

W związku z wpłynięciem w dniu 24.06.2022r. pytań od potencjalnego Wykonawcy o treści przedstawionej poniżej, Zamawiający udziela następujących odpowiedzi:

1. Ilość lokalizacji (adresy, info. co znajduje się pod danym adresem)
- jedna lokalizacja: Urząd Gminy 59-720 Warta Bolesławiecka 40C
Pozostałe dane poniżej proszę rozgraniczyć na każdą lokalizację z osobną, pozwoli to najdokładniej obliczyć czasochłonność i cenę projektu:
2. Ilość pracowników/użytkowników - **30**
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) - **44**
 - b. Ilość serwerów (fizycznych, wirtualnych) – **2/4**
 - c. Ilość pozostałych urządzeń podłączonych do sieci - **34**
4. Ilość adresów zewnętrznych - 1
5. Ilość podsieci (jaki zakres maski każdej podsieci?) – **4 (24)**
6. Ilość serwerowni i ich lokalizacja? – **1** w budynku urzędu
7. Czy mają Państwo wdrożoną Active Directory? - **tak**
8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków? – **12.400,00 zł**
9. Z jaką datą mają Państwo podpisaną Umowę grantową (chodzi o datę podpisu złożonego przez Grantodawcę)? – **04.03.2022 r.**
10. Czy termin realizacji jest negocjowalny przed podpisaniem umowy jeżeli realizacja diagnozy w pełni zmieści się w 6 miesiącach od daty podpisania umowy grantowej? - **nie ma takiej możliwości**
11. Czy poza wypełnieniem zał. 8 konkursu dla NASK wymagają Państwo również raportu z audytu dla Urzędu? - **tak**
12. 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?		X
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?		X
3.3	Czy istnieje dokumentacja architektury sieci?	X	
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?	X	
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?	X	
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?	X	
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?	X	
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?		X
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?		X
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?		X
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?		X
4	Dokumentacja procesu zarządzania incydentami		

4.2	Czy istnieje procedura informowania o wykrytych incydentach?	x	
4.3	Czy istnieją procedury reagowania na incydenty?	x	
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.		x
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.		x
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.		x
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.		x
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.		x
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.		x
7	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	x	