Załącznik nr 1

Dane Zamawiającego:
Samodzielny Publiczny
Zakład Opieki Zdrowotnej
w Mońkach
Al. Niepodległości 9
19-100 Mońki

OFERTA

DANE WYKONAWCY

1. Pełna nazwa (oznaczenie, firma) ……..……..……..……..……
2. Adres siedziby (ulica, kod pocztowy, miejscowość) …….....……..……
3. REGON …….…… NIP ……..……..……KRS/CEiDG.....……
4. Telefony (z numerem kierunkowym) ……..……..……..……..…….
5. Faks (z numerem kierunkowym) ……..……..……
6. E-mail ……..……..…….
7. Adres skrzynki ePUAP.....

Odpowiadając na zapytanie ofertowe na wykonanie Audytu bezpieczeństwa dla potrzeb Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Mońkach niniejszym oferuję:

Audyt bezpieczeństwa, 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 uprawiających 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.

   Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

   1. Certified Internal Auditor (CIA);
      1) Certified Information System Auditor (CISA);

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

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. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

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 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

Lp.	**Opis minimalnych wymaganych parametrów technicznych**	**Wartość wymagana**	**Wartość oferowana**
I. Audyt bezpieczeństwa			
1.	Posiadane zasoby do przeprowadzenia Audytu	TAK, podać zasoby	

Cena PLN

1) netto: ……..…….……..… zł

słownie: ……...……...…….…… złotych

2) stawka podatku VAT: ……...% tj. …...……...……zł

słownie: ……...……...…….złotych

3) brutto: ……...……...……..... zł

słownie: ……...……...……..……..…….. złotych

....

(Miejscowość, data) *Podpis osoby (osób) uprawnionej(ych) do składania oświadczeń woli w imieniu Wykonawcy*

Lp.	Opis minimalnych wymaganych parametrów technicznych	Wartość wymagana	Wartość oferowana
2.	Wsparcia eksperckiego w zakresie cyberbezpieczeństwa przez okres do dnia 31 grudnia 2022 r.	TAK, podać	

Cena PLN

1) netto: ……..…….……..… zł

słownie: ……...……...…….…… złotych

2) stawka podatku VAT: ……...% tj. …...……..…...……zł

słownie: ……...……...……złotych

3) brutto: ……...…….…...……..... zł

słownie: ……...……...…….…..…….. złotych

....

(Miejscowość, data) *Podpis osoby (osób) uprawnionej(ych) do składania oświadczeń woli w imieniu Wykonawcy*

2. Oświadczamy, że zrealizujemy przedmiot zamówienia **w terminie …….. (wymagany 4 miesiące)** od dnia podpisania umowy.
3. Przystępując do postępowania o udzielenie zamówienia publicznego oferujemy realizację przedmiotu zamówienia zgodnie z zasadami określonymi w Specyfikacji Warunków Zamówienia.
4. Oferowany przez nas termin płatności wynosi **do 60 dni, o**d daty podpisania przez Strony Protokołu zdawczo – odbiorczego potwierdzającego należyte wykonanie Przedmiotu Umowy.
5. Oświadczam/y, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO** wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. [W przypadku gdy

wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (przez jego wykreślenie)].

....

(Miejscowość, data) Podpis osoby (osób) uprawnionej(ych)

6. do składania oświadczeń woli w imieniu Wykonawcy

7. **WSZELKĄ KORESPONDENCJĘ** w sprawie niniejszego postępowania należy kierować do:

Imię i nazwisko	
Adres	
Telefon	
e-mail	

Oferty cenowe należy złożyć w formie pisemnej w Sekretariacie SP ZOZ w Mońkach lub przy użyciu środków komunikacji elektronicznej na adres e-mail: sekretariat@szpital-monki.h2.pl; informatyk@szpital-monki.h2.pl w terminie **do 27.05.2022 roku, do godz. 12:00**

Kontakt:
Andrzej Haffke, tel.: 668 877 555
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mońkach
ul. Al. Niepodległości 9
19-100 Mońki