BURMISTRZ BYCZYNY

ul. Rynek 1
46-220 Byczyna

tel/fax.: 77/413 41 50
e-mail: um@byczyna.pl

Byczyna, dnia 24 czerwca 2022 r.

OŚ.271.7.3.2022.Asz

Wszyscy Wykonawcy

Wyjaśnienia treści Specyfikacji Warunków Zamówienia

dot.: postępowania na zadanie:
Zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych. Diagnoza cyberbezpieczeństwa dla GMINY BYCZYNA w projekcie Cyfrowa Gmina w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia" dotyczącego realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

Działając na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz.U. z 2021 r. poz. 1129 – dalej „Pzp"), Zamawiający informuję, iż do Zamawiającego wpłynął wniosek o wyjaśnienie treści Specyfikacji Warunków Zamówienia. Poniżej Zamawiający przedstawia treść zapytań wraz z udzielonymi odpowiedziami:

Pytanie:
Czy wszystkie wnioski i protokoły mogą sporządzane w wersji elektronicznej i podpisywane podpisem kwalifikowanym?
Odpowiedź:
Zamawiający dopuszcza możliwość składania wniosków i protokołów w wersji elektronicznej, zastrzega sobie jednak możliwość żądania dokumentów w klasycznej postaci papierowej.

Pytanie:
W jakim terminie od wezwania lub podpisania umowy Zamawiający udostępni Wykonawcy wszelkie niezbędne informacje i dokumenty do świadczenia usług objętych przedmiotem niniejszej umowy?
Odpowiedź:
Wszelkie niezbędne do wykonania zamówienia informacje i dokumenty dostępne będą dla Wykonawcy od dnia podpisania umowy w siedzibie Zamawiającego.

Pytanie:
Proszę o doprecyzowanie, wykonania jakich dodatkowych czynności oraz dokumentów oczekuje od Wykonawy Zamawiający pisząc w załączniku do SWZ - SOPZ:
„ 5. Wykonawca przedstawi wynik testów w postaci raportu zawierającego zestawienie sprawdzeń oraz zestawu zaleceń umożliwiających minimalizację zidentyfikowanych ryzyk.

6. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowej diagnozy/audytu bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu oraz opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami.

Odpowiedź:

Zgodnie z zapisami pkt 6 Zamawiający wymaga "raportu z wytycznymi do doskonalenia i rekomendacjami".

Pytanie:

Ilość lokalizacji (adresy, info. co znajduje się pod danym adresem)

Pozostałe dane poniżej proszę rozgraniczyć na każdą lokalizację z osobna, pozwoli to najdokładniej obliczyć czasochłonność i cenę projektu:

Odpowiedź:

Jedna lokalizacja – Byczyna, Rynek 1.

Pytanie:

Ilość pracowników/użytkowników

Odpowiedź:

40 pracowników.

Pytanie:

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:

a. Ilość komputerów (również przenośnych) - 60
b. Ilość serwerów (fizycznych, wirtualnych) – 2 fizyczne, 4 wirtualne
c. Ilość pozostałych urządzeń podłączonych do sieci - 60

Pytanie:

Ilość adresów zewnętrznych

Odpowiedź:

2

Pytanie:

Ilość podsieci (jaki zakres maski każdej podsieci?)

Odpowiedź:

1, 255.255.192.0

Pytanie:
Ilość serwerowni i ich lokalizacja?
Odpowiedź:
Jedna serwerownia.

Pytanie:

Czy mają Państwo wdrożoną Active Directory?
Odpowiedź:

Tak.

Pytanie:

Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?

Odpowiedź:

Zamawiający poda kwotę, jaką przeznaczył na realizację zamówienia zgodnie z zapisami art. 222 ust. 4 ustawy Prawo zamówień publicznych.

Pytanie:

Z jaką datą mają Państwo podpisaną Umowę grantową (chodzi o datę podpisu złożonego przez Grantodawcę)?

Odpowiedź:

11.02.2022 r.

Pytanie:
Czy termin realizacji jest negocjowalny przed podpisaniem umowy jeżeli realizacja diagnozy w pełni zmieści się w 6 miesiącach od daty podpisania umowy grantowej?
Odpowiedź:
Termin wykonania umowy stanowi kryterium oceny ofert, więc co do zasady nie może podlegać negocjacją.

Pytanie:

Wspomnianym w treści zapytania raportem z audytu ma być jedynie zał. 8 konkursu i omówienie zaleceń i rekomendacji jakie z niego wynikną?

Odpowiedź:

Zamawiający oczekuje dodatkowo raportu w którym zawarte zostaną zalecenia i rekomendacje w każdym z audytowanych obszarów.

Pytanie:

Odnosząc się do treści zał. 8 konkursu zawartej w arkuszu KRI i CERT, proszę o informacje czy posiadają Państwo Dokumentację oraz Raporty/Wyniki z audytów tam wskazane, aby było możliwe ich sprawdzenie/ocena podczas Diagnozy?

3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**	**Tak**	**Nie**
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?		
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?		
3.3	Czy istnieje dokumentacja architektury sieci?		

3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?		
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?		
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?		
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?		
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?		
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?		
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?		
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?		
4	**Dokumentacja procesu zarządzania incydentami**		
4.2	Czy istnieje procedura informowania o wykrytych incydentach?		
4.3	Czy istnieją procedury reagowania na incydenty?		
5	**Aspekty techniczne do weryfikacji**		
5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.		
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.		
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.		
5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.		
6	**Aspekty organizacyjne do weryfikacji**		
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników		

	podnoszących ich świadomość zagrożeń.		
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.		
7	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)		

Odpowiedź:

Powyższe pytanie nie stanowi wniosku o wyjaśnienie treści SWZ. Analiza zagadnień zawartych w pytaniu i idąca za tym odpowiedź Zamawiającego jest częścią przedmiotu zamówienia, którego realizacja leży po stronie Wykonawcy.

Z poważaniem

BURMISTRZ BYCZYNY

/-/Iwona Sobania

Otrzymują:
1. Strona prowadzonego postępowania
2. a/a

Sporządziła:
Aneta Sztojko-Chałupczyńska