



Choroszcz, dn. 21.06.2022r.

Nr sprawy: SZP 3820 – 25/22

**Zapytanie ofertowe dla zamówienia publicznego o wartości mniejszej niż 130 000 złotych
na podstawie art. 2 ust. 1 pkt. 1 ustawy Prawo zamówień publicznych
(t.j. Dz. U. 2021 poz. 1129 z póź. zm.)**

1. **Zamawiający:** Samodzielny Publiczny Psychiatryczny Zakład Opieki Zdrowotnej im. dr. Stanisława Deresza w Choroszczu ul. Plac Z. Brodowicza 1 16-070 Choroszcz zaprasza do udziału w zapytaniu ofertowym na **wykonanie audytu bezpieczeństwa dla potrzeb Samodzielnego Publicznego Psychiatrycznego Zakładu Opieki Zdrowotnej w Choroszczu.**
2. Przedmiot umowy:
 - 1) Celem audytu jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety.
 - 2) Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak.
 - 3) Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.
 - 4) Opis działań:

Nazwa obszaru	Opis działań skutkujących podniesieniu poziomem bezpieczeństwa teleinformatycznego u świadczeniodawców
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 postępowania -Zarządzanie tożsamością / dostęp do systemów w zakresie: -- Przydzielanie dostępu -- Odbieranie dostępu
Monitorowanie i reagowanie na incydenty	-Procedury zarządzania incydentami -Raportowanie poziomów pokrycia scenariuszami znanych incydentów -Dokumentacja dotycząca przekazywania informacji do właściwego zespołu

bezpieczeństwa	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

5) Audyt bezpieczeństwa, może być przeprowadzony przez:

- a) 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, 974), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
- b) co najmniej dwóch audytorów posiadających:
 - certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
 - co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
 - 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.

6) Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

- a) 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.
2. Termin realizacji zamówienia: **do 15.12.2022r. od podpisania umowy.**
 3. Przy wyborze oferty zostaną zastosowane następujące kryteria oceny ofert: **Cena – 100%**
 4. **Wykonawca składa następujące dokumenty:**
 - 1) *Uzupełniony formularz ofertowy – wg wzoru stanowiącego Załącznik nr 1 do niniejszego zapytania*
 5. Termin złożenia oferty i otwarcia ofert:
Oferty należy złożyć do dnia **29.06.2022 r. do godz. 10:00**
Otwarcie ofert nastąpi w dniu **29.06.2022 r. o godz. 10:15**
 6. **Sposób przygotowania oferty:**
Ofertę na formularzu ofertowym należy złożyć przy użyciu środków komunikacji elektronicznej na adres e-mail: joanna.zalewska@sppchoroszcz.med.pl
 7. **Osoba uprawniona do kontaktów z wykonawcami :**
Joanna Zalewska tel. 85/7191091 wew. 404 e-mail: joanna.zalewska@sppchoroszcz.med.pl
 8. **Zamawiający zastrzega sobie prawo:**
 - 1) w toku badania i oceny ofert do żądania od Wykonawców dodatkowych wyjaśnień dotyczących treści złożonych ofert,
 - 2) podjęcia ewentualnych dalszych negocjacji cenowych w celu zawarcia umowy,
 - 3) swobodnego wyboru oferty lub rezygnacji z wyboru oferty bez podania przyczyny,
 - 4) jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans cenowy, Zamawiający przeprowadzi negocjacje z Wykonawcami,
 - 5) unieważnienia zapytania lub zmiany jego warunków, w tym ograniczenia zakresu zamówienia, bez podania przyczyny.
 11. **W załączeniu:**
 - 1) Załącznik nr 1 – Formularz ofertowy
 - 2) Załącznik nr 2 – Projekt umowy

*p.o. Dyrektora
Samodzielnego Publicznego Psychiatrycznego
Zakładu Opieki Zdrowotnej
im. dr. Stanisława Deresza w Choroszczy*

mgr Bogdana Minkiewicz