Opis Przedmiotu Zamówienia

Nazwa zadania: Audyt bezpieczeństwa według KRI Ośrodka Pomocy Społecznej w Rybniku.

Dane zamawiającego: Ośrodek Pomocy Społecznej ul. Żużlowa 25, 44-200 Rybnik.

Osoba do kontaktu: Tadeusz Króliczek e-mail: administracyjny@opsrybnik.pl. tel. 32 43 99 328

Termin realizacji zamówienia: 30 listopada 2021 roku

Przedmiot zamówienia:

Przeprowadzenie audytu dotyczącego spełnienia wymagań 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 2012 r., poz. 526) klasyfikowanego zgodnie z normą iso/iec 27001.

Celem audytu jest dokonanie oceny działania systemów teleinformatycznych pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz przestrzegania wymagań zawartych w Krajowych Ramach Interoperacyjności.

I. AUDYT OBEJMUJE NASTĘPUJĄCE GŁÓWNE OBSZARY:

1. Wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami/rejestrami informatycznymi i wspomagania świadczenia usług drogą elektroniczną.
2. Zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych podmiotów publicznych dla osób niepełnosprawnych.

II. SZCZEGÓŁOWA TEMATYKA I OBSZARY AUDYTU:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1) Usługi elektroniczne:
   a) świadczenie usług w formie elektronicznej w tym udostępnionej na platformie ePUAP, zgodnie z art. 16 ust. la ustawy o informatyzacji;
   b) zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI.

Dowodami z audytu są: dokumentacja usług elektronicznych podmiotu, w tym: lista usług świadczonych w formie elektronicznej, dokumentacja (wydruki) stron internetowych, itp.

2) Centralne repozytorium wzorów dokumentów elektronicznych.
3) Model usługowy:

Model usługowy został zdefiniowany w §2 pkt 8 rozporządzenia KRI. To model, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji (inaczej: system zorientowany na usługi).

Audytowi podlegają:

a) poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu, zgodnie z §15 ust. 2 rozporządzenia KRI;

b) weryfikacja sposobu zarządzania usługami w oparciu o ustalone procedury w tym możliwość zidentyfikowania właściciela merytorycznego usług (komórka organizacyjna podmiotu), ustalenie odpowiedzialności za utrzymanie usług od strony technicznej, określenie poziomu świadczenia usług, monitorowanie poziomu świadczenia usług na zadeklarowanym poziomie.

4) Współpraca systemów teleinformatycznych z innymi systemami.

Audytowi podlegają:

a) poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrami referencyjnymi, zgodnie z §5 ust. 3 pkt 3 rozporządzenia KRI;

b) sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI, zgodnie z §16 ust. 1 rozporządzenia KRI.

Dowodami z audytu są: umowy (porozumienia) z podmiotami prowadzącymi rejestry referencyjne dotyczące dostępu do danych referencyjnych uzyskiwanych w drodze wymiany, opis interfejsów systemu teleinformatycznego, dokumentacja systemu teleinformatycznego.

5) Obieg dokumentów w podmiocie publicznym.

Audytowi podlegają: regulacje wewnętrzne opisujące sposób zarządzania dokumentacją, w tym zakres stosowania elektronicznego obiegu dokumentów, zgodnie z §20 ust. 2 pkt 9 rozporządzenia KRI.

Dowodami z audytu są: dokumentacja systemu zarządzania dokumentacją, w tym procedury i zasady postępowania z dokumentami zawarte w instrukcjach kancelaryjnych oraz dokumentacja stosowania ww. procedur.

6) Formaty danych udostępniane przez systemy teleinformatyczne.

Audytowi podlegają:

a) sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu, zgodnie z §17 ust. 1 rozporządzenia KRI;

b) sposób udostępniania zasobów informatycznych z systemów teleinformatycznych, zgodnie z §18 ust. 1 rozporządzenia KRI;
c) sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne, zgodnie z §18 ust. 2 rozporządzenia KRI.

Dowodami z audytu są: opis formatów danych w systemach podmiotu, dokumentacja systemu teleinformatycznego.

2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym możliwości skutecznego zarządzania bezpieczeństwem informacji w podmiocie.

1) **Dokumenty z zakresu bezpieczeństwa informacji: Polityka Bezpieczeństwa Informacji oraz funkcjonujące w jej** ramach inne polityki, regulaminy i procedury.

Audytowi podlegają:

a) dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI, Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI, zgodnie z §20 ust. 1 rozporządzenia KRI;
b) działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI, zgodnie z §20 ust. 2 pkt 1 rozporządzenia KRI;
c) stopień zaangażowania kierownictwa podmiotu w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI (przeglądy SZBI, szacowanie

i obsługa ryzyka BI, egzekwowanie działań związanych z BI), zgodnie z §20 ust. 2 rozporządzenia KRI.

Dowodami z audytu są: dokumentacja SZBI w tym polityka BI oraz inne dokumenty stanowiące SZBI, dokumentacja z przeglądów SZBI, dokumentacja audytów z zakresu BI, dokumentacja zmian wynikających z wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI.

2) Analiza zagrożeń związanych z przetwarzaniem informacji.

Audytowi podlegają:

a) regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w podmiocie;
b) dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem, zgodnie z §20 ust. 2 pkt 3 rozporządzenia KRI;.
c) działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka.

Dowodami z audytu są*:* dokumentacja zarządzania ryzykiem w tym: procedura przeprowadzania analizy ryzyka, rejestr ryzyk, plan postępowania z ryzykiem, dowody utrzymywania i doskonalenia systemu zarządzania ryzykiem oraz dokumentacja zmian w zabezpieczeniach związanych z bieżącą analizą ryzyka.

3) Inwentaryzacja sprzętu i oprogramowania informatycznego.

Audytowi podlegają:

a) regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych;
b) rejestr zasobów teleinformatycznych zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku, zgodnie z §20 ust. 2 pkt 2 rozporządzenia KRI;
c) sposób aktualizacji rejestru zasobów teleinformatycznych.

***Dowodami z audytu są**:* dokumentacja zarządzania sprzętem i oprogramowaniem, w tym: rejestr zasobów informatycznych, procedury prowadzenia rejestru zasobów informatycznych, procedury przydzielania, zwrotu sprzętu i oprogramowania, procedury korzystania z zasobów informatycznych przez użytkowników oraz dokumentacja wykonywania ww. procedur.

4) Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Audytowi podlegają:

a) regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych;
b) adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień), zgodnie z §20 ust. 2 pkt 4 rozporządzenia KRI;
c) działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.;
d) sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych, zgodnie z §20 ust. 2 pkt 5 rozporządzenia KRI.

***Dowodami z audytu są**:* dokumentacja zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym procedury nadawania, zmiany i odbierania uprawnień do pracy w systemach teleinformatycznych i dokumentacja wykonywania ww. procedur.

5) Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Audytowi podlegają:

a) regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych
w procesie przetwarzania informacji w systemach teleinformatycznych;
b) dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach,

wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń, zgodnie z §20 ust. 2 pkt 6 rozporządzenia KRI.

Dowodami z audytu są: dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji, w tym: agendy szkoleń i listy uczestników.

6) Praca na odległość i mobilne przetwarzanie danych.

Audytowi podlegają:

a) regulacje wewnętrzne określające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, zgodne z §20 ust. 2 pkt 8 rozporządzenia KRI;
b) działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość.

Dowodami z audytu są: dokumentacja dotycząca zarządzania urządzeniami przenośnymi i pracą na odległość, w tym: procedury bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość.

7) Serwis sprzętu informatycznego i oprogramowania.

Audytowi podlegają:

a) regulacje wewnętrzne, w których określono zasady współpracy z podmiotami zewnętrznymi
w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym wymagane klauzule prawne;
b) umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI, zgodne z §20 ust. 2 pkt 1 Rozporządzenia KRI.

Dowodami z audytu są: zapisy umów serwisowych oraz umów dotyczących rozwoju systemów teleinformatycznych.

8) Procedury zgłaszania incydentów naruszenia BI.

Audytowi podlegają:

a) regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji;
b) sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL, zgodnie z §20 ust. 2 pkt 13 rozporządzenia KRI.

Dowodami z audytu są: dokumentacja postępowania z incydentami naruszenia BI w tym rejestr incydentów naruszenia BI, procedury zgłaszania i postępowania z incydentami, dokumentacja wykonywania ww. procedur.

9) Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Audytowi podlegają:

a) regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;
b) sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z §20 ust. 2 pkt 14 rozporządzenia KRI;
c) działania podjęte w wyniku zaleceń poaudytowych.

Dowodami z audytu są: dokumentacja audytów z zakresu BI i dokumentacja realizacji zaleceń poaudytowych.

10) **Kopie zapasowe.**

Audytowi podlegają:

a) określenie zasad tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu, zgodnie §20 ust. 2 pkt 12 lit. b rozporządzenia KRI;
b) działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja z tych działań.

Dowodami z audytu są: dokumentacja wykonywania kopii zapasowych w tym: procedury wykonywania, przechowywania i testowania kopii zapasowych oraz dokumentacja wykonywania ww. procedur.

11) Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.

Audytowi podlegają:

a) zapewnienie warunków dla uzyskania odpowiedniej funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności

systemów informatycznych w fazie ich projektowania, wdrażania i eksploatacji, zgodnie z §15 ust. 1 rozporządzenia KRI;

b) regulacje wewnętrzne opisujące wymagania w zakresie projektowania systemów teleinformatycznych dotyczące architektury systemu, sposób licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągnięcia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu;
c) regulacje wewnętrzne opisujące wymagania w zakresie wdrażania systemów teleinformatycznych

   w dotyczące: sposobu dostarczenia i instalacji systemu teleinformatycznego, wymagań sprzętowych i środowiskowych dla systemu;
d) regulacje wewnętrzne opisujące sposób przeprowadzania zmian w systemach teleinformatycznych (w trakcie ich eksploatacji) w tym opis: sposobu zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany;
e) regulacje wewnętrzne opisujące proces monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanych wobec wzrostu ilości systemów teleinformatycznych, ilości przetwarzanych danych, ilości użytkowników poprzez podejmowanie działań zapobiegawczych;
f) działania związane z wdrażaniem nowych systemów teleinformatycznych oraz wprowadzaniem zmian w systemach eksploatowanych;
g) działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności;
h) działania zapobiegawcze będące wynikiem dostrzeżonych problemów podczas monitorowania ich pracy.

Dowodami z audytu są: dokumentacja wdrożeń nowych systemów teleinformatycznych, dokumentacja wprowadzanych zmian w systemach eksploatowanych, dokumentacja monitorowania systemów teleinformatycznych oraz działań zapobiegawczych będących wynikiem dostrzeżonych problemów podczas monitorowania.

12) Zabezpieczenia techniczno-organizacyjne dostępu do informacji.

Audytowi podlegają:

a) regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem, zgodne z §20 ust. 2 pkt 11 rozporządzenia KRI;

b) regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie, zgodnie z §20 ust. 2 pkt 7 i 9 rozporządzenia KRI;

c) działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związane z monitorowaniem ruchu osobowego w podmiocie, zgodnie z § 20 ust. 2 pkt 7 lit a) rozporządzenia KRI;

d) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia BI, zgodnie z §20 ust. 2 pkt 7 lit b) rozporządzenia KRI;

e) działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych
i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem, zgodnie z § 20 ust. 2 pkt 7 lit c) rozporządzenia KRI;

f) działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji,

w tym urządzeń mobilnych, zgodne z wynikami analizy ryzyka i planem postępowania z ryzykiem;

g) działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI.

Dowodami z audytu są: dokumenty wprowadzające stosowanie zabezpieczeń, dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń, dokumentacja wykonywania ww. procedur.

13) Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

Audytowi podlegają:

a) regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem, zgodnie z §20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI;

b) działania związane z aktualizacją oprogramowania oraz redukcją ryzyk, aktualizacją oprogramowania antywirusowego i antyspamowego, aktualizacją oprogramowania zabezpieczającego ruch sieciowy;

c) działania związane z minimalizowaniem ryzyka utraty informacji w wyniku awarii oraz ochroną przed błędami, utratą i nieuprawnioną modyfikacją a także zapewnienie bezpieczeństwa plików systemowych poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych, w tym np.: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia, monitorowania parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci;

d) działania związane z zastosowaniem mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa poprzez stosowanie zabezpieczeń kryptograficznych np.: dla transmisji do urządzeń mobilnych, poczty elektronicznej, a także podpisów kwalifikowanych do autoryzacji dokumentów;

e) działania podejmowane w związku z dostrzeżeniem nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
f) działania związane z kontrolą zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Dowodami z audytu są: plan postępowania z ryzykiem, dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń i dokumentacja wykonywania ww. procedur.

14) Rozliczalność działań w systemach informatycznych.

Audytowi podlegają:

a) regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych, zgodnie z §21 rozporządzenia KRI;
b) działania związane z zapewnieniem rozliczalności użytkowników, szczególnie posiadających uprawnienia: administrowania systemami użytkowymi, zmiany konfiguracji systemów operacyjnych i ich zabezpieczeń, przetwarzania danych podlegających prawnej ochronie;
c) działania związane z zapewnieniem rozliczalności działań użytkowników lub obiektów systemowych a także rejestracji innych zdarzeń systemowych w zakresie wynikającym z analizy ryzyka;
d) działania związane z regularnym przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych;
e) okres i sposób przechowywania dzienników systemowych.

Dowodami z audytu są: dokumenty zawierające analizę ryzyka, dokumentacja dzienników systemowych, w tym: procedury prowadzenia i dostępu do dzienników systemowych oraz dokumentacja wykonywania ww. procedur.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

Uwzględniając potrzeby osób niepełnosprawnych podmiot powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie

się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z §19 rozporządzenia KRI w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia. Termin dostosowania systemów teleinformatycznych do prezentacji zasobów informacyjnych wg powyższego standardu minął 30 maja 2015 r.

Audytowi podlegają: sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu, zgodnie z §19 rozporządzenia KRI.
Dowodami z audytu są: Opis zastosowanych rozwiązań technicznych umożliwiających osobom niedosłyszącym lub niedowidzącym zapoznanie się z treścią informacji na stronach internetowych systemów teleinformatycznych podmiotu, dokumentacja systemu teleinformatycznego.

III. ZAPLANOWANIE AUDYTU

1. Przeprowadzenie audytu

Konsultanci mają określić spełnienie poszczególnych wymagań na podstawie analizy zapisów z realizowanych procesów, analizy dostarczonej dokumentacji, rozmów i wywiadów z pracownikami a także weryfikacji bezpieczeństwa przetwarzania danych (np. ochrona wydruków, niszczenie informacji, itp.).
Obok audytu procesowego, konsultanci będą mogli zapoznać się także z zabezpieczeniami technicznymi stosowanymi w podmiocie. W tym celu zweryfikowana zostanie skuteczność stosowanych mechanizmów bezpieczeństwa fizycznego, a także poprawność utrzymania posiadanych urządzeń (np. okresowe przeglądy systemów alarmowych, kontroli dostępu itp.). Wymagana jest co najmniej 1 wizyta audytora w siedzibie Zamawiającego celem zapoznania się z stanem faktycznym dokumentacji, zabezpieczeń.

2. Opracowanie i przedstawienie wyników

Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, opracowany zostanie pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian. W tym celu konsultanci przygotują mapę spełnienia wymagań

Rozporządzenia lub normy – w opracowaniu której uwzględnione zostaną wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali:

1) **spełnione** – oznacza, że wymaganie normy zostało całkowicie wdrożone,
2) **częściowo spełnione** – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego" jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników),
3) **niespełnione** – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

3. Plan prac audytowych.

Plan prac może podlegać szczegółowym ustaleniom i związanym z tym zmianom. Poszczególne etapy mogą być realizowane równolegle.

IV. W RAMACH AUDYTU PRZEPROWADZONE MAJĄ ZOSTAĆ TESTY PENETRACYJNE INFRASTRUKTURY IT.

Zakres testów.

Przedmiotem prowadzonej analizy bezpieczeństwa mają być usługi sieciowe dostępne z sieci Internet pod adresem IP zawierającymi się w jednej z publicznych przestrzeni adresowych należących lub użytkowanych przez Zamawiającego -188.137.112.130 (1 punkty styku z siecią Internet),

Wyżej wymieniony adres będzie sprawdzany na wszystkich portach TCP/UDP 1-65535.

W podanej przestrzeni adresowej działają m.in. tunele VPN.

Testy bezpieczeństwa będą wykonywane z perspektywy „zerowej" wiedzy o testowanym obiekcie (black-box testing).

Testy bezpieczeństwa składać się będą z następujących po sobie etapów:

- rozpoznanie badanego systemu informatycznego lub jego elementów,
- analiza podatności na zagrożenia na podstawie uzyskanych informacji,
- wykonanie kontrolowanych ataków i zweryfikowanie podatności; ataki typu DDoS (unieruchomienia usługi) powinny być wykonane na żądanie i w uzgodnionym z Zamawiającym terminie,
- sporządzenie listy wykrytych luk wraz z oceną realnego zagrożenia.

Testom powinny zostać poddane:

a) sieciowe urządzenie brzegowe,
b) router i brama,
c) system firewall,
d) serwery obsługujące połączenia VPN,
e) systemy antywirusowe,
f) systemy wykrywania włamań (IDS),
g) systemy przeciwdziałania włamaniom (IPS),
h) serwery aplikacji,
i) serwery DNS,
j) systemy operacyjne.

Testy powinny umożliwić wykrycie:

a) możliwości uzyskania nieautoryzowanego dostępu do sieci wewnętrznej organizacji,
b) możliwości wykorzystania sieci organizacji do przeprowadzania ataków na inne sieci,
c) możliwości omijania wdrożonych systemów zabezpieczeń,
d) obecności znanych błędów i luk bezpieczeństwa w stosowanych urządzeniach sieciowych i oprogramowaniu,
e) podatności sieci na propagację oprogramowania złośliwego,
f) zagrożeń dla dostępności, poufności oraz integralności przetwarzanych informacji,
g) możliwości przejęcia nieautoryzowanej kontroli nad usługami lub serwerami,
h) możliwości nieautoryzowanego zwiększenia uprawnień przez użytkowników usług,
i) możliwości manipulacji usługami świadczonymi przez serwery,
j) możliwości destabilizacji i zablokowania pracy serwerów.

W przypadku stwierdzenia podatności krytycznych Wykonawca musi o nich niezwłocznie powiadomić Zamawiającego.

Produktem końcowym testów ma być raport zawierający:

a) zakres testów bezpieczeństwa i opis przeprowadzonych działań,
b) listę wykrytych zagrożeń i nieprawidłowości,
c) ocenę wykrytych zagrożeń wg skali: niska, średnia, krytyczna,
d) propozycje usprawnień mające na celu wyeliminowanie wykrytych zagrożeń, gdzie przedstawione rekomendacje mogą dzielić się na rekomendacje tymczasowe (tj. doraźnie rozwiązanie problemu) oraz rekomendacje docelowe, czyli opis stanu oczekiwanego, którego osiągnięcie pozwala na całkowite wyeliminowanie podatności.

V. PO ZAKOŃCZENIU AUDYTU.

Wykonawca zapewni opiekę doradczą w zakresie zaleceń zawartych w raportach, przez okres **3 miesięcy** od zakończenia audytu.

VI TERMIN SKŁADANIA OFERT: 13.10.2021 ROKU

Składanie ofert.

Oferty należy składać w formie elektronicznej (zeskanowany formularz ofertowy podpisany przez osoby uprawnione do reprezentacji Wykonawcy) na adres administracyjny@opsrybnik.pl lub w formie papierowej w Sekretariacie Ośrodka Pomocy Społecznej ul. Żużlowa 25, 44-200 Rybnik, z dopiskiem na kopercie: Oferta na zadanie: „Audyt bezpieczeństwa według KRI" zgodnie z załącznikiem nr 1 do Opisu Przedmiotu Zamówienia.

VII INFORMACJE O FORMALNOŚCIACH:

1) Jeżeli Wykonawca, którego oferta została wybrana uchyli się od podpisania umowy, Zamawiający wybierze kolejną ofertę najkorzystniejszą spośród złożonych ofert, bez przeprowadzania ich ponownej oceny.
2) W niniejszym postępowaniu nie mają zastosowania przepisy Ustawy Prawo zamówień publicznych.
3) Zamawiający zastrzega sobie możliwość nie dokonania wyboru oferty, bez podania przyczyny.

4) W postępowaniu może wziąć udział Wykonawca, który dysponuje zespołem minimum dwóch specjalistów z kwalifikacjami popartymi posiadaniem niżej wyszczególnionych certyfikatów:
    a. audytorzy muszą posiadać certyfikat audytora wewnętrznego SZBI wg wymagań normy ISO27001 lub certyfikat audytora wiodącego SZBI wg wymagań normy ISO 27001:2005.
    b. zespół audytorów musi udokumentować łącznie stosownymi certyfikatami posiadanie wiedzy z zakresu: ochrony danych osobowych, analizy ryzyka, przeprowadzenia analizy bezpieczeństwa w kontekście rozporządzenia KRI oraz umiejętności opracowania stosownej dokumentacji w tym zakresie dla Ośrodka.
5) Wykonawca musi posiadać doświadczenie w przeprowadzaniu co najmniej 3 audytów bezpieczeństwa informacji w ciągu 2 lat w urzędach administracji publicznej lub jednostkach samorządu terytorialnego.
6) W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z formularzem oferty: certyfikatów oraz wykazu zrealizowanych audytów bezpieczeństwa informacji w urzędach administracji publicznej lub jednostkach samorządu terytorialnego.

VIII KRYTERIA OCENY OFERT: 100% CENA.

Za najkorzystniejszą zostanie uznana oferta z najniższą ceną

IX OBOWIĄZEK INFORMACYJNY WYNIKAJĄCY Z ART. 13 RODO

Zgodnie z art. 13 ust. 1 i 2 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- administratorem Pani/Pana danych osobowych jest Dyrektor Ośrodka Pomocy Społecznej z siedzibą przy ul. Żużlowej 25, 44-200 Rybnik*;*
- inspektorem ochrony danych osobowych w *Ośrodku Pomocy Społecznej* jest Pan Wacław Knura*, kontakt: e-mail: iod@opsrybnik.pl, tel.: 32 43 99 319**;
- Pani/Pana dane osobowe przetwarzane będą w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia poza ustawą PZP;

- Dane osobowe mogą być udostępniane podmiotom upoważnionym do uzyskania informacji na podstawie przepisów prawa;
- Podanie danych osobowych jest dobrowolne, ale niezbędne do przeprowadzenia postępowania;
- Dane osobowe będą przechowywane jedynie w okresie niezbędnym do spełnienia celu, dla którego zostały zebrane lub w okresie wskazanym przepisami prawa;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

** Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania ani zmianą istotnych postanowień umowy;*

*** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania z ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

Załączniki:

- Załącznik nr 1 - formularz ofertowy
- Załącznik nr 2- wzór umowy
- Załącznik nr 3 – wzór umowy powierzenia przetwarzania danych osobowych