

Załącznik nr 1 do zapytania ofertowego nr FERC.02.02-CS.01-0666/23

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie usługi w Urzędzie Miejskim w Kozienicach polegającej na przeprowadzeniu audytu wstępnego zgodności z Krajowymi Ramami Interoperacyjności w ramach projektu grantowego „Cyberbezpieczny samorząd” w zakresie zgodnym z regulaminem naboru Konkursu Grantowego dostępnym na stronie <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd> oraz określonym w niniejszym zapytaniu, a także zdefiniowaniu celowości wprowadzenia potrzeb określonych w projekcie.

I. Miejsce realizacji zamówienia:

Urząd Miejski w Kozienicach, ul. Parkowa 5, 26-900 Kozienice.

II. Dane dotyczące systemu teleinformatycznego:

dwie lokalizacje pod jednym adresem,

liczba serwerów – 4 szt.,

liczba klientów sieci/użytkowników – 130,

serwisy internetowe – 2,

urządzenia typu UTM – 2.

Uwaga: liczba urządzeń i użytkowników została podana na dzień ogłoszenia zapytania. Zamawiający zastrzega możliwość nieznacznej zmiany liczby urządzeń i użytkowników w okresie trwania umowy,

III. Audyt musi zostać wykonany po odbyciu wizji lokalnej miejsca realizacji zamówienia. Jedynie w przypadku konieczności drobnych zmian lub uzupełnień, dopuszczalna jest forma zdalna.

IV. Audyt wstępny musi być przeprowadzony przez osobę posiadającą uprawnienia wymienione w pkt. IX zapytania ofertowego.

V. Wykonanie usługi obejmuje następujące etapy:

Wykonanie audytu wstępnego zgodności KRI zgodnie z przepisami prawa obowiązującymi w tym zakresie oraz uwzględniającego zagadnienia określone w Załączniku Nr 6 do Regulaminu konkursu grantowego „Cyberbezpieczny samorząd”

Raport z audytu Wykonawca dostarcza Zamawiającemu w wersji papierowej i elektronicznej. Raport z audytu wstępnego powinien być podpisany przez audytora opracowującego audyt własnoręcznie w



przypadku wersji papierowej podpisem, a w przypadku wersji elektronicznej podpisem kwalifikowanym lub podpisem. Zamawiający zastrzega prawo do wniesienia uwag do przedłożonej dokumentacji, a Wykonawca zobowiązuje się do jej skorygowania i uwzględnienia wniesionych uwag.

VI. Audyt początkowy

Przeprowadzenie audytu początkowego zgodnego z KRI/KSC obejmuje:

1. Analizę wstępną stanu bezpieczeństwa informacji w Urzędzie w zakresie objętym audytem.
2. Zebranie wstępnych odpowiedzi i dowodów audytowych.
3. Wspólne zdefiniowanie rekomendowanych działań korygujących w zakresie objętym audytem;
4. Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) w szczególności:

1) Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC);

- wyznaczenie osoby do kontaktu – KSC,
- przekazanie danych osoby wyznaczonej – KSC,
- zapewnienie zarządzania incydem – KSC,
- zgłaszanie incydentu – KSC,
- zapewnienie obsługi incydentu – KSC,
- zapewnienie dostępu do wiedzy – KSC,
- opracowanie, ustanowienie i wdrożenie SZBI – KRI,
- monitorowanie i przegląd SZBI – KRI,
- doskonalenie SZBI – KRI,
- aktualizowanie regulacji wewnętrznych – KRI,
- inwentaryzacja sprzętu i oprogramowania – KRI,
- przeprowadzanie okresowych analiz ryzyka – KRI,
- postępowanie z ryzykiem – KRI,
- zarządzanie uprawnieniami – KRI,
- szkolenia i uświadamianie – KRI,
- monitorowanie dostępu do informacji – KRI,
- monitorowanie nieautoryzowanych zmian – KRI,
- zabezpieczenie nieautoryzowanego dostępu – KRI,





- ustanowienie zasad bezpiecznej pracy mobilnej – KRI,
- zabezpieczenie informacji przed nieuprawnionym ujawnieniem – KRI,
- zabezpieczenie informacji przed nieuprawnioną modyfikacją – KRI,
- zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – KRI,
- zawieranie w umowach serwisowych zapisów o bezpieczeństwie – KRI,
- ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – KRI,
- aktualizowanie oprogramowania – KRI,
- minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – KRI,
- ochrona systemu przed błędami – KRI,
- stosowanie mechanizmów kryptograficznych w systemach – KRI,
- zapewnienie bezpieczeństwa plików systemowych – KRI,
- zarządzanie podatnościami systemów – KRI,
- kontrola zgodności systemów z regulacjami – KRI,
- zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – KRI.

2) Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących

3) Wsparcie poaudytowe, które polegać ma m.in. na udzielaniu informacji na temat audytowanych elementów wynikających z raportu. Czas dla Zamawiającego na zapoznanie się z raportem i zadawanie pytań odnośnie raportu min. 3 miesiące od przeprowadzenia audytu i przedstawieniu raportu.

