

Ogłoszenie o zamówieniu
Dostawy
Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla
Pałuckiego Centrum Zdrowia Sp. z o.o. w Żninie

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: PAŁUCKIE CENTRUM ZDROWIA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

1.4) Krajowy Numer Identyfikacyjny: REGON 093213309

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Szpitalna 30

1.5.2.) Miejscowość: Żnin

1.5.3.) Kod pocztowy: 88-400

1.5.4.) Województwo: kujawsko-pomorskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL617 - Inowrocławski

1.5.9.) Adres poczty elektronicznej: zamowienia@szpitalznin.pl

1.5.10.) Adres strony internetowej zamawiającego: <http://szpitalznin.pl/>

1.6.) Rodzaj zamawiającego: Zamawiający publiczny - osoba prawna, o której mowa w art. 4 pkt 3 ustawy (podmiot prawa publicznego)

1.7.) Przedmiot działalności zamawiającego: Zdrowie

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Pałuckiego Centrum Zdrowia Sp. z o.o. w Żninie

2.4.) Identyfikator postępowania: ocids-148610-07b7d921-40b9-11ed-9171-f6b7c7d59353

2.5.) Numer ogłoszenia: 2022/BZP 00372827/01

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2022-09-30 14:45

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Nie

2.11.) O udzielenie zamówienia mogą ubiegać się wyłącznie wykonawcy, o których mowa w art. 94 ustawy: Nie

2.14.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Nie

2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną

Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA

3.1.) Adres strony internetowej prowadzonego postępowania

<https://platformazakupowa.pl/pn/szpitalznin>

3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia: Nie

3.4.) Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej: Tak

3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej: Postępowanie prowadzone jest w języku polskim za pośrednictwem platformazakupowa.pl pod adresem: <https://platformazakupowa.pl/pn/szpitalznin>

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: -Zamawiający będzie przekazywał wykonawcom informacje za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji "Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.

-Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.

-W wyjątkowych sytuacjach awaryjnych np. w przypadku braku działania <https://platformazakupowa.pl/pn/szpitalznin>. Zamawiający może również komunikować się z wykonawcami za pomocą poczty elektronicznej (adres: zamowienia@szpitalznin.pl). Wykonawca na żądanie Zamawiającego niezwłocznie potwierdza fakt ich otrzymania. W przypadku nie potwierdzenia ze strony Wykonawcy odbioru przesłanych informacji (pomimo takiego żądania), Zamawiający uzna, że wiadomość została mu doręczona w sposób umożliwiający Wykonawcy zapoznanie się z treścią pism.

-Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 31 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.: a. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s, b. komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje, c. zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10.0, d. włączona obsługa JavaScript, e. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf, f. Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.

g. Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

Wymagania techniczne i organizacyjne dot. korespondencji elektronicznej zawarte są w Rozdziale XI i XIV SWZ.

3.8.) Zamawiający wymaga sporządzenia i przedstawienia ofert przy użyciu narzędzi elektronicznego modelowania danych budowlanych lub innych podobnych narzędzi, które nie są ogólnie dostępne: Nie

3.12.) Oferta - katalog elektroniczny: Nie dotyczy

3.14.) Języki, w jakich mogą być sporządzane dokumenty składane w postępowaniu:

polski

3.15.) RODO (obowiązek informacyjny): 1.Zgodnie z art. 13 i 14 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 „RODO”, informuję, że: – Administratorem danych osobowych jest Pałuckie Centrum Zdrowia Sp. z o. o. – ul. Szpitalna 30, 88-400 Żnin

2. We wszystkich sprawach związanych z przetwarzaniem i ochroną Pani/Pana danych osobowych może się Pani/Pan z nami kontaktować przez Inspektora Ochrony Danych Osobowych Pana Tomasza Powalę tel: 503 585 225, poczta elektroniczna iod@szpitalznin.pl

3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego.

4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art.18 ust 5 pkt. 1 i 2 oraz art. 74 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (t.j. Dz.U. z 2021 r. poz. 1129 z późn. zm.), dalej „ustawa Pzp”;

5. Dane osobowe zgromadzone w ramach postępowania o udzielenia zamówienia będą przechowywane przez okres 5 lat licząc w pełnych latach kalendarzowych, poczynając od dnia 1 stycznia roku następującego po zakończeniu danego postępowania

6. Podanie danych osobowych w związku udziałem w postępowaniu o zamówienia publiczne nie jest obowiązkowe, ale jest warunkiem niezbędnym do wzięcia w nim udziału.

Konsekwencją nie podania danych osobowych może być nieważność oferty w postępowaniu i niemożność zawarcia umowy, co wynika z przepisów ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (t.j. Dz.U. z 2021 r. poz. 1129 z późn. zm.) oraz wydanych do niej przepisów wykonawczych, a w szczególności na podstawie Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 roku w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz.U. z 2020 r. poz. 2415);

7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

8. Posiada Pani/Pan:na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych**;

na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem

przypadków, o których mowa w art. 18 ust. 2 RODO ***;
 prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
 9 .Nie przysługuje Pani/Panu:w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.

4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe: Nie

4.1.2.) Numer referencyjny: PCZ/II-ZP/16/2021

4.1.3.) Rodzaj zamówienia: Dostawy

4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.1.8.) Możliwe jest składanie ofert częściowych: Nie

4.1.13.) Zamawiający uwzględni aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia: Nie

4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:

4.2.2.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa do siedziby Zamawiającego oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych wraz z wykonaniem usług podnoszących bezpieczeństwo systemów IT w ramach środków pochodzących z Funduszu Przeciwdziałania COVID-19 – podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców (Zarządzenie nr 68/2022/BIIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022r.), w tym:

1. Wykonanie diagnozy cyberbezpieczeństwa
2. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
3. Wykonanie audytu bezpieczeństwa
4. Przeprowadzenie szkolenia
5. Dostawa Systemu ochrony klasy GRC (Governance, risk management and compliance)
6. Dostawa systemu SIEM (security information and event management)
7. Dostawa zapory sieciowej sprzętowej Firewall Next Generation Firewall)
8. Wykonane instalacji i konfiguracji zapory sieciowej (Next Generation Firewall)
9. Dostawa oprogramowania antywirusowego
10. Dostawa serwer NAS – Network Attached Storage
11. Dostawa zasilacza awaryjnego UPS
12. Dostawa oprogramowania do backupu
13. Dostawa oprogramowania do wizualizacji
14. Wykonanie usług w zakresie instalacji i konfiguracji dostarczonego sprzętu i oprogramowania

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

- 30230000-0 - Sprzęt związany z komputerami
- 48000000-8 - Pakiety oprogramowania i systemy informatyczne
- 48761000-0 - Pakiety oprogramowania antywirusowego
- 48732000-8 - Pakiety oprogramowania do zabezpieczania danych
- 72810000-1 - Usługi audytu komputerowego
- 72317000-0 - Usługi przechowywania danych

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2022-11-28

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.3.) Kryteria oceny ofert**4.3.1.) Sposób oceny ofert:** Przy wyborze ofert Zamawiający kierować się będzie kryteriami:

- cena - 100%

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo**4.3.3.) Stosowane kryteria oceny ofert:** Wyłącznie kryterium ceny**Kryterium 1****4.3.5.) Nazwa kryterium:** Cena**4.3.6.) Waga:** 100**4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert:** Nie**SEKCJA V - KWALIFIKACJA WYKONAWCÓW****5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia:** Nie**5.3.) Warunki udziału w postępowaniu:** Tak**5.4.) Nazwa i opis warunków udziału w postępowaniu.**

4) zdolności technicznej i zawodowej

Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że:

4.1) posiada wiedzę i doświadczenie niezbędne do wykonywania przedmiotu zamówienia, tj.:

1. W okresie ostatnich 3 lat przed upływem terminu składania ofert a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie co najmniej 2 usługi polegające na opracowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości działania, w skład której wchodzi kompletna dokumentacja Bezpieczeństwa Informacji i Ciągłości działania

o wartości nie mniejszej niż 40 000 PLN netto.

2. W okresie ostatnich 3 lat przed upływem terminu składania ofert a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie co najmniej 1 usługę polegającą na opracowaniu dokumentacji bezpieczeństwa informacji i ciągłości działania, w tym postępowania w sytuacjach kryzysowych w organizacji zatrudniającej nie mniej niż 150 osób.

3. Posiada certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2021 r. poz. 514 z późn. zm.), w zakresie certyfikacji osób

4. Posiada 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 (t.j. Dz.U. z 2021 r., poz. 514 z późn. zm.), w zakresie certyfikacji osób, lub równoważny.

5. Przeprowadził w okresie ostatnich trzech lat szkolenia:

- co najmniej 3 akredytowane szkolenia audytorów wiodących systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub,

- co najmniej 3 akredytowane szkolenia Audytora bezpieczeństwa informacji ISO 27001 lub,

- co najmniej 3 akredytowane szkolenia Managera bezpieczeństwa informacji ISO 27001.

4.2) Spełnia wymagania do przeprowadzenia Audytu bezpieczeństwa, tj.:

1. Zamawiający uzna spełnienie warunku, jeżeli Wykonawca wykaże, że posiada akredytację zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (tj. Dz. U. 2022, r. poz. 5, 974), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2. Zamawiający uzna spełnienie warunku, jeżeli Wykonawca wykaże, że dysponuje osobami zdolnymi do wykonania zamówienia (kadra), tj.: co najmniej dwoma audytorami posiadającymi:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu staowiącego przedmiot zamówienia:

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

- 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 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.

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.

4.3 Wykonawca posiada co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymuje 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.

Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, uważa się udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów

w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

o przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;

o przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;

o przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r., poz. 2070 z późn. zm.);

o wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r.

o kontroli w administracji rządowej (t.j. Dz. U. z 2020 r., poz. 224 z późn. zm.);

o wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (t.j. Dz. U. z 2020 r. poz. 1200 z późn. zm.).

Wykonawca spełnia wymagania określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r., poz. 1999).

5.5.) Zamawiający wymaga złożenia oświadczenia, o którym mowa w art.125 ust. 1 ustawy: Tak

5.6.) Wykaz podmiotowych środków dowodowych na potwierdzenie niepodlegania wykluczeniu: 9. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że:

wniosek o dopuszczenie do udziału w postępowaniu albo oferta Wykonawcy podlegają odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub

zachodzą przesłanki unieważnienia postępowania.

a) Jeżeli złożone przez Wykonawcę oświadczenie, o którym mowa w art. 125 ust. 1 uPzp lub podmiotowe środki dowodowe budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełnienia przez Wykonawcę warunków udziału w postępowaniu lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.

b) W przypadku przekazywania przez Wykonawcę dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie kwalifikowanym podpisem elektronicznym pliku zawierającego skompresowane dane jest równoznaczne z poświadczeniem przez Wykonawcę za zgodność z oryginałem wszystkich elektronicznych kopii dokumentów zawartych w tym pliku, z wyjątkiem kopii poświadczonych odpowiednio przez innego Wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot na którego zdolnościach lub sytuacji polega Wykonawca, albo przez podwykonawcę, albo przez gwaranta wadium.

c) Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

d) W zakresie nie uregulowanym w SWZ, zastosowanie mają przepisy rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy (Dz. U. 2020 poz. 2415).

5.7.) Wykaz podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu: a)

Oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej – załącznik nr 5 do SWZ;

b) Wykaz usług wykonanych w okresie ostatnich 3 lat polegających na wykonaniu należytych co najmniej dwóch usług opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości działania w skład którego wchodzi kompletna

dokumentacja Bezpieczeństwa Informacji i Ciągłości działania o wartości nie mniejszej niż 40 000 PLN netto, oraz co najmniej dwóch usług opracowania dokumentacji bezpieczeństwa informacji i ciągłości działania, w tym postępowania w sytuacjach kryzysowych w organizacji zatrudniającej nie mniej niż 150 osób. Dla w/w usług należy wskazać daty wykonania usługi i podmioty, na rzecz których usługi zostały wykonane, oraz załączyć dowody określające, czy te usługi zostały wykonane należycie. Dowodami, o których mowa, są referencje sporządzone przez podmiot, na rzecz którego usługi zostały wykonane – załącznik nr 6 do SWZ;

c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2021 r. poz. 514 z późn. zm.), w zakresie certyfikacji osób .

d) 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 (t.j. Dz.U. z 2021 r., poz. 514 z późn. zm.), w zakresie certyfikacji osób, lub równoważny.

e) Oświadczenie Wykonawcy – potwierdzające przeprowadzenie w przeciągu ostatnich trzech lat szkolenia, tj.:

- co najmniej 3 akredytowane szkolenia audytorów wiodących systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub,

- co najmniej 3 akredytowane szkolenia Audytora bezpieczeństwa informacji ISO 27001 lub,

- co najmniej 3 akredytowane szkolenia Managera bezpieczeństwa informacji ISO 27001.

f) Wymagane dokumenty, certyfikaty wraz z wykazem osób, które będą uczestniczyć w wykonywaniu zamówienia , zgodnie z rozdz. VI, ust.2 pkt.4.2 SWZ – Załącznik nr 7 do SWZ

g) Oświadczenie Wykonawcy, dotyczące praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych, zgodnie z rozdz. VI, ust.2 pkt.4.2).

5.9.) Zamawiający przewiduje uzupełnienie przedmiotowych środków dowodowych: Nie

SEKCJA VI - WARUNKI ZAMÓWIENIA

6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe: Nie

6.3.) Zamawiający przewiduje aukcję elektroniczną: Nie

6.4.) Zamawiający wymaga wadium: Nie

6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Nie

6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:

W przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, do oferty należy załączyć pełnomocnictwo do reprezentowania ich w postępowaniu

o udzielenie zamówienia publicznego albo do reprezentowania ich w postępowaniu i do zawarcia umowy w sprawie zamówienia publicznego

Pełnomocnictwo powinno dokładnie określać zakres umocowania, w tym ewentualnie prawo do udzielenia dalszych pełnomocnictw. Wszystkie pełnomocnictwa składane wraz z ofertą muszą być złożone w postaci elektronicznej opatrzone podpisem elektronicznym lub jeśli zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa powyżej, może dokonać również notariusz.

W przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, do oferty należy załączyć oświadczenie Wykonawców wspólnie ubiegających się o zamówienie, z którego wynika, które dostawy, usługi, wykonają poszczególni Wykonawcy – Załącznik nr 10 do SWZ.

6.7.) Zamawiający przewiduje unieważnienie postępowania, jeśli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały przyznane: Tak

SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY

7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie

7.3.) Zamawiający przewiduje zmiany umowy: Tak

7.4.) Rodzaj i zakres zmian umowy oraz warunki ich wprowadzenia:

O ile Umowa nie stanowi inaczej, zmiany treści Umowy mogą być dokonywane wyłącznie w formie aneksu podpisanego przez obie Strony, pod rygorem nieważności w zakresie:

1) zmiany szczegółowych zasad wykonywania przedmiotu Umowy określonych

w załącznikach do Umowy, spowodowane zmianami organizacyjnymi u Zamawiającego;

2) zmiany zakresu realizacji Przedmiotu Umowy, w przypadku wystąpienia zmiany okoliczności powodującej, że:

a) realizacja części Przedmiotu Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawierania Umowy,

b) realizacja części Przedmiotu Umowy nie jest zasadna na skutek zmiany lub planowanej zmiany powszechnie obowiązujących przepisów prawa.

3) zmiany postanowień Umowy będące następstwem zmian powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy i z których treści wynika konieczność lub zasadność wprowadzenia zmian postanowień Umowy;

powyższa zmiana dotyczy także zmiany postanowień Umowy w związku ze zmianą przepisów dotyczących ochrony danych osobowych, w szczególności w zakresie obowiązku spełniania przez Wykonawcę wymagań określonych przez Zamawiającego, poddania się kontroli oraz odstąpienia od Umowy przez Zamawiającego w związku z nieprzestrzeganiem przez Wykonawcę obowiązków związanych z ochroną danych osobowych lub poddaniu się kontroli;

4) zmiany terminu wykonania Umowy spowodowane zmianą powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy;

5) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest konieczna w celu prawidłowego wykonania Przedmiotu Umowy;

6) niezbędna jest zmiana terminu realizacji Umowy w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które obie Strony nie miały wpływu. W takim przypadku termin realizacji umowy zostanie odpowiednio wydłużony o czas trwania przyczyny uniemożliwiającej realizację Umowy;

7.5.) Zamawiający uwzględnił aspekty społeczne, środowiskowe, innowacyjne lub etykiety związane z realizacją zamówienia: Nie

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2022-10-10 08:00

8.2.) Miejsce składania ofert: Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: <https://platformazakupowa.pl/pn/szpitalznin>

8.3.) Termin otwarcia ofert: 2022-10-10 08:30

8.4.) Termin związania ofertą: 30 dni