Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Znak sprawy: WI.271.25.2022. Załącznik nr 5 do zapytania ofertowego

Sporządzenie diagnozy cyberbezpieczeństwa(postępowanie nr 2)

1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa w siedzibie Zamawiającego - Urząd Miasta Mława (cztery lokalizacje, mieszczące się w obrębie 1km, 110 pracowników).
2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina.
3. Diagnoza musi być przeprowadzona przez **osobę posiadającą certyfikat** uprawniający do przeprowadzenia audytu.

3.1. Polskie uprawnienia do wykonywania określonej działalności lub czynności.

Wykonawca musi **posiadać uprawnienie** 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 roku o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w ww. rozporządzeniu znajduje się poniżej:
1) CertifiedInternal 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 CertifiedPractitioner (SSCP);
10) CertifiedReliability Professional;
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 CybersecurityExpert.

lub jej aktualizację (nowe wydanie certyfikacji)

Dowód: przedstawienie imiennego certyfikatu wymienionego w ww. Rozporządzeniu lub normie po aktualizacji.

3.2. Międzynarodowe uprawnienia do wykonywania określonej działalności lub czynności.

Wykonawca może okazać się normą wystawioną przez **Międzynarodowy Komitet Normalizacji** uprawniającą do przeprowadzenia audytu w zakresie cyberbezpieczeństwa.

Dowód: przedstawienie certyfikatu od Międzynarodowego Komitetu Normalizacji.

4. Wykonawca przekaże wynik przeprowadzonej diagnozy **w postaci podpisanych dokumentów papierowych oraz pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym** (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego). Podpisane dokumenty muszą być przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.
5. Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowa Gmina" są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze powyższy cel przeprowadzenia diagnozy i jej przeznaczenie.
6. W przypadku podważenia wyników diagnozy przez NASK z winy Wykonawcy, Wykonawca daje gwarancję na poprawienie i uzupełnienie wyników diagnozy w celu ponownego wysłania do NASK.

<u>Dodatkowe wymagania:</u>

1. Wykonawca powinien wykazać na etapie oferty, że posiada **normę Polskiego Komitetu Normalizacyjnego** (*lub jej aktualizację*) do której odnoszą się krajowe akty prawne dotyczące programu. W tym wypadku posiadanie normy należy potwierdzić poprzez przesłanie skanu potwierdzonych dokumentów licencji Polskiego Komitetu Normalizacyjnego lub jej aktualizację
   lub
   Wykonawca powinien wykazać na etapie oferty, że posiada **normę Międzynarodowego Komitetu Normalizcji**. W tym wypadku posiadanie normy należy potwierdzić poprzez przesłanie skanu dokumentu licencji Międzynarodowego Komitetu Normalizacji.

2. Wykonawca powinien wykazać na etapie oferty, że dysponuje zasobami do przeprowadzenia audytu zgodnie z rozporządzeniem. Na tym etapie powinny zostać

przedstawione **certyfikaty audytorów wiodących** (nie jakichkolwiek audytorów), wystawione przez certyfikowane ośrodki certyfikujące. Audytor wiodący powinien posiadać co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych.

3. Wykonawca dokona przeglądu dokumentacji bezpieczeństwa oraz zweryfikuje zabezpieczenia w siedzibie zamawiającego. Wgląd do dokumentacji i zasobów technicznych tylko w siedzibie zamawiającego.
4. **Wszystkie opracowane materiały muszą zawierać informację o współfinansowaniu i logotypy. Logotypy i informacja o współfinansowaniu muszą być zgodne z wytycznymi: „Podręcznik wnioskodawcy i beneficjenta programów polityki spójności 2014 – 2020 w zakresie informacji i promocji" wydanego przez Ministra Infrastruktury i Rozwoju, zamieszczonego na stronie internetowej www.funduszeeuropejskie.gov.pl.**

Piotr Tomaszewski;
UM Mława

Elektronicznie podpisany przez
Piotr Tomaszewski; UM Mława
Data: 2022.07.04 13:55:05 +02'00'

Diagnoza cyberbezpieczeństwa:

Przeprowadzona zgodnie z zakresem oraz formularzem stanowiącym załącznik pn.: *„Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa"*
(w załączeniu) przez osobę posiadająca uprawnienia wykazane w *Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu* (w załączeniu).

Diagnozę cyberbezpieczeństwa należy **dostarczyć w wersji elektronicznej oraz w wersji papierowej**.

Załączniki do opisu diagnozy cyberbezpieczeństwa:

- Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa
- Rozporządzenie Mini._Cyfryzacji_wykaz_certyfikatów_uprawniających_do_przeprowadzenia_audytu