

**Ogłoszenie dotyczące zamówienia, dla którego nie ma obowiązku stosowania ustawy Pzp  
Usługi  
przeprowadzenie audytu cyberbezpieczeństwa**

**SEKCJA I – ZAMAWIAJĄCY**

**1.1.) Nazwa zamawiającego:** MAZURSKIE CENTRUM ZDROWIA SZPITAL POWIATOWY W WĘGORZEWIE PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ

**1.3.) Krajowy Numer Identyfikacyjny:** REGON 519461110

**1.4.) Adres zamawiającego**

**1.4.1.) Ulica:** ul. 3 Maja 17

**1.4.2.) Miejscowość:** Węgorzewo

**1.4.3.) Kod pocztowy:** 11-600

**1.4.4.) Województwo:** warmińsko-mazurskie

**1.4.5.) Kraj:** Polska

**1.4.6.) Lokalizacja NUTS 3:** PL623 - Etcki

**1.4.7.) Numer telefonu:** 874273252

**1.4.8.) Numer faksu:** 874273252

**1.4.9.) Adres poczty elektronicznej:** sekretariat@szpitalwegorzewo.pl

**1.4.10.) Adres strony internetowej zamawiającego:** www.mazurskiecentrumzdrowia.pl

**1.5.) Rodzaj zamawiającego:** Zamawiający publiczny - jednostka sektora finansów publicznych - samodzielny publiczny zakład opieki zdrowotnej

**1.6.) Przedmiot działalności zamawiającego:** Zdrowie

**SEKCJA II – INFORMACJE PODSTAWOWE**

**2.2.) Numer ogłoszenia:** 2022/BZP 00325256/01

**2.3.) Wersja ogłoszenia:** 01

**2.4.) Data ogłoszenia:** 2022-08-30 12:36

**SEKCJA III – INFORMACJE O ZAMÓWIENIU**

**3.1.) Nazwa zamówienia**

przeprowadzenie audytu cyberbezpieczeństwa

**3.2.) Rodzaj zamówienia:** Usługi

**3.3.) Krótki opis przedmiotu zamówienia:** Przeprowadzenie końcowego audytu cyberbezpieczeństwa w Mazurskim Centrum Zdrowia Szpitalu Powiatowym w Węgorzewie Publicznym Zakładzie Opieki Zdrowotnej w ramach dofinansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców zakończony raportem.

**3.6.) Termin składania wniosków lub ofert:** 2022-09-08 10:00

**3.7.) Informacje dla wykonawców dotyczące warunków zamówienia**

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) 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).
- 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.