Wojewódzki Szpital Rehabilitacyjny
dla Dzieci w Ameryce
Ameryka 21, 11-015 Olsztynek, tel. 089/519 48 23, fax. 089/519 48 13
e-mail: szpital@ameryka.com.pl www.ameryka.com.pl

Ameryka, dn. 09.12.2024 r.

ZAPYTANIE OFERTOWE nr 7/2024

na przeprowadzenie Audytu cyberbezpieczeństwa w Wojewódzkim Szpitalu Rehabilitacyjnym dla Dzieci w Ameryce.

1. Zamawiający:
Wojewódzki Szpital Rehabilitacyjny dla Dzieci w Ameryce, Ameryka 21, 11-015 Olsztynek NIP: 739-29-54-381 **REGON:** 000296236
strona internetowa: www.ameryka.com.pl
e-mail: szpital@ameryka.com.pl
godziny otwarcia: 7^{00} - 14^{35}
Telefon/fax: 89/519-48-23/13

2. Opis przedmiotu zamówienia:

1. Przeprowadzenie audytu cyberbezpieczeństwa w Wojewódzkim Szpitalu Rehabilitacyjnym dla Dzieci w Ameryce. Wnioski z raportu na zakończenie audytu winny uwzględniać opisy działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Zamawiającego. Audyt bezpieczeństwa winien być przeprowadzony zgodnie z Wytycznymi CeZ (zapewniający adekwatny poziom cyberbezpieczeństwa ochrony prywatności w zakresie rodzaju wdrożonych usług i rodzaju przetwarzanych danych). Raport musi zawierać jasne stanowisko audytora w zakresie spełnienia wymogów w obszarze cyberbezpieczeństwa wymienionych w dokumencie p.n. „Karta z definicjami kryteriów wyboru projektów dla Priorytetu 01 Gospodarka, Działania 1.7 E-zdrowie" w ramach programu Fundusze Europejskie dla Warmii i Mazur 2021-2027 ze środków Europejskiego Funduszu Rozwoju Regionalnego" w ramach naboru nr FEWM.01.07-IZ.00-001/24
2. Minimalny zakres:
   a) wykonanie zewnętrznych skanów podatności, które wykażą brak podatności krytycznych oraz które mogą doprowadzić do incydentu poważnego w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
   Po wykryciu podatności krytycznych zamawiający ma 2 tygodnie na ich usunięcie, a oferent ma ponownie wykonać audyt w tym zakresie, aż wszystkie luki krytyczne zostaną usunięte.

b) audyt systemu poczty elektronicznej , którego wynik potwierdzi skuteczność wdrożenia SPF, DMARK, DKIM , antyspam oraz ochronę antywirusową.

SPF, czyli Sender Policy Framework, to rodzaj rekordu dla domeny, który działa w ramach usługi DNS (strefy domeny). Jest on odpowiedzialny przede wszystkim za poprawną identyfikację serwera pocztowego, uprawnionego do wysyłania poczty elektronicznej w imieniu danej domeny

DMARC to **protokół uwierzytelniania poczty elektronicznej**, który pozwala właścicielom domen pocztowych określić, jakich mechanizmów używają do uwierzytelniania swoich wiadomości e-mail oraz w jaki sposób serwery pocztowe otrzymujące wiadomości z ich domeny powinny obsługiwać niepowodzenia uwierzytelniania.

DKIM to skrót od DomainKeys Identified Mail. Jest to metoda uwierzytelniania wiadomości e-mail, która pozwala nadawcom zapobiegać zmianie treści wiadomości e-mail podczas procesu dostarczania.

c) audyt systemu kopii zapasowej, którego wynik potwierdzi utworzenie odmiejscowionej kopii zapasowej i odtworzenie z niej kompletnego systemu oraz wykonanej dokumentacji bezpieczeństwa

d) audyt systemu Endpoint Detection and Response zainstalowanego na wszystkich stacjach roboczych oraz serwerach, potwierdzającego prawidłowość wdrożenia systemu. Po wykryciu podatności krytycznych zamawiający ma 2 tygodnie na ich usunięcie, a oferent ma ponownie wykonać audyt w tym zakresie, aż wszystkie luki krytyczne zostaną usunięte.

e) przeprowadzenie skanów podatności oraz testów penetracyjnych wewnętrznych systemów usługodawców, w tym przeprowadzone konfiguracje, mające na celu usunięcie wykrytych podatności (utwardzanie systemów)

3. Termin realizacji zamówienia:

Wykonawca jest zobowiązany wykonać audyt w terminie: **01- 31.12.2026 r.**

4. O udzielenie niniejszego zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki, dotyczące:

1. Audyt bezpieczeństwa, musi 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) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub

b) 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.

c) co najmniej dwie wystawione referencje potwierdzające wykonanie audytów cyberbezpieczeństwa.

2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1) Certified Internal Auditor (CIA).
2) Certified Information System Auditor (CISA).
3) 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.
4) 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.
5) Certified Information Security Manager (CISM).
6) Certified in Risk and Information Systems Control (CRISC).
7) Certified in the Governance of Enterprise IT (CGEIT).
8) Certified Information Systems Security Professional (CISSP).
9) Systems Security Certified Practitioner (SSCP).
10) Certified Reliability Professional.
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

3. Minimalny zakres audytu powinien obejmować:

Nazwa obszaru	Opis
Skuteczność działania infrastruktury	– 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
Procesy zarządzania bezpieczeństwem informacji	– Nośniki wymienne – udokumentowany sposób podstępowania – Zarządzanie tożsamością / dostęp do systemów w zakresie: o Przydzielanie dostępu o Odbieranie dostępu – Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję OUK (Dz.U. 2019 poz. 2479)
Monitorowanie i reagowanie na incydenty bezpieczeństwa	– 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
Zarządzanie ciągłością działania	– 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
Utrzymanie systemów informacyjnych	– Harmonogramy skanowania podatności – Aktualny status realizacji postępowania z podatnościami – Procedury związane ze z identyfikowaniem (wykryciem) podatności – Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami
Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	– Polityka bezpieczeństwa w relacjach z dostawcami – Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa – Dostęp zdalny – Metody uwierzytelnienia

Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

5. Informacje o dokumentach, jakie mają dostarczyć Wykonawcy.

1. W celu potwierdzenia wymaganych wyżej warunków wraz z ofertą należy dostarczyć:

1) dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu,
2) referencje potwierdzające prawidłowe wykonanie audytu.

6. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

7. Osoby upoważnione do kontaktowania się z Wykonawcami:

Osobą upoważnioną ze strony Zamawiającego do kontaktowania się z Wykonawcami jest Leszek Chmielewski:
89/519-48-68, l.chmielewski@ameryka.com.pl

8. Kryterium oceny ofert:

1. Za najkorzystniejszą ofertę zostanie uznana oferta spełniająca wszystkie wymogi zawarte w Zapytaniu oraz ta, która uzyska najkorzystniejszy bilans przyznanych punktów, tj.:

$$\text{Liczba punktów danej oferty} = \frac{\text{cena najtańszej oferty brutto}}{\text{cena badanej oferty brutto}} \times 100\% \times 100$$

1) Cena oferty musi zawierać wszystkie koszty związane z prawidłową realizacją zamówienia.

2) Cenę oferty stanowi cena brutto.
3) Cena oferty musi być wyrażona w polskich złotych.

4) Zamawiający dopuszcza zmianę ceny jednostkowej brutto w sytuacji zmiany stawki podatku VAT

5) Jeżeli do niniejszego Zapytania zostaną złożone oferty o takiej samej cenie, to Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia ofert dodatkowych, w terminie 3 dni roboczych od daty otrzymania powiadomienia.

9. Termin złożenia oferty cenowej i jej otwarcia

1. Ofertę należy przesłać drogą elektroniczną przez platformę zakupową: https://platformazakupowa.pl/pn/szpital_ameryka do dnia **16.12.2024 r.**, do godz. **10:00**.
2. Decydujące znaczenie dla oceny zachowania terminu ma data i godzina wpływu oferty.
3. Oferty otrzymane po terminie nie będą rozpatrywane.
4. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych oferty.
5. Otwarcie ofert nastąpi w dniu **16.12.2024 r.**, o godz. **10:15**.

10. Zamawiający zastrzega sobie prawo przedłużenia terminu składania ofert bez podawania przyczyn.

11. Zamawiający zastrzega sobie prawo niewybrania oferenta.

12. Załączniki:

1. Załącznik nr 1 – formularz ofertowy,
2. Załącznik nr 2 – projekt umowy.

13. Informacje dodatkowe:

1. Oferta powinna być sporządzona w formie pisemnej, w języku polskim.

   Ofertę należy przygotować na dokumentach załączonych do niniejszego Zapytania.
2. W załącznikach winny być wypełnione wszystkie pozycje.
3. Każdy Wykonawca może złożyć tylko jedną ofertę.
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym.
5. Niniejsze Zapytanie nie podlega przepisom Ustawy z dnia 11 września 2019 r. Prawo zamówień Publicznych.
6.

14. Klauzula informacyjna z art. 13 RODO do zastosowania przez Zamawiających w celu związanym z Zapytaniem ofertowym:

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 „RODO", Zamawiający informuje, że:

1. administratorem Pani/Pana danych osobowych jest: Wojewódzki Szpital Rehabilitacyjny dla Dzieci w Ameryce, Ameryka 21, 11-015 Olsztynek, dane kontaktowe: mail szpital@ameryka.com.pl, tel. 89/ 519-48-23, faks 89/519-48-13;
2. Inspektorem ochrony danych osobowych jest Pani Marzena Grabowska- Pycko, tel. 507-106-511;
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym Zapytaniem ofertowym;
4. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja;
5. Pani/Pana dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia;
6. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach związanych z udziałem w Zapytaniu ofertowym;
7. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
8. posiada Pani/Pan:
   1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
   3) 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;
   4) 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:
   1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   2) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   3) 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.

Z upoważnienia Dyrektora,

Kierownik
Działu Administracyjno-Gospodarczego
mgr Grzegorz Tomaszewski