

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Znak sprawy: 271.25.2022.

Załącznik nr 5 do zapytania ofertowego

Sporządzenie diagnozy cyberbezpieczeństwa

1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa w siedzibie Zamawiającego - Urząd Miasta Mława (cztery lokalizacje, mieszczące się w obrębie 1 km, 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, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

3.1. Uprawnienia do wykonywania określonej działalności lub czynności

Wykonawca musi posiadać 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 roku 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 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.

Dowód: przedstawienie imiennego certyfikatu wymienionego w ww. Rozporządzeniu.

4. Wykonawca prześle 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.

Dodatkowe wymagania:

1. Wykonawca powinien wykazać na etapie oferty, że posiada normy Polskiego Komitetu Normalizacyjnego, do których odnoszą się krajowe akty prawne dotyczące programu. Posiadanie norm poprzez przesłanie skanów potwierdzonych dokumentów licencji Polskiego Komitetu.
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.funduszeuropejskie.gov.pl.**

Diagnoza cyberbezpieczeństwa:

Przeprowadzona zgodnie z zakresem oraz formularzem stanowiącym załącznik pn.: „Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa” (w załączeniu) przez osobę posiadającą 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