

Pytania i odpowiedzi

dot. postępowania na wykonanie zamówienia w zakresie wykonania Audytu Cyberbezpieczeństwa (audyt wstępny i końcowy) wraz z testami penetracyjnymi w ramach projektu „Cyberbezpieczny Samorząd w Mieście Kobyłka” realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Pytanie 1

Ilość lokalizacji Urzędu (adresy, info. co znajduje się pod danym adresem – jakie Wydziały, Referaty, Filie itp.) Pytania z pkt. 2-5 proszę rozgraniczyć na każdą lokalizację z osobna, jeśli jest ich kilka

Odpowiedź 1

Ilość lokalizacji: 3 - ul. Wołomińska 1, 05-230 Kobyłka (Archiwum, Kancelaria, Urząd Stanu Cywilnego, Kasa, Działalność Gospodarcza, Wydział Ochrony Środowiska, Inspektor Ochrony Danych Osobowych, Obrona Cywilna, Zespół ds. Integracji Danych Miejskich i Informatyki, Wydział Promocji i Informacji, Wydział Oświaty, Wydział Spraw Społecznych, Sportu i Zdrowia, Zespół ds. Pozyskiwania Funduszy i Rozwoju, Sekretarz Miasta, Zespół Radców Prawnych, Wydział Kadr i Płac, Sekretariat Burmistrza, Burmistrz Miasta, Zastępca Burmistrza Miasta, Wydział Podatków i Opłat, Wydział Budżetu i Planowania, Skarbnik Miasta, Wydział Inwestycji, Wydział Zamówień Publicznych, Wydział Gospodarki Przestrzennej) - ul. Wołomińska 1b, 05-230 Kobyłka (Wydział Administracji, Biuro Rady Miasta) - ul. Wołomińska 3, 05-230 Kobyłka (Wydział Gospodarczy, Wydział Ochrony Środowiska, Wydział Infrastruktury).

Pytanie 2

Ilość pracowników/użytkowników

Odpowiedź 2

- Wołomińska 1: 74
- Wołomińska 1b: 5
- Wołomińska 3: 33

Pytanie 3

Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.). W tym rozgraniczyć:

- a. Ilość komputerów (również przenośnych)
- b. Ilość serwerów (fizycznych, wirtualnych)
- c. Ilość pozostałych urządzeń podłączonych do sieci

Odpowiedź 3

- a. Ilość komputerów: 100
- b. Ilość serwerów: 13
- c. Ilość pozostałych urządzeń podłączonych do sieci: ok 130 w tym 95 telefonów Voip

Pytanie 4

Ilość adresów zewnętrznych/publicznych

Odpowiedź 4

4

Pytanie 5

Ilość podsieci (jaki zakres maski każdej podsieci?)

Odpowiedź 5

Pragniemy zwrócić Państwa uwagę, iż tego typu szczegółowe dane stanowią informacje wrażliwe. Ze względów bezpieczeństwa oraz zgodnie z obowiązującymi procedurami, udostępnienie takich informacji nastąpi dopiero po pomyślnym zakończeniu formalnego postępowania ofertowego i podpisaniu umowy z wykonawcą.

Pytanie 6

Ilość serwerowni i ich lokalizacja?

Odpowiedź 6

Ilość serwerowni 1, natomiast w kwestii jej lokalizacji to pragniemy zwrócić Państwa uwagę, iż tego typu szczegółowe dane stanowią informacje wrażliwe. Ze względów bezpieczeństwa oraz zgodnie z obowiązującymi procedurami, udostępnienie takich informacji nastąpi dopiero po pomyślnym zakończeniu formalnego postępowania ofertowego i podpisaniu umowy z wykonawcą.

Pytanie 7

Czy mają Państwo wdrożoną Active Directory?

Odpowiedź 7

tak

Pytanie 8

Czy zakres audytu wstępnego (audyt bezpieczeństwa, testy penetracyjne i socjotechniczne) ma być w pełni powtórzony w audycie końcowym (do którego dodatkowo trzeba dołożyć uzupełnienie Ankiety Dojrzałości)?

Odpowiedź 8

tak

Pytanie 9

Jakim budżetem brutto dysponują Państwo na realizację zadań opisanych w niniejszym postępowaniu (jaki budżet został przewidziany we wniosku grantowym)?

Odpowiedź 9

Kwotę podamy przed otwarciem ofert

Pytanie 10

Szanowni Państwo, Mam następujące pytanie dotyczące zapytania ofertowego na: wykonanie Audytu Cyberbezpieczeństwa (wstępnego i końcowego) wraz z testami penetracyjnymi. Czy dopuszczacie Państwo realizację usługi w formie zdalnej?

Odpowiedź 10

Zamawiający dopuszcza częściowo realizację usługi w formie zdalnej, ale szczegóły tego

zostaną ustalone z wybranym Wykonawcą.

Pytanie 11

Liczba lokalizacji Urzędu?

Odpowiedź 11

3

Pytanie 12

Liczba pracowników, w tym działu IT?

Odpowiedź 12

112, w tym 1.5 etatu składającego się na dział IT

Pytanie 13

Liczba urządzeń komputerowych (stacjonarnych, laptopów) i mobilnych?

Odpowiedź 13

100

Pytanie 14

Liczba serwerów, typy serwerów (fizyczne, wirtualne)?

Odpowiedź 14

5 fizycznych, 8 wirtualnych

Pytanie 15

Urządzenia sieciowe (firewalle, switchy, routery)?

Odpowiedź 15

ok. 130 w tym 95 telefonów Voip

Pytanie 16

Aplikacje i systemy: używane systemy (np. ERP, CRM), mechanizmy uwierzytelniania (LDAP, 2FA), zabezpieczenia aplikacji webowych (WAF)?

Odpowiedź 16

Pragniemy zwrócić Państwa uwagę, iż tego typu szczegółowe dane stanowią informacje wrażliwe. Ze względów bezpieczeństwa oraz zgodnie z obowiązującymi procedurami, udostępnienie takich informacji nastąpi dopiero po pomyślnym zakończeniu formalnego postępowania ofertowego i podpisaniu umowy z wykonawcą.

Pytanie 17

W związku z koniecznością prawidłowej wyceny przedmiotu zamówienia zwracamy się z prośbą o udzielenie następujących informacji:

1. Prosimy o wskazanie producenta przełączników sieciowych, routerów oraz firewalli.
2. Jaki jest typ serwera pocztowego i ochrony na nim zaimplementowanej?

Odpowiedź 17

Pragniemy zwrócić Państwa uwagę, iż tego typu szczegółowe dane stanowią informacje wrażliwe. Ze względów bezpieczeństwa oraz zgodnie z obowiązującymi procedurami, udostępnienie takich informacji nastąpi dopiero po pomyślnym zakończeniu formalnego postępowania ofertowego i podpisaniu umowy z wykonawcą.

Pytanie 18

Szanowni Państwo, zwracam się z uprzejmą prośbą o wyjaśnienie treści zapytania ofertowego dot. 4. warunków udziału w zapytaniu, 4.2. Wykonawca wykaże, że posiada odpowiednie doświadczenie tj. w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, minimum trzy usługi przeprowadzenia audytów cyberbezpieczeństwa w podmiotach publicznych zgodnych z wymaganiami KRI (audyt KRI/SZBI zgodnie z ISO 27001) wraz z audytem bezpieczeństwa systemów informatycznych, każda na kwotę minimum 15.000,00 zł brutto.

Czy w związku z powyższym Wykonawca powinien posiadać doświadczenie które dotyczy: zarówno audytu KRI, jak i SZBI (ISO 27001) – czyli że każda z wymaganych usług musiała obejmować jednocześnie oba te elementy, czy audytu KRI lub SZBI – czyli że wystarczy, aby każda z usług obejmowała przynajmniej jeden z tych dwóch typów audytu?

Odpowiedź 18

Zamawiający informuje, iż sformułowanie nie rozdziela KRI lub SZBI i odnosi się do jednoczesnej realizacji audytów zgodnych z oboma standardami lub audytu odnoszącego się do podstaw KRI skupiającego się na spełnieniu minimalnych wymagań określonych w krajowych przepisach dla podmiotów publicznych w celu zapewnienia zgodności z krajowymi regulacjami oraz zgodności z ISO 27001 opierającego się na międzynarodowej normie ISO 27001 celem oceny skuteczności i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Wskazany audyt powinien również zawierać audyt bezpieczeństwa systemów informatycznych czyli kontrolowane, bezinwazyjne badanie oraz kontrolowane próby włamania do systemów informatycznych, aplikacji, infrastruktury sieciowej oraz urządzeń, w celu odkrycia ich słabości i podatności na ataki cybernetyczne, a także testy socjotechniczne, testy aplikacji webowych, testy stron www i serwera pocztowego.