**Załącznik nr 1H do FORMULARZA OFERTOWEGO**

**Parametry techniczne i wyposażenie**

**CZĘŚĆ VIII –AUDYT BEZPIECZEŃSTWA**

WYPEŁNIA WYKONAWCA:

Dane Wykonawcy (nazwa, adres) : …………………………………………………………………………………….

Oferuję wykonanie audytu bezpieczeństwa zgodnie z poniższymi wymaganiami.

UWAGA:

Kolumny nr 3 pt. „Potwierdzenie spełnienia wymagań TAK/NIE” należy wypełnić stosując słowa TAK lub NIE.

W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „NIE” lub zaoferuje niższe wartości niż wymagane, oferta zostanie odrzucona, jako że jej treść jest niezgodna z warunkami zamówienia (art. 226 ust. 1 pkt 5 ustawy Pzp).

**„Dostawa urządzeń i oprogramowania wraz z  przeprowadzeniem audytu cyberbezpieczeństwa wraz ze szkoleniami dla pracowników z zakresu cyberbezpieczeństwa w ramach realizacji projektu Cyfrowa Gmina przez Gminę Ząbkowice Śląskie” z podziałem na 9 zadań/ części. ”**

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do wykonania usługi zgodnie z poniższymi wymogami.

Potwierdzenie spełniania poniższych wymagań:

| Zakres wymagania | Wymaganie / Dokument | Potwierdzenie spełnienia wymagań  TAK/NIE |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Minimalne wymagania dla usługi** | |
| **Typ** | Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina.  Diagnoza cyberbezpieczeństwa powinna zostać przeprowadzona w terminie do 60 dni od podpisania umowy.  Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza diagnozy i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Instytut/SkrytkaESP. | **[….]** |
| **Plan audytu** | Audyt musi składać się z minimum:  1. Audyt dokumentacji i procesów:  - ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)  - ocena wybranych aspektów bezpieczeństwa systemów informatycznych  - ocena dojrzałości wybranych procesów bezpieczeństwa  - opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny  2. Testy penetracyjne infrastruktury sieciowej  - Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci  - skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci)  - skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy  - sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy  - sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł  - weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych  - weryfikacja zabezpieczeń urządzeń sieciowych - testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej  - wykonanie raportu zawierającego minimum:   * opis wszystkich elementów, które zostały poddane audytowi * podział podatności ze względu na ryzyko: wysoki, średni, niski * wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności * wylistowanie wszystkich podatności ze względu na ryzyko: wysoki, średni, niski * określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności   - Wsparcie poaudytowe – Wykonawca ma obowiązek na udzielenie informacji na temat audytowanych elementów wynikających z raportu w terminie maksymalnie 7 dni od wykonania raportu. | **[….]** |
| **Wymagania dla audytora** | Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu 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 (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), 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 | **[….]** |

............................, dn. \_ \_ . \_ \_ . \_ \_ \_ \_r.

**KWALIFIKOWANY PODPIS ELEKTRONICZNY Wykonawcy**

**lub osób uprawnionych do składania oświadczeń**

**woli w imieniu Wykonawcy**