STAROSTWO POWIATOWE W ŻAGANIU

Starostwo Powiatowe w Żaganiu
ul. Dworcowa 39
68-100 Żagań
tel. 068 477 79 01, faks: 068 477 79 20
NIP: 924-16-33-119

ZP.271.21.2019 Żagań, 11 kwietnia 2019 r.

Powiat Żagański zwraca się z prośbą o przedstawienie oferty cenowej na zadanie pn. **„Opracowanie dokumentacji i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Żaganiu"**

I. Nazwa i adres Zamawiającego:

Powiat Żagański, ul. Dworcowa 39, 68-100 Żagań

II. Opis przedmiotu zamówienia:

opracowanie dokumentacji systemowej do wdrożenia w ramach wymagań **Krajowych Ram Interoperacyjności**

1. Wykonanie usługi opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie
2. Opracowanie dokumentacji musi być poprzedzone audytem diagnostycznym jako element rozpoznania i wymagań organizacyjno-technicznych Urzędu.
3. Wykonanie usługi opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie realizowane w oparciu o:
   a. ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2017 r., poz. 570 ze zm.),
   b. przepisy rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247),
   c. polskie normy PN-ISO/IEC 27001:2017, PN-ISO/IEC 27002/2014-12, PN-ISO/IEC 27005/2014-01 oraz PN-ISO/IEC 31000:2012,
   d. wytyczne Ministra Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych wydane dnia 15 grudnia 2015 roku
   e. z uwzględnieniem wymagań NIK w obszarze badania systemów teleinformatycznych i Krajowych Ram Interoperacyjności
4. Minimalny wymagany zakres audytu diagnostycznego zakończonego raportem w wersji wydrukowanej i elektronicznej to:

a) Wykonanie testów penetracyjnych infrastruktury ICT min.:

- Badanie luk systemów informatycznych (aplikacji).
- Badanie luk urządzeń sieciowych.
- Badanie luk baz danych.
- Badanie luk komputerów i notebooków.
- Badanie luk serwerów.
- Badanie luk sieci WiFi.
- Inwentaryzację otwartych portów.
- Analizę bezpieczeństwa stosowanych protokołów.
- Identyfikację podatności systemów i sieci na ataki typu: DoS, DDoS, Sniffing, Spoffing, XSS, Hijacking, Backdoor, Flooding, Password, Guessing i inne.
- Skanowanie aktywnych urządzeń sieci komputerowej, w tym routery, zapory (firewall), przełączniki, serwery i stacje robocze na występowanie luk/podatności w tych urządzeniach oraz błędów w konfiguracji zmniejszających poziom bezpieczeństwa systemów
- Badanie podatności i błędy w konfiguracji systemów będących w posiadaniu organizacji z uwzględnieniem poziomu ważności ze względu na bezpieczeństwo.
- skanowanie z autentykacją w celu potwierdzenia podatności systemu operacyjnego oraz oprogramowania pakietów biurowych i systemu poczty elektronicznej.
- Badanie legalności oprogramowania – scaning próby
- Badanie stacji roboczych – scannig próby kadrowej wraz z wywiadem socjotechnicznym kadr organizacji
- Badanie polityk zarządzania usługami.

- Badanie procesów autoryzacji.
- Badanie zarządzania uprawnieniami i logowanie zdarzeń.
- Badanie zarządzania zmianami konfiguracyjnymi i aktualizacjami.
- Ocenę konfiguracji systemu operacyjnego.
- Dostępność i ciągłość działania systemów .
- Analizę systemu zarządzania kopiami zapasowymi.
- Analizę bezpieczeństwa funkcji i protokołów specyficznych dla aplikacji /serwera.
- Ocenę mechanizmów bezpieczeństwa (firewalli).
- Analizę dostępów do urządzeń aktywnych
- Badanie routingu.
- Badanie redundancji rozwiązań

b) Badanie stanu i sposobu realizacji na dzień audytu
   - Badanie Procedur zarządzania systemami teleinformatycznymi.
   - Procedur planowania aktualizacji systemów teleinformatycznych.
   - Zasad ochrony przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.
   - Procedur zarządzania historią zmian.
   - Procedur zarządzania kopiami zapasowymi.
   - Procedur zabezpieczania nośników.
   - Polityk kontroli dostępu do systemów.
   - Zasad odpowiedzialności użytkowników.
   - Procedur dostępu do systemów operacyjnych.
   - Procedur dostępu i kontroli do usług internetowych.
   - Zasad zarządzania hasłami.
   - Zasad stosowania zabezpieczeń kryptograficznych.
   - Zasad kontroli eksploatowanego oprogramowania
   - Procedur kontroli zabezpieczeń komputerów przenośnych.
   - Bezpieczeństwa sieci LAN, WAN, WiFi.
   - Zasad użytkowania Internetu.
   - Zasad użytkowania systemów monitorujących.
   - Procedur rejestracji błędów.
   - Zasad funkcjonowania metod autoryzacji na stacjach roboczych.
   - Analiz stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe.
   - Weryfikacji zasad postępowania z urządzeniami przenośnymi w szczególności tymi, na których przetwarzane są dane osobowe.
   - Zasad wytycznych związanych z użytkowaniem sprzętu poza siedzibą.
   - Zasad funkcjonowania procedur bezpiecznego przekazywania sprzętu.
   - Niszczenie niepotrzebnych nośników.
   - Zasad funkcjonowania poprawności składowania danych elektronicznych.
   - Analiz procedur backupu (sposób wykonywania kopii bezpieczeństwa, zakres kopiowanych danych, przechowywanie kopii bezpieczeństwa), oraz procesu ich administracji.
   - Analiz planów ciągłości działania
c) Badanie i analizy dokumentacyjnej treści procedur i dokumentacji z obszaru Ochrony Danych Osobowych UODO i RODO na dzień audytu
d) Badanie jako próba audytowa i wywiad on-site dla badania stanu zabezpieczeń i realizacji wymagań m.in.:
   - Kontrola zabezpieczeń obszaru przetwarzania danych osobowych.
   - Kontrola zabezpieczeń pomieszczeń.
   - Kontrola zabezpieczeń zbiorów tradycyjnych.
   - Kontrola zabezpieczeń zbiorów archiwalnych.
   - Kontrola ochrony przed zdarzeniami losowymi.
   - Kontrola ochrony sprzętu przed kradzieżą.
   - Kontrola działania sytemu monitoringu.
   - Kontrola działania systemu alarmowego.
   - Weryfikacja dokumentów wewnętrznych Zamawiającego regulujących przetwarzanie danych osobowych.

- Przeprowadzenie analizy wytycznych w zakresie dostępu osób upoważnionych do przetwarzania danych osobowych.
- Weryfikacja ewidencji osób upoważnionych do przetwarzania danych osobowych.
- Przeprowadzenie analizy możliwości dostępu fizycznego do danych przez osoby nieupoważnione.
- Weryfikacja pracy użytkowników w obszarach, w których przetwarzane są dane osobowe.
- Weryfikacja sposobu przetwarzania danych osobowych.
- Weryfikacja kontroli nad przepływem danych osobowych.
- Weryfikacja przechowywania danych osobowych.
- Weryfikacja poufności, dostępności i udostępniania danych osobowych.
- Identyfikacja zagrożeń, słabych stron związanych z przetwarzania danych osobowych.
- Weryfikacja dostępu osób nieupoważnionych do miejsc, gdzie przetwarzane są dane osobowe.
- Weryfikacja zapisów umów ze stronami trzecimi (SLA)

e) Wykonanie przeglądów i badania stanu stron informacyjnych (www, itp.) pod kątem obowiązku informacyjnego i WCGA 2.0

Wynikiem przeprowadzonego audytu jest raport z w/w czynności wraz z wydaniem rekomendacji dla stwierdzonych niezgodności.

III. Minimalny wymagany zakres opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o normy ISO 27001, ISO 27005 , ISO 20000 jako dokumentacji realizującej wymagania art. 15, art. 20 Krajowych Ram Interoperacyjności to:

1. Procedury/zapisy przeprowadzania analizy ryzyka wraz z wsparciem informatycznym w obszarze zarządzania ochrona danych , szacowania ryzyka, planów minimalizacji ryzyka w ujęciu cyberbezpieczeństwa
2. Procedury/zapisy przeprowadzania wewnętrznych i zewnętrznych audytów, zawierających wskazanie: częstotliwości audytów; sposobu przygotowywania i zatwierdzania ich planów; sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.
3. Procedury/zapisy działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania. W szczególności procedura określać będzie: zdarzenia mogące zainicjować określenie i wprowadzenie działania korygującego; sposób analizy niezgodności i identyfikowania działań korygujących; sposób ich wprowadzania i dokumentowania; przegląd ich realizacji.
4. Procedury/zapisy wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania. W szczególności procedura określać będzie: zdarzenia mogące zainicjować określenie i wprowadzenie działań zapobiegawczych; sposób analizy zidentyfikowanych problemów i określanie działań zapobiegawczych; sposób ich wprowadzania i dokumentowania; przegląd ich realizacji.
5. Procedury/zapisy przeglądu systemu zarządzania, w szczególności określającej: częstotliwość przeglądów; zakres i sposób ich przeprowadzania; materiały źródłowe niezbędne do przeprowadzenia przeglądu; tryb wdrażania wniosków.
6. Procedury/zapisy nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania. W szczególności zostaną określone Zasady/zapisy wersjonowania, zatwierdzania, dystrybucji, przechowywania, archiwizowania i niszczenia dokumentów.
7. Procedury/zapisy nadzoru nad zapisami, określającej zasady/zapisy przechowywania, archiwizowania oraz niszczenia zapisów.
8. Procedury wymagań w zakresie zabezpieczeń teleinformatycznych.
9. Zasady/zapisy bezpiecznego przetwarzania informacji przez pracowników
10. Stosowanie zasady/zapisy czystego biurka i czystego ekranu.
11. Procedury wymagań zabezpieczenia stacji roboczych.
12. Zasady/zapisy klasyfikacji informacji i postępowania z informacjami klasyfikowanymi
13. Zasady/zapisy zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień.
14. Zasady/zapisy zarządzania dostępem do usług informatycznych, w tym usług sieciowych
15. Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami.
16. Zasady/zapisy publikacji informacji.
17. Zasady/zapisy wymiany danych z podmiotami zewnętrznymi.
18. Zasady/zapisy wewnętrznej wymiany danych

19. Zasady/zapisy postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach.
20. Zasady/zapisy wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych, z uwzględnieniem testowania bezpieczeństwa wprowadzanych rozwiązań.
21. Zasady/zapisy i wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych.
22. Zasady/zapisy zgłaszania podatności w mechanizmach przetwarzających informacje
23. Zasady/zapisy postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji.
24. Zasady/zapisy kontroli bezpieczeństwa informacji.
25. Zasady/zapisy zarządzania oprogramowaniem.
26. Zasady/zapisy zarządzania kopiami zapasowymi.
27. Zasady/zapisy zarządzania kopiami archiwalnymi.
28. Zasady/zapisy konserwacji i serwisu zabezpieczeń technicznych i systemów informatycznych.
29. Zasady/zapisy monitorowania bezpieczeństwa infrastruktury informatycznej.
30. Zasady/zapisy przygotowania urządzeń IT do ponownego użycia.
31. Zasady/zapisy wycofywania urządzeń IT z użycia.
32. Zasady/zapisy bezpiecznego korzystania z urządzeń mobilnych.
33. Zasady/zapisy bezpiecznej pracy zdalnej.
34. Zasady/zapisy ochrony przed złośliwym oprogramowaniem.
35. Zasady/zapisy zarządzania mechanizmami kryptograficznymi.
36. Zasady/zapisy monitorowania przepisów prawnych związanych z zabezpieczeniem przetwarzanych informacji oraz wprowadzania zmian wynikających z obowiązków prawnych.
37. Zasady/zapisy i wytyczne w zakresie ochrony fizycznej i technicznej infrastruktury IT.
38. Zasady/zapisy i wytyczne w zakresie monitorowania przepisów prawnych związanych z ochroną informacji.
39. Zasady/zapisy i wytyczne w zakresie bezpiecznej współpracy z podmiotami zewnętrznymi.
40. Wytyczne w zakresie bezpiecznego świadczenia usług związanych z przetwarzaniem informacji.
41. Zasady/zapisy i wytyczne w zakresie bezpieczeństwa osobowego w procesach rekrutacji i zarządzania personelem.
42. Zasady/zapisy/ wytyczne i dokumenty w zakresie ciągłości działania, w tym:
    a. ciągłość przetwarzania informacji,
    b. plan ciągłości działania dla sytuacji uniemożliwienia przetwarzania informacji,
    c. plan komunikacji kryzysowej na wypadek braku możliwości przetwarzania informacji,
    d. Zasady/zapisy testowania planu ciągłości działania.
43. Procedury/zapisy zarządzania usługami IT
    a. Projektowanie i wdrażanie nowych lub zmodyfikowanych usług.
    b. Zarządzanie poziomem usług.
    c. Raportowanie usług.
    d. Zarządzanie dostępnością usług.
    e. Zapewnienie ciągłości świadczenia usług.
    f. Budżetowanie i rozliczanie usług.
    g. Zarządzania pojemnością.
    h. Zarządzanie relacjami.
    i. Zarządzanie incydentami.
    j. Zarządzanie problemami.
    k. Zarządzanie konfiguracją
    l. Zarządzanie wydaniami.

IV. Minimalny zakres prac wdrożeniowo - audytowych:

1. Audyt Najwyższego Kierownictwa
2. Audyt próby Dyrektorów/Kierowników
3. Audyt próby kadrowej i stacji rob.
4. Audyt pionu IT i testy penetracyjne
5. Szkolenie z zakresu SZBI/KRI kadr kierowniczych min. 6 h/grupa
6. Szkolenie z zakresu SZBI/KRI kadr pracowniczych min. 5 grupach z pre i post testem wiedzy
7. Szkolenie wybranego max. 4 osobowego zespołu na audytora wewnętrznego ISO 27001 min. 3 dni zakończone egzaminem i wydaniem certyfikatu

V. W ramach realizacji zadania wymagany jest audyt nadzoru skuteczności opracowanego i wdrożonego systemu w okresie do 12 miesięcy od daty końcowego protokołu odbioru wykonania w/w usług.

VI. Opracowany system KRI/SZBI musi być zgodny i zintegrowany z dokumentacją oraz wymaganiami systemu ochrony badanych osobowych funkcjonującym w urzędzie.

VII. Warunki udziału w postepowaniu: - doświadczenie

a. Co najmniej 3 opracowanych systemów zarządzania bezpieczeństwem informacji (KRI/SZBI) wg standardu PN-ISO/IEC 27001 zakończone w okresie ostatnich 36 miesięcy w jednostkach administracji publicznej zakończony w okresie ostatnich 48 miesięcy jako SZBI/SMS.
b. Co najmniej 2 usługi polegające na przeprowadzeniu audytu bezpieczeństwa systemów teleinformatycznych, w tym testów penetracyjnych oraz analiz konfiguracji systemów ICT ora WCGA 2.0 pod kątem bezpieczeństwa, przy czym wartość każdej usługi była nie mniejsza niż 20 000 PLN brutto zakończone w okresie ostatnich 48 miesięcy.
c. Co najmniej dwie usługi polegające na przeprowadzeniu szacowania ryzyka w obszarze bezpieczeństwa informacji zgodnie z wymaganiami PN-ISO/IEC 27005:2014 w organizacji posiadającej rozproszoną strukturę, o liczbie zatrudnionych osób nie mniejszej niż 100 zakończone w okresie ostatnich 48 miesięcy.
d. Co najmniej jeden projekt powinien obejmować dostosowanie do wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w ramach usług zewnętrznych.

VIII. Warunki udziału w postepowaniu: - kwalifikacje zespołu audytowo-konsultacyjnego Zespół składający się z co najmniej 5 osóbw tym:

a. Kierownika o wykształceniu wyższym informatycznym, posiadającego certyfikat audytora wiodącego ISO/IEC 27001 i ISO/IEC 20000, ISO 22301 lub osób posiadających poszczególne certyfikaty
b. min. 1 audytor / ekspert o wykształceniu wyższym prawniczym oraz certyfikatem audytora ISO 27001,
c. Pozostali członkowie zespołu to osoby posiadające wykształcenie wyższe i doświadczenie w realizacji audytów z obszaru ochrony danych osobowych z min. certyfikatem audytora ISO 27001.

IX. Termin realizacji zadania: **do 29.11.2019** W ramach realizacji zadania wymagany jest audyt nadzoru skuteczności opracowanego i wdrożonego systemu w okresie do 12 miesięcy od daty końcowego protokołu odbioru wykonania w/w usług.

Ofertę prosimy dostarczyć w kopercie/opakowaniu z napisem: **„Opracowanie dokumentacji i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Żaganiu" do dnia 18 kwietnia 2019 r. do pokoju nr 18** w budynku Starostwa Powiatowego w Żaganiu ul. Dworcowa 39, 68-100 Żagań w godzinach pracy urzędu.

Zamawiający **dopuszcza** złożenie oferty w formie:
- elektronicznej na adres zamowienia.publiczne@powiatzaganski.pl (podpisany skan dokumentu)
- lub faxem na nr: 68 477-79-20 (podpisany dokument)

Osoba do kontaktu:
- Tomasz Makowski – Informatyk w dni robocze w godzinach od 8.00 do 15.00 tel. 730 940 040

W załączeniu przesyłamy :
- załącznik nr 1 – formularz ofertowy
- załącznik nr 2 – wykaz prac
- załącznik nr 3 – wykaz osób
- załącznik nr 3a - zobowiązanie do współpracy
- załącznik nr 3b - zobowiązanie innych podmiotów do udostepnienia osób niezbędnych do wykonania zamówienia

Z up. STAROSTY
Roman Śliwiński
Członek Zarządu