryfikacji dojrzałości pod kątem cyberbezpieczeństwa

Typ:

Rok: 2021

Dział 1. Ankieta.

W przypadku problemów technicznych (zapomniałam/łam hasła, nie widzę ankiety, coś nie działa w ankiecie) prosimy o zgłoszenia na adres statystyka@cez.gov.pl, lub pod numery telefonów 501 369 856, 501 370 599, 501 368 812, 501 369 795.

W przypadku problemów związanych z merytorycznym wypełnieniem ankiety prosimy o kontakt na adres csirt@cez.gov.pl.

Ankieta weryfikacji dojrzałości pod kątem cyberbezpieczeństwa		
Dane podmiotu		
Nazwa jednostki: Szpital Powiatowy im. PCK	NIP: 8652074945	Kod świadczeniodawcy: 09R/010011
		Numer księgi rejestrowej: 000000010158
Pytania ankietowe		

Zarządzanie (ZA)	Zespół odpowiedzialny za bezpieczeństwo (ZA.1)	W jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych (ZA.1.1)	001	TAK
		W jednostce jest dedykowana osoba odpowiedzialna za bezpieczeństwo fizyczne (ZA.1.2)	002	TAK
		W jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo (ZA.1.3)	003	BRAK
		Osoby odpowiedzialne za cyberbezpieczeństwo, ochronę danych osobowych podlegają bezpośrednio pod kierownika jednostki (ZA.1.4)	004	NIE
	Działania zarządu jednostki (ZA.2)	Dyrektor jednostki odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku (ZA.2.1) Podać datę szkolenia w dolnej części	005	NIE
				Data:
		Dyrektor jednostki cyklicznie przegląda raport oceny ryzyka w jednostce (ZA.2.2)	006	TAK
		Dyrektor jednostki wydał zarządzenie o zintegrowanym systemie zarządzania bezpieczeństwem w jednostce (ZA.2.3)	007	NIE
		Dyrektor jednostki opublikował politykę bezpieczeństwa jednostki z uwzględnieniem cyberbezpieczeństwa (ZA.2.4)	008	NIE

Zarządzanie bezpieczeństwem informacji (SZBI)	Kroki podjęte w celu zapewnienia bezpieczeństwa informacji (SZBI.1)	SZBI.1.1 - konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji jednostki	009	JEST
		SZBI.1.2 - zidentyfikowano cele bezpieczeństwa informacji, określono sposoby ich realizacji oraz przypisano odpowiedzialność za ich realizację	010	JEST
		SZBI.1.3 - działania w zakresie bezpieczeństwa informacji podjęto przed rokiem 2021	011	JEST
		SZBI.1.4 - jednostka opracowała i przyjęła kompleksową politykę bezpieczeństwa informacji (PBI)	012	JEST
		SZBI.1.5 - PBI opracowana w oparciu o właściwe standardy i dobre praktyki	013	JEST
		SZBI.1.6 - ostatni przegląd PBI jednostki przeprowadzono nie wcześniej niż rok temu	014	NIE WIEM
	Zarządzanie (SZBI.2) - Zasady, procedury i procesy zarządzania i monitorowania wyników w zakresie regulacyjnym, prawnym, ryzyka, ochrony środowiska i operacyjnym w organizacji są zrozumiałe i informują o zarządzaniu ryzykiem cyberbezpieczeństwa	SZBI.2.1 - Polityka cyberbezpieczeństwa organizacji jest przekazywana pracownikom w toku okresowych szkoleń stanowiskowych	015	NIE MA
		SZBI.2.2 - zidentyfikowano kluczowe aktywa informacyjne (zbiory danych / systemy / usługi)	016	JEST
		SZBI.2.3 - aktywa zostały uwzględnione w rejestrze ryzyk jednostki	017	JEST
		SZBI.2.4 - Zarządzanie w organizacji oraz zarządzanie ryzykiem odnoszą się do zagrożeń związanych z cyberbezpieczeństwem	018	NIE WIEM
	Szacowanie ryzyka (SZBI.3) - Organizacja rozumie ryzyko cyberbezpieczeństwa dla działalności organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób	SZBI.3.1 - Podatności w zasobach są identyfikowane i dokumentowane	019	NIE
		SZBI.3.2 - w jednostce dokonuje się szacowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji	020	NIE
		SZBI.3.3 - Zagrożenia, zarówno wewnętrzne, jak i zewnętrzne, są identyfikowane i dokumentowane	021	NIE
		SZBI.3.4 - Zagrożenia, podatności, prawdopodobieństwo wystąpienia i skutki są używane do określania ryzyka	022	NIE
		SZBI.3.5 - Odpowiedzi na ryzyko są identyfikowane i priorytetyzowane	023	NIE
	Strategia zarządzania ryzykiem (SZBI.4) - Priorytety, ograniczenia, tolerancja ryzyk i zaradania organizacją są określone i wspierają decyzje dotyczące ryzyka operacyjnego	SZBI.4.1 - Procesy zarządzania ryzykiem są ustanawiane, zarządzane i ugiadniane z dyrektorem jednostki	024	NIE
		SZBI.4.2 - w organizacji wdrożono system oceny ryzyka	025	NIE
	Zarządzanie ryzykiem we współpracy zewnętrznej (SZBI.5) - Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wykorzystywane do wspierania decyzji o ryzyku związanych z zarządzaniem ryzykiem faktyczna dostaw, Organizacja ustanowiła i wdrożyła procesy identyfikacji, szacowania i zarządzania ryzykiem faktyczna dostaw	SZBI.5.1 - Procesy zarządzania ryzykiem cyberbezpieczeństwa są identyfikowane, ustanawiane, oceniane	026	NIE
		SZBI.5.2 - Partnerzy zewnętrzni i dostawcy w zakresie systemów informacyjnych, komponentów i usług są identyfikowani, priorytetyzowani i oceniani za pomocą procesu oceny ryzyka cyberbezpieczeństwa	027	NIE
		SZBI.5.3 - Umowy z dostawcami i partnerami zewnętrznymi są wykorzystywane do wdrażania odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa	028	NIE
		SZBI.5.4 - Dostawcy i partnerzy zewnętrzni są stale oceniani przy użyciu audytów, wyników testów lub innych form oceny w celu potwierdzenia, że wywiązują się ze swoich zobowiązań w zakresie bezpieczeństwa	029	NIE

OCHRONA (OCH)	Zarządzanie tożsamościami, uwierzytelnianie i kontrola dostępu (OCH.1)	OCH.1.1 - W jednostce wdrożono system zarządzania tożsamością i uprawnieniami	030	NIE WIEM
		OCH.1.2 - Ryzykowny dostęp do zasobów jest zarządzany i chroniony	031	NIE WIEM
		OCH.1.3 - Dostęp zdalny jest zarządzany	032	NIE WIEM
		OCH.1.4 - Uprawnienia dostępu i aktywności są zarządzane z uwzględnieniem zasady najniższych uprawnień i rozdzielania obowiązków	033	TAK
		OCH.1.5 - Integralność sieci jest chroniona (np. poprzez segregację sieci czy jej segmentację)	034	NIE
		OCH.1.6 - Weryfikacja dostępu opiera się o MFA (uwierzytelnianie wieloskładnikowe) - jest wykorzystywana aktualnie	035	NIE
	Świadomość i podnoszenie kompetencji (OCH.2)	OCH.2.1 - W jednostce wdrożono system zarządzania tożsamością i uprawnieniami	036	NIE WIEM
		OCH.2.2 - Wykonnicy ze związanymi uprawnieniami rozumieją swoje role i obowiązki	037	NIE WIEM
		OCH.2.3 - Podmioty zewnętrzne (np. dostawcy, klienci, partnerzy) rozumieją swoje role i obowiązki	038	NIE WIEM
		OCH.2.4 - Kierownicy wyższego szczebla rozumieją swoje role i obowiązki	039	NIE WIEM
		OCH.2.5 - Personel cyfrowego bezpieczeństwa oraz bezpieczeństwa fizycznego rozumie swoje role i obowiązki	040	NIE WIEM
	Bezpieczeństwo danych (OCH.3)	OCH.3.1 - Dane w sprawozdaniu są chronione	041	TAK
		OCH.3.2 - Różne dane są chronione	042	NIE
		OCH.3.3 - Zasady są formalnie zarządzane podczas użycia, przechowywania i dysponowania	043	NIE WIEM
		OCH.3.4 - Utrzymywana jest odpowiednia zdolność do zapewnienia ciągłości	044	NIE
		OCH.3.5 - Wdrażane mechanizmy ochrony przed wyciekami danych	045	NIE
	Bezpieczeństwo kopii zapasowych, Plan reagowania na zagrożenia (OCH.4)	OCH.4.1 - Kopie zapasowe informacji są przechowywane, przechowywane i testowane	046	NIE
		OCH.4.2 - Dostęp do kopii zapasowych jest dodatkowo chroniony	047	NIE WIEM
		OCH.4.3 - Dane są niszczone zgodnie z funkcjonującymi politykami	048	TAK
		OCH.4.4 - Opracowano plan bieżącego i odnowienia kopii zapasowych	049	NIE
		OCH.4.5 - Organizacja posiada i zarządza planami reagowania (w zakresie reagowania na incydenty i ciągłości działania) oraz planami odzyskiwania (w zakresie odzyskiwania po incydencie i powodzi)	050	NIE
		OCH.4.6 - Plan reagowania i odzyskiwania są weryfikowane i testowane	051	NIE
		OCH.4.7 - Opracowano i wdrożono plan zarządzania podatkością	052	NIE
	Technologia ochronna (OCH.5)	OCH.5.1 - Zapisy logów/inspekcji są określone, dokumentowane, wdrażane i sprawdzane zgodnie z politykami	053	NIE
		OCH.5.2 - Nosniki wymienne są chronione, a ich stosowanie ograniczone zgodnie z politykami	054	NIE
		OCH.5.3 - Zasady najmniejszej funkcjonalności jest wdrożona poprzez odpowiednią konfigurację systemów tak, by posiadały tylko niezbędne możliwości	055	NIE WIEM
		OCH.5.4 - Łączyma komunikacyjne do Internetu są chronione (AnyDoS, inne)	056	NIE WIEM
		OCH.5.5 - Odpowiednie mechanizmy (jak np. fail-safe, równoważenie obciążenia, interakcje) wdrażane w celu odciążenia wymagających odpowiedni w normalnych i niekorzystnych sytuacjach	057	NIE WIEM

Zdarzenia i monitoring(CM)	Anomalie i zdarzenia (CM.1)	CM.1.1 - Wykryte zdarzenia są analizowane aby zrozumieć cele i metody ataku	058	NIE
		CM.1.2- Dane o zdarzeniach są pozyskiwane oraz korelowane z wielu źródeł i czujników	059	NIE
	Ciągłe monitorowanie bezpieczeństwa (CM.2)	CM.2.1 - Sieć jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa. (SIEM)	060	NIE
		CM.2.2 - Środowisko fizyczne jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa	061	NIE
		CM.2.3 - Aktywność personelu jest monitorowana w celu wykrycia potencjalnych zdarzeń związanych z cyberbezpieczeństwem	062	NIE
		CM.2.4 - Złośliwy kod jest wykrywany	063	NIE
		CM.2.5 - Nieautoryzowany kod mobilny jest wykrywany (np. ActiveX, JavaScript)	064	NIE
		CM.2.6 - Aktywność zewnętrznego dostawcy usług jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa	065	NIE
		CM.2.7 - Przeprowadza się monitorowanie pod kątem nieautoryzowanego personelu, połączeń, urządzeń i oprogramowania	066	NIE
		CM.2.8 - Przeprowadza się skanowanie podatności	067	NIE
REAGOWANIE (RE)	Planowanie reagowania (RE)	RE.1 - Plan reagowania jest realizowany w trakcie lub po incydencie	068	NIE WIEM
	Komunikacja (KO)	KO.1 - Personel zna swoje role i kolejność operacji, na wypadek konieczności reagowania	069	NIE WIEM
		KO.2 - Incydenty są zgłaszane zgodnie z ustalonymi kryteriami	070	NIE WIEM
		KO.3 - Informacje są udostępniane zgodnie z planami reagowania	071	NIE WIEM
		KO.4 - Koordynacja z zainteresowanymi stronami jest prowadzona w sposób zgodny z planami reagowania	072	NIE WIEM
		KO.5 - Dobrowolna wymiana informacji z zewnętrznymi podmiotami jest prowadzona w celu osiągnięcia szerszej świadomości sytuacyjnej w zakresie cyberbezpieczeństwa	073	NIE WIEM
	Mitygacja (MI)	MI.1 - Incydenty są opanowywane	074	NIE WIEM
		MI.2 - Incydenty są mitygowane	075	NIE WIEM
		MI.3 - Nowo zidentyfikowane podatności są mitygowane lub dokumentuje się akceptację ryzyka związanego z nimi	076	NIE WIEM
	Udoskonalanie (UD)	UD.1 - Plany reagowania uwzględniają wyciągnięte wnioski	077	NIE WIEM
		UD.2 - Strategie reagowania są aktualizowane	078	NIE WIEM
ODTWARZANIE (OD)	Planowanie odtwarzania (OD.1)	OD.1.1 - Plan odtwarzania jest realizowany w trakcie lub po incydencie cyberbezpieczeństwa	079	NIE WIEM
	Aktualizacja (OD.2)	OD.2.1 - Plany odtwarzania zawierają wyciągnięte dotychczas wnioski	080	NIE WIEM
		OD.2.2 - Strategie odtwarzania są aktualizowane	081	NIE WIEM

INFRASTRUKTURA (IN)	Sieć LAN (IN.1)	IN.1.1 przełączniki klasy enterprise, wsparcie	082	NIE WIEM
		IN.1.2 segmentacja sieci	083	NIE
	Ochrona brzegowa (IN.2)	IN.2.1 Firewall klasy enterprise, aktualne wsparcie, aktualizacje na bieżąco	084	NIE WIEM
		IN.2.2 połączenia VPN oraz certyfikaty dla wszystkich użytkowników	085	NIE
	Poczta (IN.3)	IN.3.1 serwer poczty	086	NIE
		IN.3.2 wdrożony SANBOX	087	NIE
		IN.3.3 wdrożony MFA dla wszystkich użytkowników usług pocztowych i aktualnie wykorzystywany	088	NIE
	Wirtualizacja (IN.4)	IN.4.1 serwery wirtualne	089	TAK
		IN.4.2 wsparcie i aktualizacje	090	NIE WIEM
	Kopia zapasowa (IN.5)	IN.5.1 Kopia odmiejszczona	091	NIE
		IN.5.2 Napęd taśmowy (biblioteka taśmowa)	092	TAK
		IN.5.3 System kopii zapasowej izolowany od środowisk produkcyjnych	093	NIE
	Systemy bezpieczeństwa (IN.6)	IN.6.1 SIEM	094	NIE
		IN.6.2 DLP	095	NIE WIEM
		IN.6.3 NAC	096	NIE
		IN.6.4 WAF	097	NIE WIEM
		IN.6.5 DAM	098	NIE
		IN.6.6 EDR	099	NIE
		IN.6.7 DNS Protection	100	NIE
		IN.6.8 IPS/IDS	101	TAK
		IN.6.9 Antyvirus	102	TAK
		IN.6.10 SOC	103	NIE
	Urządzenia specjalizowane (IN.7)	IN.7.1 Tomograf komputerowy	104	TAK
		IN.7.2 Urządzenia do rezonansu magnetycznego	105	NIE
		IN.7.3 Cyfrowe urządzenia RTG	106	TAK
		IN.7.4 Kardiomonitor	107	TAK
		IN.7.5 Audiografy	108	NIE
		IN.7.6 Pompy infuzyjne	109	TAK

Telekomunikacja	typ łącza telekomunikacyjnego	110	1)Dzierżawione światłowodowe symetryczne
	przepustowość (w przypadku łącz niesymetrycznych suma download + upload)	111	6) od 10 do 99,9 Mbps
	Usługa AntiDDoS	112	NIE MA
	firewall dostarczony przez operatora i prze operatora zarządzany	113	NIE MA
	firmowe telefony komórkowe	114	TAK
	telefonii VoIP wewnątrz jednostki	115	JEST
	łącze głosowe	116	99) NIE WIEM
	łącze głosowe awaryjne, niezależne od zasilania lokalnego	117	4) NIE MA
	centralika telefoniczna	118	5) stacjonarna cyfrowa z obsługą ISDN PRA, ISDN
Zasilanie Awaryjne	UPS na stanowisku roboczym	119	na wybranych
	Wszystkie serwerownie zasilane z UPS w czasie rozruchu generatora	120	TAK
	Wszystkie serwery z zasilaczami redundantnymi	121	TAK
	Generator awaryjny na potrzeby wszystkich serwerowni i intensywnej terapii	122	TAK
	SZR załączający generator awaryjny w trakcie pracy na UPS	123	NIE WIEM
	Zatankowany zbiornik paliwa wystarczy na	124	1) do 12 h
	Zasilanie jednostki z dwóch stacji transformatorowych SN/NN	125	TAK
	Awaryjne zasilanie we wszystkich serwerowniach	126	NIE WIEM

