Adres strony internetowej, na której zamieszczona będzie specyfikacja istotnych warunków zamówienia (jeżeli dotyczy):

http://www.wokiss.pl/

Ogłoszenie nr 49505 - 2017 z dnia 2017-03-22 r.

Poznań: Wykonanie Audytu Stanu bezpieczeństwa informacji

OGŁOSZENIE O ZAMÓWIENIU - Usługi

Zamieszczanie ogłoszenia: obowiązkowe

Ogłoszenie dotyczy: zamówienia publicznego

Zamówienie dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej

tak

Nazwa projektu lub programu

Cyfrowe samorządy atutem Wielkopolski-nowe obszary świadczenia e-usług w 22 gminach województwa wielkopolskiego

O zamówienie mogą ubiegać się wyłącznie zakłady pracy chronionej oraz wykonawcy, których działalność, lub działalność ich wyodrębnionych organizacyjnie jednostek, które będą realizowały zamówienie, obejmuje społeczną i zawodową integrację osób będących członkami grup społecznie marginalizowanych

nie

Należy podać minimalny procentowy wskaźnik zatrudnienia osób należących do jednej lub więcej kategorii, o których mowa w art. 22 ust. 2 ustawy Pzp, nie mniejszy niż 30%, osób zatrudnionych przez zakłady pracy chronionej lub wykonawców albo ich jednostki (w %)

SEKCJA I: ZAMAWIAJĄCY

Postępowanie przeprowadza centralny zamawiający

nie

Postępowanie przeprowadza podmiot, któremu zamawiający powierzył/ powierzyli przeprowadzenie postępowania

nie

Informacje na temat podmiotu któremu zamawiający powierzył/ powierzyli prowadzenie

postępowania:

Postępowanie jest przeprowadzane wspólnie przez zamawiających

nie

Jeżeli tak, należy wymienić zamawiających, którzy wspólnie przeprowadzają postępowanie oraz podać adresy ich siedzib, krajowe numery identyfikacyjne oraz osoby do kontaktów wraz z danymi do kontaktów:

Postępowanie jest przeprowadzane wspólnie z zamawiającymi z innych państw członkowskich Unii Europejskiej

nie

W przypadku przeprowadzania postępowania wspólnie z zamawiającymi z innych państw członkowskich Unii Europejskiej – mające zastosowanie krajowe prawo zamówień publicznych:

Informacje dodatkowe:

I. 1) NAZWA I ADRES: Wielkopolski Ośrodek Kształcenia i Studiów Samorządowych, krajowy numer identyfikacyjny 004806007, ul. Piotra Wawrzyniaka 37, 60-504 Poznań, woj. wielkopolskie, państwo Polska, tel. 61 847 54 22, e-mail agnieszka.mendelewska@wokiss.pl, faks 61 624 37 64.

Adres strony internetowej (URL): http://www.wokiss.pl/

I. 2) RODZAJ ZAMAWIAJĄCEGO: Inny: Stowarzyszenie

I.3) WSPÓLNE UDZIELANIE ZAMÓWIENIA (jeżeli dotyczy):

Podział obowiązków między zamawiającymi w przypadku wspólnego przeprowadzania postępowania, w tym w przypadku wspólnego przeprowadzania postępowania z zamawiającymi z innych państw członkowskich Unii Europejskiej (który z zamawiających jest odpowiedzialny za przeprowadzenie postępowania, czy i w jakim zakresie za przeprowadzenie postępowania odpowiadają pozostali zamawiający, czy zamówienie będzie udzielane przez każdego z zamawiających indywidualnie, czy zamówienie zostanie udzielone w imieniu i na rzecz pozostałych zamawiających):

I.4) KOMUNIKACJA:

Nieograniczony, pełny i bezpośredni dostęp do dokumentów z postępowania można uzyskać pod adresem (URL)

nie

Adres strony internetowej, na której zamieszczona będzie specyfikacja istotnych warunków zamówienia

tak

http://www.wokiss.pl/

Dostęp do dokumentów z postępowania jest ograniczony - więcej informacji można uzyskać pod adresem

nie

Oferty lub wnioski o dopuszczenie do udziału w postępowaniu należy przesyłać:

Elektronicznie

nie

adres

Dopuszczone jest przesłanie ofert lub wniosków o dopuszczenie do udziału w postępowaniu w inny sposób:

nie

Wymagane jest przesłanie ofert lub wniosków o dopuszczenie do udziału w postępowaniu w inny sposób:

tak

Inny sposób:

Pocztą, osobiście, kurierem

Adres:

ul. Piotra Wawrzyniaka 37, 61-504 Poznań

Komunikacja elektroniczna wymaga korzystania z narzędzi i urządzeń lub formatów plików, które nie są ogólnie dostępne

nie

Nieograniczony, pełny, bezpośredni i bezpłatny dostęp do tych narzędzi można uzyskać pod adresem: (URL)

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) Nazwa nadana zamówieniu przez zamawiającego: Wykonanie Audytu Stanu bezpieczeństwa informacji

Numer referencyjny: 4/PZP/AUD

Przed wszczęciem postępowania o udzielenie zamówienia przeprowadzono dialog techniczny

nie

II.2) Rodzaj zamówienia: usługi

II.3) Informacja o możliwości składania ofert częściowych

Zamówienie podzielone jest na części:

Tak

Oferty lub wnioski o dopuszczenie do udziału w postępowaniu można składać w odniesieniu do:

wszystkich części maksymalnej liczby części 3

II.4) Krótki opis przedmiotu zamówienia (wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań) a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane: Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS). Podział na zadania: 1. Zadanie 1 I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 6 urzędów gmin: Gmina Chodzież, Gmina Drawsko, Gmina Krzyż Wielkopolski, Gmina Lubasz, Gmina Łobżenica, Gmina Skoki. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne

stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001

„Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania”. Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci” rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania”. Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać

będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy. 2. Zadanie 2 I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 7 urzędów gmin: Gmina Czempiń, Gmina Kostrzyn, Gmina Miejska Luboń, Gmina Mosina, Gmina Opalenica, Gmina Stęszew, Gmina Śrem. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje

i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-

Wymagania". Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych

zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy. 3. Zadanie 3 I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 5 urzędów gmin: Gmina Brudzew, Gmina Czerniejewo, Gmina Przykona, Gmina Słupca, Gmina Strzałkowo. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa

Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji- Wymagania”. Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu,

przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia

dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy. 4. Zadanie 4 I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 4 urzędów gmin: Gmina Bojanowo, Gmina Jaraczewo, Gmina Miejska Górka, Gmina Ostrów Wielkopolski. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie

audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania”. Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i

rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i

wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy. 5. Zadanie 5 I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla Zamawiającego. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Zamawiającego (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Zamawiającego (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do organizacji. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanej jednostki w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań

prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Zamawiającego, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania”. Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla Zamawiającego, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie

dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do organizacji. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi Zamawiającego, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Zamawiającego, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników dla Zamawiającego, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się

do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi Zamawiającego, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do ustalenia z Zamawiającym harmonogramu prac w terminie 10 dni od daty podpisania umowy. Ogólne wymagania dotyczące przedmiotu zamówienia oraz jego realizacji: Zamawiający dopuszcza możliwość składania ofert częściowych. Zamawiający nie dopuszcza możliwości składania ofert wariantowych. Przyjęte typy materiałów i urządzeń (wskazane w dokumentacji technicznej) zostały użyte wyłącznie przykładowo, w celu opisania przedmiotu zamówienia. Wykonawca uprawniony jest do przedstawienia w ofercie materiałów i urządzeń równoważnych, o nie gorszych parametrach. Wykonawca powinien określić ich parametry, celem wykazania, że spełniają warunki określone w opisie przedmiotu zamówienia. Rozwiązania równoważne, zgodnie ze swoją definicją, muszą posiadać parametry oraz spełniać standardy nie gorsze niż produkty podane przykładowo. W miejscu gdzie Zamawiający dokonuje opisu przedmiotu zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3 Ustawy, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy 'lub równoważne'. Wykonawca może złożyć ofertę na 3 części. Wykonawcy może zostać udzielone zamówienie na 3 części. Zamawiający przewiduje konieczność przeniesienia praw własności intelektualnej lub udzielenia licencji. Zamawiający na podstawie art. 29 ust 3a stawy PZP zastrzega, że poniższe rodzaje czynności wymagają zatrudnienia na postawie umowy o pracę przez wykonawcę lub podwykonawcę: • przeprowadzanie wywiadów z klientami w celu zebrania informacji potrzebnych do badań i analizy klienta w zakresie bezpieczeństwa informacji • weryfikacja dokumentacji klienta • opracowywanie dokumentacji z zakresu bezpieczeństwa informacji dla klienta • opracowywanie Raportów przedstawiających poziom bezpieczeństwa informacji klienta • badanie fizyczne zabezpieczeń obszarów przetwarzania danych osobowych (testowanie zabezpieczenia pomieszczeń/budynku) • badanie i analizowanie sieci komputerowej klienta na próby ataków, przeprowadzanie testów

II.5) Główny kod CPV:

II.6) Całkowita wartość zamówienia (jeżeli zamawiający podaje informacje o wartości zamówienia):

Wartość bez VAT:

Waluta:

(w przypadku umów ramowych lub dynamicznego systemu zakupów – szacunkowa całkowita maksymalna wartość w całym okresie obowiązywania umowy ramowej lub dynamicznego systemu zakupów)

II.7) Czy przewiduje się udzielenie zamówień, o których mowa w art. 67 ust. 1 pkt 6 i 7 lub w art. 134 ust. 6 pkt 3 ustawy Pzp: nie

II.8) Okres, w którym realizowane będzie zamówienie lub okres, na który została zawarta umowa ramowa lub okres, na który został ustanowiony dynamiczny system zakupów:

data zakończenia: 31/07/2017

II.9) Informacje dodatkowe:

SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

III.1) WARUNKI UDZIAŁU W POSTĘPOWANIU

III.1.1) Kompetencje lub uprawnienia do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów

Określenie warunków: Zamawiający nie precyzuje warunków w tym zakresie

Informacje dodatkowe

III.1.2) Sytuacja finansowa lub ekonomiczna

Określenie warunków: Zamawiający nie precyzuje warunków w tym zakresie

Informacje dodatkowe

III.1.3) Zdolność techniczna lub zawodowa

Określenie warunków: Wykonawca posiada doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał co najmniej 3 zadania polegające na przeprowadzeniu Audytu KRI oraz co najmniej 3 zadania polegające na przeprowadzeniu Audytu Bezpieczeństwa Sieci. Wykonawca dysponuje co najmniej: 2 osobami, które brały

udział w realizacji minimum 3 Audytów KRI oraz minimum 3 Audytów Bezpieczeństwa Sieci oraz: a) przynajmniej jedna z tych osób jest audytorem wiodącym zgodnie z PN-ISO/IEC 27001 zakwalifikowanym przez jedną z jednostek certyfikujących, b) przynajmniej jedna z tych osób posiada co najmniej jeden z certyfikatów: CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control), ITIL® FOUNDATION (Information Technology Infrastructure Library) c) przynajmniej jedna z tych osób posiada praktyczne, minimum półroczne doświadczenie w zakresie zarządzania bezpieczeństwem danych osobowych lub w zakresie pełnienia funkcji Administratora Bezpieczeństwa Informacji.

Zamawiający wymaga od wykonawców wskazania w ofercie lub we wniosku o dopuszczenie do udziału w postępowaniu imion i nazwisk osób wykonujących czynności przy realizacji zamówienia wraz z informacją o kwalifikacjach zawodowych lub doświadczeniu tych osób: nie

Informacje dodatkowe:

III.2) PODSTAWY WYKLUCZENIA

III.2.1) Podstawy wykluczenia określone w art. 24 ust. 1 ustawy Pzp

III.2.2) Zamawiający przewiduje wykluczenie wykonawcy na podstawie art. 24 ust. 5 ustawy Pzp nie

III.3) WYKAZ OŚWIADCZEŃ SKŁADANYCH PRZEZ WYKONAWCĘ W CELU WSTĘPNEGO POTWIERDZENIA, ŻE NIE PODLEGA ON WYKLUCZENIU ORAZ SPEŁNIA WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ SPEŁNIA KRYTERIA SELEKCJI

Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu

tak

Oświadczenie o spełnianiu kryteriów selekcji

nie

III.4) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW , SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI , O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 3 USTAWY PZP:

III.5) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI , O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 1 USTAWY PZP

III.5.1) W ZAKRESIE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

a) Wykaz usług wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz

których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. b) Wykaz osób, skierowanych przez wykonawcę do realizacji zamówienia publicznego wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami.

III.5.2) W ZAKRESIE KRYTERIÓW SELEKCJI:

III.6) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 2 USTAWY PZP

III.7) INNE DOKUMENTY NIE WYMIENIONE W pkt III.3) - III.6)

SEKCJA IV: PROCEDURA

IV.1) OPIS

IV.1.1) Tryb udzielenia zamówienia: przetarg nieograniczony

IV.1.2) Zamawiający żąda wniesienia wadium:

tak,

Informacja na temat wadium

12. WYMAGANIA DOTYCZĄCE WADIUM 12.1. Wykonawca zobowiązany jest wnieść wadium w wysokości: - 1 170,00 zł w zakresie zadania nr 1 - 1 365,00 zł w zakresie zadania nr 2 - 975,00 zł w zakresie zadania nr 3 - 780,00 zł w zakresie zadania nr 4 - 195,00 zł w zakresie zadania nr 5 12.2. Wadium należy wnieść przed upływem terminu składania ofert, przy czym wniesienie wadium w pieniądzu za pomocą przelewu bankowego Zamawiający będzie uważał za skuteczne tylko wówczas gdy przed upływem terminu składania ofert kwota wniesionego wadium będzie uznana na rachunku bankowym Zamawiającego. Zaleca się, aby kopię dowodu wniesienia wadium załączyć do oferty. 12.3. Wadium może być wnoszone w jednej lub kilku następujących formach: a) pieniądzu: przelewem na rachunek bankowy Zamawiającego: 81 1050 1520 1000 0090 3089 2302 b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym; c) gwarancjach bankowych; d)

gwarancjach ubezpieczeniowych; e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt. 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości. 12.4. Zwrot lub zatrzymanie wadium następuje na zasadach określonych w art. 46 Ustawy. 12.5. Wadium wnoszone w innej niż pieniądz formie musi posiadać ważność co najmniej do końca terminu związania wykonawcy złożoną przez niego ofertą. 12.6. W przypadku wniesienia wadium w innej formie niż pieniądz należy załączyć do oferty odpowiedni dokument, nie spięty w całość z ofertą.

IV.1.3) Przewiduje się udzielenie zaliczek na poczet wykonania zamówienia:

nie

IV.1.4) Wymaga się złożenia ofert w postaci katalogów elektronicznych lub dołączenia do ofert katalogów elektronicznych:

nie

Dopuszcza się złożenie ofert w postaci katalogów elektronicznych lub dołączenia do ofert katalogów elektronicznych:

nie

Informacje dodatkowe:

IV.1.5.) Wymaga się złożenia oferty wariantowej:

nie

Dopuszcza się złożenie oferty wariantowej

nie

Złożenie oferty wariantowej dopuszcza się tylko z jednoczesnym złożeniem oferty zasadniczej:

nie

IV.1.6) Przewidywana liczba wykonawców, którzy zostaną zaproszeni do udziału w postępowaniu (przetarg ograniczony, negocjacje z ogłoszeniem, dialog konkurencyjny, partnerstwo innowacyjne)

Liczba wykonawców

Przewidywana minimalna liczba wykonawców

Maksymalna liczba wykonawców

Kryteria selekcji wykonawców:

IV.1.7) Informacje na temat umowy ramowej lub dynamicznego systemu zakupów:

Umowa ramowa będzie zawarta:

Czy przewiduje się ograniczenie liczby uczestników umowy ramowej:

nie

Informacje dodatkowe:

Zamówienie obejmuje ustanowienie dynamicznego systemu zakupów:

nie

Informacje dodatkowe:

W ramach umowy ramowej/dynamicznego systemu zakupów dopuszcza się złożenie ofert w formie katalogów elektronicznych:

nie

Przewiduje się pobranie ze złożonych katalogów elektronicznych informacji potrzebnych do sporządzenia ofert w ramach umowy ramowej/dynamicznego systemu zakupów:

nie

IV.1.8) Aukcja elektroniczna

Przewidziane jest przeprowadzenie aukcji elektronicznej (przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem) nie

Należy wskazać elementy, których wartości będą przedmiotem aukcji elektronicznej:

Przewiduje się ograniczenia co do przedstawionych wartości, wynikające z opisu przedmiotu zamówienia:

nie

Należy podać, które informacje zostaną udostępnione wykonawcom w trakcie aukcji elektronicznej oraz jaki będzie termin ich udostępnienia:

Informacje dotyczące przebiegu aukcji elektronicznej:

Jaki jest przewidziany sposób postępowania w toku aukcji elektronicznej i jakie będą warunki, na jakich wykonawcy będą mogli licytować (minimalne wysokości postąpień):

Informacje dotyczące wykorzystywanego sprzętu elektronicznego, rozwiązań i specyfikacji technicznych w zakresie połączeń:

Wymagania dotyczące rejestracji i identyfikacji wykonawców w aukcji elektronicznej:

Informacje o liczbie etapów aukcji elektronicznej i czasie ich trwania:

Aukcja wieloetapowa

etap nr czas trwania etapu

Czy wykonawcy, którzy nie złożyli nowych postąpień, zostaną zakwalifikowani do następnego etapu: nie

Warunki zamknięcia aukcji elektronicznej:

IV.2) KRYTERIA OCENY OFERT

IV.2.1) Kryteria oceny ofert:

IV.2.2) Kryteria

Kryteria	Znaczenie
Cena	50
Doświadczenie osób wyznaczonych do realizacji przedmiotu zamówienia	30
Termin realizacji	20

IV.2.3) Zastosowanie procedury, o której mowa w art. 24aa ust. 1 ustawy Pzp (przetarg nieograniczony)

nie

IV.3) Negocjacje z ogłoszeniem, dialog konkurencyjny, partnerstwo innowacyjne

IV.3.1) Informacje na temat negocjacji z ogłoszeniem

Minimalne wymagania, które muszą spełniać wszystkie oferty:

Przewidziane jest zastrzeżenie prawa do udzielenia zamówienia na podstawie ofert wstępnych bez przeprowadzenia negocjacji nie

Przewidziany jest podział negocjacji na etapy w celu ograniczenia liczby ofert: nie

Należy podać informacje na temat etapów negocjacji (w tym liczbę etapów):

Informacje dodatkowe

IV.3.2) Informacje na temat dialogu konkurencyjnego

Opis potrzeb i wymagań zamawiającego lub informacja o sposobie uzyskania tego opisu:

Informacja o wysokości nagród dla wykonawców, którzy podczas dialogu konkurencyjnego przedstawili rozwiązania stanowiące podstawę do składania ofert, jeżeli zamawiający przewiduje nagrody:

Wstępny harmonogram postępowania:

Podział dialogu na etapy w celu ograniczenia liczby rozwiązań: nie

Należy podać informacje na temat etapów dialogu:

Informacje dodatkowe:

IV.3.3) Informacje na temat partnerstwa innowacyjnego

Elementy opisu przedmiotu zamówienia definiujące minimalne wymagania, którym muszą odpowiadać wszystkie oferty:

Podział negocjacji na etapy w celu ograniczeniu liczby ofert podlegających negocjacjom poprzez zastosowanie kryteriów oceny ofert wskazanych w specyfikacji istotnych warunków zamówienia:

nie

Informacje dodatkowe:

IV.4) Licytacja elektroniczna

Adres strony internetowej, na której będzie prowadzona licytacja elektroniczna:

Adres strony internetowej, na której jest dostępny opis przedmiotu zamówienia w licytacji elektronicznej:

Wymagania dotyczące rejestracji i identyfikacji wykonawców w licytacji elektronicznej, w tym wymagania techniczne urządzeń informatycznych:

Sposób postępowania w toku licytacji elektronicznej, w tym określenie minimalnych wysokości postąpień:

Informacje o liczbie etapów licytacji elektronicznej i czasie ich trwania:

Licytacja wieloetapowa

etap nr czas trwania etapu

Wykonawcy, którzy nie złożyli nowych postąpień, zostaną zakwalifikowani do następnego etapu: nie

Termin otwarcia licytacji elektronicznej:

Termin i warunki zamknięcia licytacji elektronicznej:

Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia

publicznego, albo ogólne warunki umowy, albo wzór umowy:

Wymagania dotyczące zabezpieczenia należytego wykonania umowy:

Informacje dodatkowe:

I V.5) ZMI ANA UMOWY

Przewiduje się istotne zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy: nie

I V.6) I NFORMACJE ADMI NI STRACYJNE

I V.6.1) Sposób udostępniania informacji o charakterze poufnym (jeżeli dotyczy):

Środki służące ochronie informacji o charakterze poufnym

I V.6.2) Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu:

Data: 30/03/2017, godzina: 11:00,

Skrócenie terminu składania wniosków, ze względu na pilną potrzebę udzielenia zamówienia (przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem):

nie

Wskazać powody:

Język lub języki, w jakich mogą być sporządzane oferty lub wnioski o dopuszczenie do udziału w postępowaniu

>

I V.6.3) Termin związania ofertą: okres w dniach: 30 (od ostatecznego terminu składania ofert)

I V.6.4) Przewiduje się unieważnienie postępowania o udzielenie zamówienia, w przypadku nieprzyznania środków pochodzących z budżetu Unii Europejskiej oraz niepodlegających zwrotowi środków z pomocy udzielonej przez państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA), które miały być przeznaczone na sfinansowanie całości lub części zamówienia: nie

I V.6.5) Przewiduje się unieważnienie postępowania o udzielenie zamówienia, jeżeli środki służące sfinansowaniu zamówień na badania naukowe lub prace rozwojowe, które zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu przyznane

nie

I V.6.6) Informacje dodatkowe:

ZAŁĄCZNIK I - INFORMACJE DOTYCZĄCE OFERT CZĘŚCIOWYCH

Część nr: 1 Nazwa:

1) Krótki opis przedmiotu zamówienia (wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań) a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane: I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 6 urzędów gmin: Gmina Chodzież, Gmina Drawsko, Gmina Krzyż Wielkopolski, Gmina Lubasz, Gmina Łobżenica, Gmina Skoki. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla

niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres

działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności

osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy.

2) Wspólny Słownik Zamówień (CPV): 79212000-3

3) Wartość części zamówienia (jeżeli zamawiający podaje informacje o wartości zamówienia):

Wartość bez VAT:

Waluta:

4) Czas trwania lub termin wykonania: data zakończenia: 31/07/2017

5) Kryteria oceny ofert:

Kryteria	Znaczenie
Cena	50
Doświadczenie osób wyznaczonych do realizacji przedmiotu zamówienia	30
Termin realizacji	20

6) INFORMACJE DODATKOWE:

Część nr: 2 Nazwa: Zadanie 2

1) Krótki opis przedmiotu zamówienia (wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań) a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane: I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 7 urzędów gmin: Gmina Czempiń, Gmina Kostrzyn, Gmina Miejska Luboń, Gmina Mosina, Gmina Opalenica, Gmina Stęszew, Gmina Śrem. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi

określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI.

Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany

rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy.

2) Wspólny Słownik Zamówień (CPV): 79212000-3

3) Wartość części zamówienia (jeżeli zamawiający podaje informacje o wartości zamówienia):

Wartość bez VAT:

Waluta:

4) Czas trwania lub termin wykonania: data zakończenia: 31/07/2017

5) Kryteria oceny ofert:

Kryteria	Znaczenie
Cena	50
Doświadczenie osób wyznaczonych do realizacji przedmiotu zamówienia	30

Termin realizacji 20

6) INFORMACJE DODATKOWE:

Część nr: 3 Nazwa: Zadanie 3

1) Krótki opis przedmiotu zamówienia (wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań) a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane: I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 5 urzędów gmin: Gmina Brudzew, Gmina Czerniejewo, Gmina Przykona, Gmina Słupca, Gmina Strzałkowo. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian

uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych

urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w

audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy.

2) Wspólny Słownik Zamówień (CPV): 79212000-3

3) Wartość części zamówienia (jeżeli zamawiający podaje informacje o wartości zamówienia):

Wartość bez VAT:

Waluta:

4) Czas trwania lub termin wykonania: data zakończenia: 31/07/2017

5) Kryteria oceny ofert:

Kryteria	Znaczenie
Cena	50
Doświadczenie osób wyznaczonych do realizacji przedmiotu zamówienia	30
Termin realizacji	20

6) INFORMACJE DODATKOWE:

Część nr: 4 Nazwa: Zadanie 4

1) Krótki opis przedmiotu zamówienia (wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań) a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane: I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla 4 urzędów gmin: Gmina Bojanowo, Gmina Jaraczewo, Gmina Miejska Górka, Gmina Ostrów Wielkopolski. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych

przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Gmin (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Gmin (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanych jednostek w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli

wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla każdego podmiotu, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie wzór Polityki Bezpieczeństwa Informacji dopasowany do JST. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Gmin, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników indywidualnie dla każdego podmiotu,

wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi, indywidualnie dla każdego podmiotu, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3. Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do przedłożenia Zamawiającemu harmonogramu prac dla danej grupy Gmin w terminie 10 dni od daty podpisania umowy.

2) Wspólny Słownik Zamówień (CPV): 79212000-3

3) Wartość części zamówienia (jeżeli zamawiający podaje informacje o wartości zamówienia):

Wartość bez VAT:

Waluta:

4) Czas trwania lub termin wykonania: data zakończenia: 31/07/2017

5) Kryteria oceny ofert:

Kryteria	Znaczenie
Cena	50

Doświadczenie osób wyznaczonych do realizacji przedmiotu zamówienia 30

Termin realizacji 20

6) INFORMACJE DODATKOWE:

Część nr: 5 Nazwa: Zadanie 5

1) Krótki opis przedmiotu zamówienia (wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań) a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane: I. Wykonanie Audytu Systemu zarządzania bezpieczeństwem informacji w celu oceny stopnia spełnienia wymogów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Audytu KRI) wraz z Audytem Bezpieczeństwa Sieci dla oceny topologii sieci komputerowej oraz zidentyfikowania, a następnie wskazania sposobów wyeliminowania podatności na zagrożenia w systemach informatycznych (Audytu BS) dla Zamawiającego. II. Zamawiający przez „Audyt KRI" rozumie sprawdzenie czy systemy informatyczne wykorzystywane przez dany podmiot oraz procedury stosowane w danym podmiocie i dokumentacja je opisująca zapewniają skuteczną ochronę danych przetwarzanych w podmiotach poddanych sprawdzeniu, a w szczególności spełniają wymogi określone w § 20 Rozporządzenia KRI. Przedmiot zamówienia obejmuje w szczególności: a) analizę regulacji wewnętrznych Zamawiającego (polityk, instrukcji, regulaminów) i zapisów w zakresie bezpieczeństwa informacji, b) przeprowadzenie czynności audytorskich w siedzibach Zamawiającego (weryfikacja zabezpieczeń fizycznych, organizacyjnych, technicznych), c) opracowanie wyników w postaci Raportu z Audytu KRI zawierającego opis stanu aktualnego, ewentualne stwierdzone nieprawidłowości oraz wnioski, rekomendacje i zalecenia w celu spełnienia wymagań Rozporządzenia KRI. W ramach Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do organizacji. Zakres działań w ramach Audytu KRI powinien obejmować skontrolowanie audytowanej jednostki w następujących obszarach: a) Zgodność z prawem: • Cel: W organizacji wprowadzane są dokumenty niezbędne do realizacji wymagań prawnych. • Ryzyko: Organizacja nie spełnia wymogów prawnych. b) Aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji: • Cel: Zapewnienie prawdziwej i szybkiej informacji na temat sprzętu i oprogramowania. • Ryzyko: W organizacji trudno uzyskać informacje na temat oprogramowania oraz sprzętu. c) Ocena przeprowadzanych analiz ryzyka: • Cel: Zidentyfikowanie zagrożeń mogących wystąpić w organizacji. • Ryzyko: Organizacja nie posiada zidentyfikowanych potencjalnych zagrożeń. d) Weryfikacja uprawnień: • Cel: Zapewnienie, że wszystkie osoby posiadają odpowiednie uprawnienia dostępu do informacji. • Ryzyko: Dostęp do informacji mogą posiadać nieuprawnione osoby. e) Procedury zmiany uprawnień: • Cel: Zapewnienie, że

procedury zmian uprawnień dostępu do informacji są stosowane. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji dla niech nieprzeznaczonych. f) Uświadamianie użytkowników: • Cel: Pracownicy mają świadomość dotyczącą bezpieczeństwa informacji. • Ryzyko: Pracownicy nie znają procedur bezpieczeństwa i jak się zachować przy przetwarzaniu informacji. g) Zabezpieczenia fizyczne informacji: • Cel: Zapewnienie bezpieczeństwa fizycznego przetwarzanym informacjom. • Ryzyko: Dostęp do informacji może być możliwy dla osób nieupoważnionych przez złe stosowanie zabezpieczeń. h) Bezpieczeństwo w pracy mobilnej i na odległość: • Cel: Wykonywana praca przez pracowników odbywa się bezpiecznie bez względu na miejsce pracy. • Ryzyko: Zagrożenie wycieku informacji, spowodowane niewłaściwą pracą mobilną i wykonywaną na odległość. i) Weryfikacja dostępu do informacji: • Cel: Ochrona przed nieautoryzowaną modyfikacją, usunięcie informacji. • Ryzyko: Informacja nie jest chroniona przed nieautoryzowaną modyfikacją i ochroną. j) Kontakty ze stronami trzecimi: • Cel: Zapewnienie bezpieczeństwa informacji podczas dostępu do informacji przez firmy zewnętrzne. • Ryzyko: Brak nadzoru nad dostępem do informacji przez firmy zewnętrzne. k) Postępowanie z informacją: • Cel: Zapewnienie minimalizacji wystąpienia ryzyka kradzieży informacji. • Ryzyko: Osoby nieuprawnione mają dostęp do informacji. l) Bezpieczeństwo teleinformatyczne: • Cel: Zapewnienie bezpieczeństwa przetwarzania informacji w systemach informatycznych: • Ryzyko: Systemy informatyczne nie są odpowiednio chronione. m) Działania związane z incydentami: • Cel: Organizacja posiada informacje na temat występowania incydentów. • Ryzyko: Organizacja nie reaguje i nie likwiduje przyczyn wystąpienia incydentów. n) Wykonywanie cyklicznych kontroli wewnętrznych: • Cel: Organizacja monitoruje i poprawia SZBI. • Ryzyko: Brak poprawnie działającego SZBI. Audyt KRI zostanie przeprowadzony w oparciu o istniejącą dokumentację, wizje lokalne, wywiady przeprowadzone z pracownikami Zamawiającego, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne oraz za administrację systemami informatycznymi oraz osobami użytkującymi systemy informatyczne. Postawą realizacji prac będzie norma wskazana w Rozporządzeniu KRI: PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu KRI będzie Raport indywidualny dla Zamawiającego, przedstawiający poziom bezpieczeństwa informacji zgodnie z wymaganiami KRI, a także zalecenia i rekomendacje w celu wypełnienia wymagań Rozporządzenia i podniesienia poziomu bezpieczeństwa informacji w niej gromadzonej i przetwarzanej. Załącznikiem do Raportu z Audytu KRI będzie dostarczony wzór Polityki Bezpieczeństwa Informacji dopasowany do organizacji. Po przeprowadzeniu Audytu KRI i opracowaniu Raportu Wykonawca przeprowadzi spotkanie z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi Zamawiającego, celem zaprezentowania wyników Audytu oraz zleceń i rekomendacji zawartych w Raporcie. III. Zamawiający przez „Audyt Bezpieczeństwa Sieci" rozumie badanie struktury sieci komputerowej oraz jej podatności na próby ataków pod kątem: nieautoryzowanego dostępu, luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych. Audyt Bezpieczeństwa Sieci obejmuje analizę wskazanych urządzeń, w tym w szczególności: a) sprawdzenie wybranych urządzeń

systemowych, b) badanie wskazanych serwerów, c) sprawdzenie wskazanych stacji roboczych. Zakres działań w zakresie Audytu Bezpieczeństwa Sieci obejmuje: a) Analizę topologii sieci komputerowych w instytucji: lokalizacje, strefy i klasy adresowe (badanie sieci pod kątem stref wykrytych adresów). b) Analizę połączenia sieci lokalnych z sieciami: własnymi (inne lokalizacje np. VPN), obcymi (np. MSWiA) i sieciami publicznymi - Internet. c) Analizę warstwy aktywnej sieci - UTM, Firewall, Router, Switch, VLAN ze wskazaniem dobrych praktyk w zakresie konfiguracji i określenia reguł w urządzeniach dostępowych. d) Testy wskazanych serwerów i hostów udostępniających zasoby lub usługi w sieci. e) Sprawdzenie zasad dostępu do zasobów i usług (połączenie, uwierzytelnienie). f) Sprawdzenie mechanizmów dotyczących odporności i wykrywania podatności na ataki wewnętrzne (DoS, ARP/MAC SPOOFING). g) Przygotowanie podstawowych zaleceń ochrony do wykrytych podatności sieci i serwerów. h) Analizę i zalecenia dotyczące centralizacji lub rozproszenia zasobów i usług oraz ich redundancji. i) Zalecenia dotyczące zasad utrzymania sieci. j) Analizę polityki dostępu do zasobów. Audyt Bezpieczeństwa Sieci zostanie przeprowadzony w oparciu o wizje lokalne, testowanie wybranych urządzeń oraz wywiady przeprowadzone z pracownikami Zamawiającego, w szczególności z osobami odpowiedzialnymi za bezpieczeństwo sieci oraz za administrację systemami informatycznymi. Postawą realizacji Audytu Bezpieczeństwa Sieci będzie norma PN-ISO/IEC 27001 „Technika informatyczna - Techniki Bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji-Wymagania". Rezultatem przeprowadzonego Audytu BS będzie Raport zawierający analizę wyników dla Zamawiającego, wraz z rekomendacjami i wskazaniem dodatkowych metod ochrony sieci i jej zasobów uwzględniająca plany rozwojowe. Raport powinien zawierać opis topologii sieci i wykryte podatności podzielone i przypisane, według stopnia zagrożenia, do jednej z grup: • grupa zagrożenia centralne (Infrastruktura i serwery): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie, • grupa zagrożenia klienckie (enduser): zagrożenia krytyczne, zagrożenia wysokie, zagrożenia średnie, zagrożenia niskie. Ponadto Raport zawierać będzie następujące informacje: • wykaz stref i adresów IP hostów poddanych testom, • wykaz udostępnionych zasobów sieciowych lub usług, do których dostęp można uzyskać bez podania poświadczeń, • zalecenia dotyczące polityki uwierzytelnienia użytkowników, • sugestie dotyczące zwiększenia stopnia bezpieczeństwa i wysokiej dostępności, indywidualne zalecenia dotyczące wykrytych podatności i planów rozwojowych audytowanego środowiska. Po przeprowadzeniu Audytu BS i opracowaniu Raportu Wykonawca zobowiązuje się do przeprowadzenia spotkania z osobami odpowiedzialnymi za bezpieczeństwo teleinformatyczne i za administrację systemami informatycznymi Zamawiającego, celem zaprezentowania wyników audytu oraz zleceń i rekomendacji zawartych w Raporcie. IV. Zakres współpracy 1. Do prawidłowego wykonania usług Wykonawca będzie miał zapewniony pełny dostęp do dokumentacji określającej sposób zabezpieczania informacji w audytowanej jednostce, dostęp do pomieszczeń niezbędnych w celu analizy systemu zabezpieczeń, struktura organizacyjna audytowanej jednostki. 2. W każdej audytowanej jednostce wskazana zostanie osoba do współpracy z Wykonawcą odpowiedzialna za bezpieczeństwo informacji w audytowanych jednostkach. 3.

Wywiad oraz weryfikacja przeprowadzane będą w zależności od dostępności osób, zaangażowanych w działanie w audytowanych jednostkach. 4. Wywiad polega na zadawaniu pytań krzyżowych oraz otwartych. Przeprowadzony będzie osobiście oraz za pomocą wszelkich dostępnych środków komunikacji zgodnie z Polityką Bezpieczeństwa danego podmiotu. 5. Zadanie uważa się za wykonane w momencie przekazania Zamawiającemu protokołu z wykonanych prac podpisanego przez osobę uprawnioną do reprezentowania audytowanej jednostki i Wykonawcę. 6. Wykonawca zobowiązany będzie do ustalenia z Zamawiającym harmonogramu prac w terminie 10 dni od daty podpisania umowy.

2) Wspólny Słownik Zamówień (CPV): 79212000-3

3) Wartość części zamówienia (jeżeli zamawiający podaje informacje o wartości zamówienia):

Wartość bez VAT:

Waluta:

4) Czas trwania lub termin wykonania: data zakończenia: 31/07/2017

5) Kryteria oceny ofert:

Kryteria	Znaczenie
Cena	50
Doświadczenie osób wyznaczonych do realizacji przedmiotu zamówienia	30
Termin realizacji	20

6) INFORMACJE DODATKOWE: