Załącznik nr 2

…………………………………………..………….

(adres Wykonawcy)

**OŚWIADCZENIE WYKONAWCY**

Wykonawca oświadcza, że dysponuje osobą zdolną do realizacji usługi polegającej na kompleksowym wykonaniu diagnozy cyberbezpieczeństwa. Osoba ta posiada certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu\*.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko** | **Dane kontaktowe** | **Nazwa certyfikatu** | **Data uzyskania certyfikatu** |
| 1 |  |  |  |  |

Jednocześnie Wykonawca oświadcza, że wskazana osoba posiada doświadczenie
w wykonywaniu audytów wynikających z Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r.
w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych
i wymiany informacji postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

W przeciągu 3 lat poprzedzających złożenie oferty osoba skierowana do wykonania niniejszego zamówienia przeprowadziła minimum 1 diagnozę cyberbezpieczeństwa oraz zrealizowała co najmniej 2 audyty bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis usługi** | **Nazwa jednostki administracji publicznej** | **Okres wykonywania usługi** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |

W celu weryfikacji warunków należy załączyć dokumenty poświadczające liczbę zadeklarowanego doświadczenia oraz dokumenty potwierdzające posiadanie uprawnień do przeprowadzenia diagnozy cyberbezpieczeństwa przez osobę skierowaną do wykonania przedmiotu umowy.

............................................... ………….…………………........................

 (miejscowość, data) (podpis i pieczęć Wykonawcy)

\* Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane
w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r.
w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu
art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Wykaz certyfikatów wskazanych w ww. rozporządzeniu znajduje się poniżej:

 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 Govemance 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.