Lublin, dnia 21 listopada 2017r.

OGŁOSZENIE (Zapytanie ofertowe)

na udzielanie zamówienia publicznego bez stosowania ustawy Prawo Zamówień Publicznych - przy zastosowaniu dyspozycji wynikającej z art. 4 pkt 8.

I. NAZWA I ADRES OGŁOSZENIODAWCY

Województwo Lubelskie z siedzibą w Lublinie, ul. Artura Grottgera 4, 20 – 029 Lublin

II. NAZWA PRZEDMIOTU ZAMÓWIENIA, Z OKREŚLENIEM CZY JEST TO DOSTAWA, USŁUGA CZY ROBOTA BUDOWLANA

Przedmiotem zamówienia jest usługa:

Wykonanie audytu bezpieczeństwa – oceny ryzyka oraz zgodności z General Data Protection Regulation (RODO)

III. OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest wykonanie audytu informatycznego - oceny ryzyka oraz analizę zgodności systemów dziedzinowych w związku z Rozporządzeniem 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), zwanym dalej RODO. Audyt obejmuje analizę wszystkich systemów informatycznych Zamawiającego w których przetwarzane są dane osobowe, systemów krytycznych określonych w Polityce Bezpieczeństwa Informacji, analizę zasobów informatycznych w tym zasoby sprzętowe, oprogramowanie dziedzinowe, usługi publiczne a także analizę potrzeb bieżących i przyszłych.

Wymagania Zamawiającego zostały zawarte w niniejszym Ogłoszeniu i we Wzorze Umowy stanowiącym Załącznik nr 2 do niniejszego Zapytania ofertowego.

Przekazanie Zamawiającemu oferty Wykonawcy jest równoznaczne z akceptacją zapisów Wzoru Umowy i gotowość Wykonawcy do jej podpisania. Zamawiający przedstawia szczegółowy opis przedmiotu zamówienia, tzn. minimalne wymagania Zamawiającego odnośnie przedmiotu zamówienia, które musi spełnić Wykonawca:

IV. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. PRODUKTY ZAMÓWIENIA

Produkty wymagane do dostarczenia przez Wykonawcę w formie papierowej i elektronicznej (w tym edytowalnej), (obie formy produktów muszą zostać potwierdzone, odpowiednio, podpisem odręcznym i kwalifikowanym przez Wykonawcę):

1. PRODUKTY DO REALIZACJI:

1.1. Bezpieczeństwo organizacji i zgodność z prawem

1.1.1. Bezpieczeństwo organizacyjne
1.1.2. Rejestr ryzyka
1.1.3. Audyt zgodności z GDPR
1.1.4. Audyt ochrony danych

1.2. Bezpieczeństwo IT

1.2.1. Audyt „Przed (AS IS)”
1.2.2. Obszar bezpieczeństwa sieciowego
1.2.3. Obszar oprogramowania
1.2.4. Obszar bezpieczeństwa sprzętowego

1.3. Bezpieczeństwo fizyczne (wybrane elementy, safety)

1.3.1. Monitoring wizyjny (CCTV)
1.3.2. Fizyczny dostęp do wyposażenia

1.4. Audyt potrzeb użytkowników

1.5. Dokumentacja audytu (podsumowanie)

1.5.1. Przekazane dokumenty
1.5.2. Warianty inwestycyjne

2. SPECYFIKACJA ZAKRESU AUDYTU I ANALIZ

2.1. Informacje ogólne

Za każdym razem gdy w przedmiocie zamówienia jest mowa o urządzeniach (serwerach, osprzęcie sieciowym, kamerach CCTV i innych elementach sprzętowych) należy przyjąć, że w ramach audytu bezpieczeństwa konieczne jest zweryfikowanie:

a) aktualności firmware,
b) zgodności konfiguracji z posiadaną przez Zamawiającego dokumentacją,
c) konfiguracji urządzeń pod kątem bezpieczeństwa (wymagane przedmiotowe kompetencje przez osobę wykonującą tę czynność),
d) połączeń fizycznych urządzeń do sieci komputerowej oraz elektrycznej ze szczególnym uwzględnieniem wysokiej dostępności,
e) poprawność podziału na podsieci względem użytej adresacji, poprawność przypisania adresów do urządzeń,
f) hierarchiczności i logiki przypisania adresacji,
g) konfiguracji portów,
h) weryfikacji wykorzystania połączeń uplinkowych,
i) podziału na sieci wirtualne (VLAN),

j) jednoznacznej identyfikacji urządzeń,
k) weryfikacji konfiguracji protokołu SNMP w zakresie udostępniania informacji przy zachowaniu zasad bezpieczeństwa,
l) wszystkich warstw modelu ISO/OSI inwentaryzowanych urządzeń,
m) uruchomionych protokołów,
n) aktywnych list dostępu,
o) uruchomionych usług,
p) ustawienia serwów czasu oraz usług mających wpływ na prawidłową pracę sprzętu,
q) loginów, haseł oraz metod autoryzacji użytkowników.

Za każdym razem gdy w przedmiocie zamówienia jest mowa o oprogramowaniu (systemach operacyjnych, serwerach baz danych, www i innych usługach serwerowych, stacjach roboczych użytkowników), należy przyjąć, że w ramach audytu bezpieczeństwa konieczne jest zweryfikowanie:

a) zasad przydzielania dostępu,
b) częstotliwość aktualizacji,
c) aktualności wersji systemów operacyjnych oraz polityka implementacji poprawek,
d) poprawności podłączenia i konfiguracji interfejsów sieciowych, obciążenia, oznaczenie urządzenia nazwą DNS i adresem IP,
e) dostępu administracyjnego,
f) działających usług,
g) otwartych portów,
h) możliwości wirtualizacji,
i) konieczności migracji na nowy system,
j) przeglądu konfiguracji poszczególnych usług uruchomionych w systemach operacyjnych Windows Server oraz Linux,
k) ustawienia serwów czasu oraz usług mających wpływ na prawidłową pracę sprzętu,
l) uprawnień użytkownika na stacji roboczej,
m) możliwości podłączenia urządzeń zewnętrznych,
n) ustawień zabezpieczeń stacji roboczych łączenie z oprogramowaniem antywirusowym,
o) kopii bezpieczeństwa stacji roboczych,
p) oprogramowania zainstalowanego na stacjach roboczych,
q) procedur zarządzania stacjami roboczymi oraz oprogramowaniem serwerowym w zakresie ustawień Active Directory,
r) dostępów do zasobów serwerów i stacji roboczych,
s) logów serwerów, stacji roboczych, aplikacji serwerowych,
t) loginów, haseł oraz metod autoryzacji użytkowników.

Za każdym razem gdy w przedmiocie zamówienia jest mowa o dokumentacji (sieci, oprogramowania, bezpieczeństwa, procedur oraz procesów biznesowych i innej), należy przyjąć, że w ramach audytu bezpieczeństwa konieczne jest zweryfikowanie:

a) celowości wytworzonej dokumentacji,
b) zgodności z oczekiwaniami Zamawiającego w zakresie merytorycznym posiadanej dokumentacji,
c) oczekiwanej ciągłości działania organizacji Zamawiającego,
d) przywrócenia do działania organizacji Zamawiającego po awarii (Disaster Recovery),
e) podjęcia akcji w przypadku wystąpienia i zidentyfikowania działań mających na celu destabilizację otoczenia Zamawiającego,
f) porycia dokumentacją obszarów biznesowych i technicznych organizacji Zamawiającego,

g) interesariuszy w kontekście wystąpienia zmian w otoczeniu Zamawiającego (należy przez to rozumieć zmiany wynikające z celowych działań Zamawiającego oraz zmiany wynikające z działań zewnętrznych),
h) zawartych umów i kontraktów serwisowych w kontekście realizacji zadań oczekiwanych przez Zamawiającego oraz ich wpływu na organizację Zamawiającego. Należy zweryfikować fizyczny sposób realizacji zawartych umów przez Dostawców/Wykonawców/Pracowników Zmawiającego w kontekście zachowania najwyższego poziomu bezpieczeństwa.

2.1. Bezpieczeństwo organizacji i zgodność z prawem

2.1.1. Bezpieczeństwo organizacyjne

2.1.1.1. Audyt zależności służbowych

Audyt będzie mieć na celu wykazanie zależności w strukturze organizacyjnej, które mogą mieć negatywny wpływ na bezpieczeństwo danych osobowych lub naruszać zasady bezpieczeństwa, wraz z informacją o sposobach rozwiązania zidentyfikowanych problemów.

2.1.1.2. Audyt zastępowalności

Audyt będzie mieć na celu wykazanie skutków braku osób pełniących konkretne funkcje w organizacji na jej funkcjonowanie, opisanie ich wraz z informacją o sposobach rozwiązania zidentyfikowanych problemów.

2.1.1.3. Audyt interesariuszy

Audyt będzie mieć na celu wykazanie wszystkich stron mających wpływ na bezpieczeństwo lub powiązanych z obszarem bezpieczeństwa w organizacji. Badane jest otoczenie bliższe i dalsze w celu wizualizacji związków, które na pierwszy rzut oka nie powinny mieć wpływu na bezpieczeństwo, a w ostatecznych rozrachunku okazują się istotne.

2.1.2. Rejestr ryzyka

Rejestr ryzyka jest dokumentem, który będzie prowadzony od początku do końca audytu. W ramach rejestru będą notowane wszystkie zidentyfikowane ryzyka, wraz z informacją o sposobie zmniejszenia wpływu na organizację i punktową oceną tego wpływu. Konstrukcja rejestru ryzyka musi umożliwiać identyfikację i ocenę wpływu ryzyka na organizację oraz przyjęcie harmonogramu prac w zakresie obniżenia negatywnych skutków wystąpienia ryzyka.

2.1.3. Audyt zgodności z GDPR

2.1.3.1. Przegląd przyjętych zasad bezpieczeństwa korespondujących z GDPR

Przegląd będzie mieć na celu wykazanie elementów zgodnych i niezgodnych z GDPR oraz opisanie proponowanych rozwiązań. W ramach przeglądu przyjętych zasad dokonany będzie Audyt ich zgodności z przepisami prawa, w rozumieniu sposobu realizacji konkretnych wymagań w obszarze organizacyjnym i technicznym.

2.1.3.2. Możliwość demonstracji przyjętych zasad w zgodności z GDPR

W ramach zadania badana będzie możliwość wskazania określonych zasad, którymi kieruje się organizacja w celu zachowania zgodności z GDPR. Przez demonstrację należy rozumieć konkretne czynności mające na celu wskazanie przyjętych środków bezpieczeństwa.

2.1.3.3. Identyfikacja zbiorów danych wymagających ochrony

W ramach działania musi zostać wykonany spis znanych zbiorów danych osobowych oraz zbiorów informacji, mających istotny wpływ na organizację.

2.1.3.4. Identyfikacja zakresu danych możliwych do przetwarzania

Dla każdego ze zidentyfikowanych zbiorów musi zostać wykonany Audyt porównawczy zakresu informacji przechowywanych w zbiorze na zgodność z faktycznymi wymaganiami dotyczącymi ich przetwarzania.

2.1.3.5. Audyt zgodności zakresów z posiadanymi zezwoleniami do przetwarzania

Dla każdego ze zbiorów musi zostać wykonany Audyt porównawczy zgody dotyczącej przetwarzania danych, którą wyraża osoba fizyczna, do zakresu danych, którymi dysponuje organizacja.

2.1.3.6. Audyt zgodności procesów przetwarzania danych w perspektywie czasu

Dla każdego ze zbiorów musi zostać wykonany Audyt, który jest estymacją wskazującą na możliwość przetwarzania danych we wskazanym zakresie oraz czasie. Na podstawie Audytu identyfikowane będą zbiory danych, których przetwarzanie powinno zakończyć się w określonym czasie.

2.1.3.7. Identyfikacja podstaw prawnych do legalnego przetwarzania danych

W ramach zadania muszą zostać identyfikowane podstawy prawne umożliwiające przetwarzanie wybranych danych. Identyfikacja jest częścią procesu umożliwiającego wskazanie ścieżki dla legalności prowadzonych działań w zakresie przetwarzania danych.

2.1.3.8. Zachowanie równowagi pomiędzy interesami osoby fizycznej, a przepisami prawa

Zadanie będzie mieć na celu określenie interesu organizacji do zakresu danych, które przetwarza. Celem zadania jest ochrona organizacji przez uporczywymi próbami wymuszenia usunięcia danych konkretnej osoby z posiadanych zbiorów

2.1.3.9. Audyt pod kątem posiadania i przetwarzania danych wrażliwych

Audyt będzie mieć na celu identyfikację zbiorów danych, w których przetwarzane są dane wrażliwe.

2.1.3.10. Audyt informacji o posiadanych zbiorach danych oraz odpowiedzialności za dane

W ramach Audytu należy wykazać konkretne zbiory danych wraz z przypisaniem odpowiedzialności za przetwarzanie danych w takim zbiorze. Informacja powinna być prosta i jednoznaczna, tak aby w przypadku kontroli lub zapytania możliwe było przekazanie wszystkich wymaganych informacji.

2.1.3.11. Audyt możliwości przeniesienia danych

Audyt będzie mieć na celu wskazanie możliwości przeniesienia danych do innego podmiotu (dane wędrujące wraz z osobą). Badane będą możliwości organizacyjne i techniczne w zakresie przeniesienia (możliwość eksportu danych, czytelność danych, zakres).

2.1.3.12. Audyt możliwości aktualizacji danych

W ramach zadania muszą zostać zbadane możliwości organizacyjne i techniczne w zakresie aktualizacji przetwarzanych danych. Muszą zostać wykazane możliwości aktualizacji danych poprzez narzędzia, którymi dysponuje organizacja.

2.1.3.13. Audyt metod udostępnienia danych osobom uprawnionym

W ramach zadania muszą zostać zanalizowane możliwości organizacyjne i techniczne w zakresie sposobów, umożliwiających wskazanie i przekazanie danych osobom uprawnionym. Badany będzie czas wymagany na przekazanie oraz możliwości, którymi dysponuje organizacja w zakresie przekazywania danych powiązanych z wybraną osobą.

2.1.3.14. Audyt właściwego informowania o sprzeciwie w zakresie przetwarzania danych

W ramach zadania muszą zostać przeanalizowane informacje, które organizacja przekazuje osobom, których dane przetwarza. Celem zadania jest wypracowanie procedur, dzięki którym każda osoba będzie mogła być poinformowana w jednoznaczny i czytelny sposób o możliwościach w zakresie usunięcia danych ze zbiorów organizacji.

2.1.3.15. Audyt możliwości trwałego usunięcia danych ze wszystkich obszarów

Przedmiotem Audytu będzie możliwość trwałego usunięcia danych w przypadku zakończenia ich przetwarzania. Elementem Audytu będzie również wskazanie miejsc przechowywania i przetwarzania danych wraz z systemami informatycznymi służącymi do ich przetwarzania. Po wskazaniu systemów przedmiotem będzie szczegółowy Audyt powiązań danych oraz metod ich usunięcia.

2.1.3.16. Audyt możliwości systemów przetwarzających dane osobowe

Audyt musi wykazać faktyczne możliwości usunięcia danych przy pomocy narzędzi, którymi dysponuje organizacja, bez wyrządzania szkody w obszarze integralności danych.

2.1.3.17. Bezpieczeństwo na etapie projektowania (by design)

Audyt musi wskazać sposoby zachowania najwyższego poziomu bezpieczeństwa już na etapie projektowania określonych zbiorów danych oraz narzędzi do ich przetwarzania.

2.1.3.18. Ocena wiarygodności dostawcy oprogramowania

Audyt musi określić wiarygodność dostawcy/producenta/wdrożeniowca oprogramowania w celu wskazania ryzyka związanego z wyborem określonej ścieżki działania.

Dla obszaru zgodności z GDPR musi zostać opracowana następująca dokumentacja:

1. Lista zaleceń umożliwiających realizację założeń osiągnięcia zgodności z GDPR,
2. Rejestr ryzyka,
3. Audyt techniczny posiadanych i wymaganych narzędzi umożliwiający osiągnięcie zgodności wraz ze wskazaniem artykułów rozporządzenia.

2.1.4. Audyt ochrony danych

2.1.4.1. Audyt ochrony danych w ruchu

Audyt musi wykazać możliwości monitorowania ruchu sieciowego oraz przepływu danych wewnątrz organizacji. Wynikiem zadania będzie określenie poziomu bezpieczeństwa w zakresie możliwości pozyskania wiedzy na temat kierunku przepływu danych w określonej jednostce czasu.

2.1.4.2. Audyt ochrony danych w użyciu

Celem Audytu będzie wskazanie miejsc (stacje robocze, serwery, aplikacje komunikacyjne, protokoły przesyłania danych), w których dane są przetwarzane przez użytkowników (sposób ręczny) oraz maszyny (sposób ręczny, pół-automatyczny, w pełni zautomatyzowany).

2.1.4.3. Audyt ochrony danych identyfikowalnych

Audyt będzie mieć na celu wykazanie możliwości identyfikacji danych aplikacji również dziedzinowych, które mogą być analizowane w trybie online (okna aplikacji, przeglądarki WWW) oraz łańcuchów danych nieuporządkowanych występujące w dokumentach PDF, MS Word i innych. Identyfikowalność danych będzie niezbędna dla posiadania wiedzy o czasie, miejscu oraz sposobie przetwarzania danych.

2.1.4.4. Audyt ochrony danych w spoczynku

Audyt będzie mieć na celu wskazanie miejsc, w których dane przechowywane są w postaci kopii zapasowych lub zarchiwizowanej (niedostępnej do przetwarzania). Identyfikowane będą również możliwości usunięcia określonych danych z wybranych miejsc.

Dla obszaru Audytu ochrony danych zostanie opracowana następująca dokumentacja:

1. Rejestr ryzyka,
2. Audyt techniczny posiadanych i wymaganych narzędzi umożliwiający osiągnięcie zgodności wraz ze wskazaniem artykułów rozporządzenia.

2.2. Bezpieczeństwo IT

2.2.1. Audyt „Przed (AS IS)”

2.1.4.5. Zasady bezpieczeństwa

W ramach Audytu musi zostać określony poziom bezpieczeństwa w oparciu o spis z natury środków, którymi dysponuje organizacja oraz zaznajomienie się z obowiązującą dokumentacją dotyczącą bezpieczeństwa. Audyt będzie mieć na celu wykonanie mapowania przyjętych zasad na stan rzeczywisty.

2.1.4.6. Obszary bezpieczeństwa

Audyt będzie mieć na celu zaznajomienie się z przyjętą przez organizację identyfikacją wybranych obszarów bezpieczeństwa wraz z mapowaniem tych obszarów na faktyczne potrzeby organizacji.

2.1.4.7. Poziom świadomości organizacji

Audyt będzie mieć na celu określenie poziomu świadomości organizacji w obszarze bezpieczeństwa. Poziom określany jest na podstawie wywiadów z pracownikami oraz wskazanymi osobami kluczowymi.

2.1.4.8. Posiadana dokumentacja

W ramach zadania musi zostać przenalizowana dokumentacja obszaru bezpieczeństwa posiadana przez organizację, jej aktualność oraz stopnień wdrożenia.

2.2.2. Obszar bezpieczeństwa sieciowego

Audyt musi wykazać stopień poziomu bezpieczeństwa na styku z Internetem.

2.2.2.1. Sieć LAN

Audyt ma na celu wykazanie poziomu bezpieczeństwa wewnętrznej sieci komputerowej organizacji. Audyt umożliwia zbadanie wpływu na zaburzenie bezpieczeństwa przez pracowników oraz przez osoby zewnętrzne. Umożliwia również zbadanie poziomu informacji, które można pozyskać poprzez sieć podłączając się do niej. Elementem Audytu musi być przegląd konfiguracji urządzeń sieciowych oraz ocena możliwości konfiguracyjnych oprogramowania, w które wyposażone są urządzenia. Audyt ma na celu weryfikację posiadanej dokumentacji z obszaru sieci komputerowej organizacji do stanu rzeczywistego.

2.2.2.2. Sieć WLAN (bezprzewodowa)

Audyt będzie mieć na celu wskazanie obszarów, w których dostępna jest sieć bezprzewodowa oraz możliwość uzyskania nieautoryzowanego dostępu do tej sieci.

2.2.2.3. BYOD

BYOD (korzystanie z prywatnych zasobów (aplikacji i urządzeń) do celów realizacji zadań organizacji. Audyt będzie mieć na celu wykazanie możliwość pozyskania danych poprzez użycie prywatnych urządzeń wewnątrz organizacji, przy wykorzystaniu zasobów organizacji.

Dla obszaru sieci zostanie opracowana następująca dokumentacja:

1. Lista sprzętu dopuszczonego do użytkowania.
2. Lista producentów/dostawców sprzętu oraz estymacja wiarygodności.
3. Lista zaleceń w zakresie uszczelnienia organizacji w obszarze sprzętu.
4. Lista zgodności posiadanego sprzętu w stosunku do zaleceń GDPR.

2.2.3. Obszar oprogramowania

2.2.3.1. Aplikacje użytkowane na serwerach

Audyt będzie mieć na celu identyfikację aplikacji uruchomionych na serwerach, które mają wpływ na sposób funkcjonowania organizacji oraz zachowanie najwyższego, możliwego poziomu bezpieczeństwa.

2.2.3.2. Aplikacje usługowe (usługi sieciowe)

Audyt uruchomionych usług sieciowych będzie mieć na celu identyfikację ich wymagalności do rzeczywistych potrzeb organizacji.

2.2.3.3. Bazy danych

W ramach zadania należy przeprowadzić identyfikację baz danych oraz przechowywanych w tych bazach zasobów.

2.2.3.4. Aplikacje dedykowane i dziedzinowe

Audyt będzie mieć na celu identyfikację wszystkich systemów dziedzinowych (kadry-płace, zarządzanie organizacją, obieg dokumentów, inne) wraz z zakresem danych osobowych i sposobem, w jaki aplikacja zarządza danymi, które wykorzystywane są w organizacji.

2.2.3.5. Metody zarządzania użytkownikami

Audyt będzie mieć na celu identyfikację sposobów zarządzania użytkownikami pod kątem spełnienia założeń dla bezpieczeństwa informacji. Analizie będzie podlegać centralne logowanie, zarządzanie kontami, możliwość podjęcia szybkich akcji zaradczych w przypadku naruszenia bezpieczeństwa.

2.2.3.6. Metody zarządzania uprawnieniami

Analizie będzie podlegać system uprawnień w ramach stosowanych systemów operacyjnych oraz aplikacji. Analizie musi podlegać obszar aplikacji (również dziedzinowych) oraz różne systemy operacyjne.

2.2.3.7. Metody nadzoru nad podmiotami zewnętrznymi

Audyt będzie mieć na celu wykazanie sposobu nadzorowania zewnętrznych podmiotów, które w sposób pośredni i bezpośredni mogą uzyskać dostęp do danych przetwarzanych przez organizację.

2.2.3.8. Wirtualizacja zasobów

Audyt będzie mieć na celu zbadanie faktycznego stanu wirtualizacji zasobów pod kątem zachowania usług opartych o wirtualizację w ciągłości działania, w przypadku wystąpienia awarii fizycznych serwerów. W ramach Audytu badana jest ogólna wydajność środowiska wirtualnego, możliwości optymalizacji oraz zgodność posiadanych licencji uruchomionych na środowisku w obszarze sprzętu i oprogramowania.

2.2.3.9. Kopia zapasowa (backup)

Audyt będzie mieć na celu wskazanie metod i narzędzi w kontekście możliwości odtworzenia tych danych oraz wiarygodności danych, które podlegają zabezpieczeniu.
W kontekście RODO muszą zostać przeanalizowane najważniejsze elementy umożliwiające identyfikację i wyszukanie danych podlegających backupowi w ramach narzędzi posiadanych przez organizację.

2.2.3.10. Systemy krytyczne dla funkcjonowania organizacji

Audyt będzie mieć na celu zbadanie i wskazanie krytycznych systemów dla działania organizacji, bez których będzie ona co najmniej niewydajna, a w skrajnych przypadkach przestanie funkcjonować.

2.2.3.11. Aplikacje dziedzinowe

Audyt będzie mieć na celu zidentyfikowanie wszystkich aplikacji dziedzinowych używanych na komputerach osobistych pracowników oraz współpracowników organizacji. Audyt musi uwzględniać sposób konstrukcji aplikacji pod kątem spełnienia założeń zachowania prywatności (poufności) danych na etapie projektowania („privacy by design”) oraz bezpieczeństwa na etapie projektowania „security by design”. Audyt posłuży do budowy listy aplikacji dopuszczonych do użytkowania.

2.2.3.12. Lista aplikacji użytkowanych

Audyt musi mieć na celu opracowanie listy aplikacji dopuszczonych do użytkowania z uwzględnieniem sposobu licencjonowania, źródła pochodzenia, miejsca produkcji, sposobu dystrybucji.

Po Audycie zostanie opracowana lista następujących dokumentów:
1. Lista oprogramowania dopuszczonego do użytkowania na serwerach oraz stacjach roboczych.
2. Lista dostawców oprogramowania oraz estymacja wiarygodności.
3. Lista aplikacji dopuszczonych do użytkowania.
4. Lista zaleceń w zakresie uszczelnienia organizacji w obszarze oprogramowania.
5. Lista zgodności posiadanego oprogramowania w stosunku do zaleceń GDPR.

2.2.4. Obszar bezpieczeństwa sprzętowego

2.2.4.1. Serwerownia

2.2.4.1.1. CCTV

Audyt będzie mieć na celu wykazanie zgodności prowadzonego monitoringu wizyjnego z przyjętymi zasadami bezpieczeństwa. Wynikiem jest określenie obszaru monitoringu wraz ze wskazaniem martwych stref i ich wpływem na bezpieczeństwo danych.

2.2.4.1.2. SKD

Audyt będzie mieć na celu wykazanie zgodności stref kontroli dostępu do pomieszczeń z przyjętymi zasadami bezpieczeństwa. Wynikiem musi być określenie obszaru kontroli dostępu do pomieszczeń wraz ze wskazaniem stref stwarzając zagrożenie.

2.2.4.1.3. Klimatyzacja

Audyt musi mieć na celu wykazanie wydajności klimatyzacji w porównaniu do urządzeń zainstalowanych w serwerowni. Celem Audytu będzie ocena zagrożeń wynikających z braku prawidłowej cyrkulacji powietrza. Wynikiem będzie ocena ryzyka oraz spis zaleceń do realizacji.

2.2.4.1.4. System gaszenia

Audyt będzie dotyczyć zastosowanych instalacji gaszenia w serwerowni w funkcji wielkości pomieszczenia oraz ilości zastosowanego sprzętu. Wynikiem będzie opracowanie wskazujące na możliwość stosowania istniejących rozwiązań oraz innych dostępnych na rynku.

2.2.4.1.5. Zasilanie zapasowe

Audyt będzie mieć na celu wykazanie wydajności, jakości oraz wiarygodności zastosowanych mechanizmów podtrzymania zasilania w przypadku jego braku. Wynikiem Audytu będzie ocena konieczności reorganizacji lub optymalizacji metod zapewniających stały dostęp energii elektrycznej przez określony czas.

2.2.4.1.6. Monitoring zmiennych środowiskowych

Audyt będzie mieć na celu weryfikację narzędzi w zakresie monitorowania temperatury, wilgotności, dymu, pożaru, zalania. Wynikiem będzie ocena stanu wraz z listą zaleceń.

2.2.4.1.7. Fizyczny dostęp do osprzętu serwerowni

Audyt będzie mieć na celu wykazanie możliwości fizycznego dostępu do serwerowni uwzględniając przy tym bezpieczeństwo instalacji, danych oraz możliwość udowodnienia wejścia/wyjścia z serwerowni.

2.2.4.2. Serwery oraz dedykowany osprzęt sieciowy

2.2.4.2.1. Zarządzanie ciągłością działania

Audyt będzie mieć na celu wykazanie zastosowanych rozwiązań klastrów wysokiej dostępności. Audyt będzie dotyczyć obszaru klastrów zbudowanych w oparciu o fizyczne serwery. Jej wynikiem będzie weryfikacja działania klastra pod kątem zachowania ciągłości działania dla usług uruchomionych w ramach klastra.

2.2.4.3. Gwarancje oraz umowy wsparcia i serwisu

Celem Audytu będzie przegląd dostępnych umów wsparcia serwisu w funkcji okresu ich obowiązywania oraz dostępności sprzętu lub oprogramowania w oczekiwanym przez organizację czasie. Ważnym elementem będzie badanie dostępności elementu podlegającego umowie w zakresie dalszego rozwoju przez producenta/dostawcę.

W wyniku audytu obszaru sprzętu zostanie opracowana następująca dokumentacja:

1. Rejestr ryzyka ukierunkowany na identyfikację wszystkich zagrożeń powiązanych ze sprzętem w opisanym zakresie.
2. Audyt posiadanych umów wsparcia i serwisu w zakresie ich wiarygodności i trwałości.
3. Lista elementów wymaganych do zachowania ciągłości działania.

2.3. Bezpieczeństwo fizyczne (wybrane elementy, safety)

2.3.1. Monitoring wizyjny (CCTV)

W ramach Audytu zostanie przeprowadzony szereg czynności mających na celu wykazanie rzeczywistego stanu bezpieczeństwa wynikającego z możliwości obserwacji i odtworzenia materiału zarejestrowanego przez posiadane urządzenia. Analizie zostanie poddany obszar stref martwych i ich wpływ na bezpieczeństwo. Przeanalizowane zostanie również środowisko rejestracji: możliwości oprogramowania, inteligencja posiadanych systemów, czytelność rejestrowanego materiału oraz możliwość rozbudowy.

2.3.2. Fizyczny dostęp do wyposażenia

Przeanalizowane zostaną możliwości uzyskania fizycznego dostępu do wyposażenia organizacji pod kątem wpływu na bezpieczeństwo. Analizie podlega wyposażenie stałe oraz charakterystyka budynków.

2.4. Audyt potrzeb użytkowników

W ramach Audytu zostanie przeprowadzona Audyt potrzeb użytkowników korzystających z systemów dziedzinowych w szczególności z systemów kadrowo-płacowych w obszarze:

a) zakresu funkcjonalnego,
b) powiązania wewnętrzne między modułami,
c) powiązania z systemami zewnętrznymi,
d) integracji z systemem EZD,
e) realizacja e-usług A2A, A2B i A2C.

2.5. Dokumentacja audytu (podsumowanie)

2.5.1. Przekazane dokumenty

2.5.1.1. Wycena ryzyka

Dla każdego z opisanych poziomów zostanie opracowana Audyt ryzyka oraz dla każdego zidentyfikowanego ryzyka zostanie wykonana estymacja wyceny pod kątem:

a) finansowym,
b) wizerunkowym,
c) formalno-prawnym,
d) odpowiedzialności personalnej,
e) odpowiedzialności organizacji.

2.5.1.2. Rejestr ryzyk

Dla celów przekazania całości informacji zostanie przekazany rejestr ryzyka, umożliwiający zapoznanie się ze wszystkimi zidentyfikowanymi ryzykami.

2.5.1.3. Lista zaleceń

W kontekście zidentyfikowanych ryzyk zostanie przekazana lista zaleceń dla każdego ryzyka, mająca na celu wskazanie możliwości zminimalizowania wpływu ryzyka na organizację.

2.5.1.4. Scenariusze

W ramach zadania muszą zostać opracowane scenariusze profilaktyczno-zaradcze dla każdego zidentyfikowanego ryzyka, które zostanie określone jako krytyczne. Celem scenariuszy jest opisanie sytuacji, w której znajdzie się organizacja o ile ryzyko wystąpi.

2.5.2. Warianty inwestycyjne

Warianty inwestycyjne mają na celu wizualizację opcji przez wzgląd na cenę oraz ryzyko powiązane wymagane do akceptacji w każdym z wariantów. Podczas opracowania wariantów inwestycyjnych należy przyjąć, że czym wyższe nakłady inwestycyjne tym niższe prawdopodobieństwo wystąpienia ryzyka. Ostateczny wybór wariantu będzie należał do organizacji.
W ramach każdego wariantu inwestycyjnego musi zostać opracowany kosztorys zawierający:
a) wycenę usług,
b) wycenę zakupów,
c) wycenę utrzymania w okresie 36 miesięcy każdego z zaproponowanych rozwiązań.
Dla każdego z wariantów musi zostać opracowane uzasadnienie zawierające opis wskazań.

2.5.2.1. Lista elementów – wariant minimalny

W ramach zadania należy opracować wariant minimalny, który umożliwi spełnienie absolutnego minimum przez eliminację ryzyka określonego na poziomie krytycznym. Należy założyć, iż wymagana będzie akceptacja dużej ilości zdarzeń ryzyka, które w sposób istotny wpływają na funkcjonowanie organizacji.

2.5.2.2. Lista elementów – wariant średni

W ramach zadania należy opracować wariant średni, który umożliwi spełnienie absolutnego minimum oraz wybranych (uzgodnionych z organizacją) elementów ryzyka, które wpływają w sposób istotny na działanie organizacji. Należy założyć, iż wymagana będzie akceptacja dużej ilości zdarzeń ryzyka, które w sposób istotny wpływają na funkcjonowanie organizacji, ale przy wystąpieniu tych ryzyk organizacja ucierpi mniej niż w wariancie minimalnym.

2.5.2.3. Lista elementów – wariant pożądany

W ramach zadania należy opracować wariant pożądany, który umożliwi minimalizację wpływu ryzyka na organizację oraz akceptację wariantów wystąpienia ryzyka, które nie ma istotnego wpływu na organizację. Należy założyć, iż będzie wymagana akceptacja większego budżetu oraz czasu na wdrożenie uzgodnionych rozwiązań. Jest to wariant, w którym organizacja oraz interesariusze są chronieni w odpowiedni sposób.

3. WYMAGANIA METODYCZNE

1. W celu uzyskania maksymalnej skuteczności i rzetelności w pozyskiwaniu danych Wykonawca powinien zapewnić odpowiednią liczbę spotkań z pracownikami, na których zapozna przedstawicieli wybranych oddziałów UMWL z założeniami i zakresem audytu i badań, które zostaną przeprowadzone.
2. Elementy wymienione w pkt. 1 - PRODUKTY ZAMÓWIENIA powinny być realizowane za pomocą narzędzi elektronicznych.
3. Proces prowadzenia inwentaryzacji nie może powodować pogorszenia jakości wyników pracy UMWL.

4. W przypadku konieczności zaangażowania do prac inwentaryzacyjnych pracowników UMWL, Wykonawca obowiązkowo przeprowadzi dla nich spotkania szkoleniowo-informacyjne, które będą wkalkulowane w cenę za zrealizowanie przedmiotu zamówienia.
5. Wykonawca zapewni wsparcie Help Desk w postaci dedykowanego numery telefonów do min. 2 konsultantów dla przedstawicieli Zamawiającego oraz elektronicznego systemu zgłoszeń w zakresie przedmiotu zamówienia.
6. Audyt będzie koordynowany przez wyznaczonych pracowników UMWL tworzący Zespół Koordynacyjny.
7. Tworzona podczas inwentaryzacji dokumentacja musi być weryfikowana na bieżąco przez Wykonawcę.
8. Po zakończeniu prac inwentaryzacyjnych i analitycznych utworzona dokumentacja wraz ze źródłowymi bazami danych zostanie przekazana Zamawiającemu.
9. Przekazanie wszelkich dokumentów dotyczących realizacji przedmiotu zamówienia musi odbyć się za potwierdzeniem w formie protokołu przekazania.
10. Wykonawca musi przeprowadzić konferencję podsumowującą wyniki audytu informatycznego.

4. KOMÓRKI ORGANIZACYJNE OBJĘTE AUDYTEM

Wykaz struktury organizacyjnej UMWL jest dostępny pod adresem: https://umwl.bip.lubelskie.pl/index.php?id=26.

Audyt musi obejmować wszystkie komórki organizacyjne UMWL wykonujące zadania objęte przedmiotem niniejszego postępowania.

V. WYMAGANIA DOTYCZĄCE WYKONAWCY

1. Zamawiający wymaga aby Wykonawca posiada wiedzę i doświadczenie, rozumiane jako wykonanie/wykonywanie w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie dwóch audytów bezpieczeństwa, dotyczących audytu bezpieczeństwa teleinformatycznego uwzgledniającego w przedmiocie: serwery, urządzenia sieciowe i stacje robocze użytkowników w zakresie wykonania inwentaryzacji, wskazania elementów wymagających naprawy, przeglądu konfiguracji urządzeń, stworzenia rejestru ryzyka, analizy ciągłości biznesowej (business continuity).
2. Na potwierdzenie ww. warunków Zamawiający oczekuje okazania referencji pochodzących od klienta albo protokołów odbioru potwierdzonych przez klienta wraz z prawidłowo wystawioną fakturą VAT. Wybrany Wykonawca musi dostarczyć ww. dokumenty niezwłocznie po ogłoszeniu informacji o wyborze oferty.

VI. WYMAGANIA DOTYCZĄCE OSÓB BIORĄCYCH UDZIAŁ W REALIZACJI ZAMÓWIENIA

1. Zamawiający wymaga, aby osoby, które będą uczestniczyć w wykonywaniu zamówienia posiadały odpowiednie kwalifikacje zawodowe, doświadczenie związane z przedmiotem umowy oraz aby posiadały jasno określony zakres wykonywanych czynności, min.:

1.1. **Kierownik projektu** z doświadczeniem w zarządzaniu projektami informatycznymi - nie mniej niż jedna osoba, posiadająca:
   1.1.1. minimum 3 letnie doświadczenie zawodowe w zakresie kierowania projektami informatycznymi lub teleinformatycznymi w tym przynajmniej dwoma projektami o wartości minimum 50 000 PLN każdy,
   1.1.2. wiedzę odnośnie metodologii procesu projektowego w odniesieniu do kwalifikacji PRINCE lub cyklu projektowego zatwierdzonego przez Komisję Europejską, potwierdzoną ważnym certyfikatem PRINCE2 Practitioner lub równoważnym certyfikatem potwierdzającym umiejętność prowadzenia projektu i co najmniej 2 letnie doświadczenie w prowadzeniu projektów informatycznych,
   1.1.3. wykształcenie wyższe albo co najmniej 3 letnie doświadczenie zawodowe w prowadzeniu projektów audytów teleinformatycznych,
1.2. **Audytor z doświadczeniem w prowadzeniu analiz zasobów sieciowych** - nie mniej niż jedna osoba, posiadająca:
   1.2.1. minimum 3 letnie doświadczenie zawodowe w zakresie prowadzeniu audytów zasobów sieciowych w zakresie technicznym,
   1.2.2. wykształcenie wyższe albo co najmniej 3 letnie doświadczenie zawodowe w prowadzeniu audytów teleinformatycznych,,
   1.2.3. certyfikat Cisco Certified Network Professional Security lub równoważne* albo Cisco Certified Internetwork Expert Routing and Switching lub równoważne*.
1.3. **Audytor z doświadczeniem w prowadzeniu analiz zasobów serwerowych oraz wirtualnych** - nie mniej niż jedna osoba, posiadająca:
   1.3.1. minimum 3 letnie doświadczenie zawodowe w zakresie prowadzeniu audytów zasobów sieciowych w zakresie technicznym,
   1.3.2. certyfikat VMware Certified Professional lub równoważne*,
1.4. **Audytor z doświadczeniem w prowadzeniu analiz systemów operacyjnych** - nie mniej niż jedna osoba, posiadająca:
   1.4.1. minimum 3 letnie doświadczenie zawodowe w zakresie prowadzeniu audytów systemów operacyjnych w zakresie technicznym,
   1.4.2. certyfikat Microsoft Certified Solution Expert Server Infrastructure lub równoważne* oraz Microsoft Certified Technology Specialist Active Directory Configuration lub równoważne*,
1.5. **Audytor z doświadczeniem w prowadzeniu audytów informatycznych** - nie mniej niż jedna osoba, posiadająca:
   1.5.1. minimum 3 letnie doświadczenie zawodowe w zakresie prowadzeniu audytów w zakresie formalno-prawnym,
   1.5.2. wykształcenie wyższe prawnicze lub co najmniej 3 letnie doświadczenie zawodowe w prowadzeniu audytów teleinformatycznych uwzgledniających aspekty formalne i prawne.

Na potwierdzenie ww. warunków Zamawiający oczekuje okazania listy osób w postaci: Imię, Nazwisko, Doświadczenie, Posiadane certyfikaty. Wybrany Wykonawca musi dostarczyć ww. dokumenty niezwłocznie po ogłoszeniu informacji o wyborze oferty. Zgłoszone osoby muszą w kolejnych etapach realizować przedmiot zamówienia, a ich zmiana jest możliwa tylko po akceptacji nowych członków

*za równoważne Zamawiający uzna certyfikaty (lub dokumenty równoważne dla certyfikatów), które potwierdzają co najmniej takie umiejętności jakie potwierdzają certyfikaty wymienione w wymaganiach dla danej osoby, wystawione przez podmiot, który na dzień publikacji ogłoszenia prowadzi działalność polegającą na certyfikowaniu tj. weryfikacji i potwierdzaniu umiejętności

zespołu o kwalifikacjach, doświadczeniu i wykształceniu zgodnym z wymaganiami Zamawiającego i wymaga formy pisemnej.

VII. DOKUMENTY WYMAGANE NA ETAPIE PODPISANIA UMOWY

Wykonawca przygotuje i przedstawi:

1. Szczegółowy rzeczowy harmonogram realizacji kompletnego przedmiotu zamówienia.
2. Opis metod komunikacji.
3. Opis wszystkich faz tworzenia poszczególnych produktów zamówienia (zawartych w pkt. 1 - PRODUKTY ZAMÓWIENIA).

VIII. TERMIN I ETAPY REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło w nieprzekraczalnym terminie **60 dni roboczych od daty podpisania Umowy.**
2. Wykonawca obowiązkowo zgłosi Zamawiającemu gotowość do podpisania protokołu odbioru ilościowego i jakościowego przedmiotu Umowy nie później niż 5 dni przed zadeklarowanym terminem realizacji danego etapu.

IX. DANE DOTYCZĄCE ZŁOŻENIA OFERTY

1. Ofertę należy sporządzić w języku polskim na formularzu oferty (Załącznik nr 1 do Zapytania Ofertowego).
2. Do oferty Wykonawca musi dołączyć wypełniony i podpisany Formularz „Zobowiązanie Wykonawcy do spełnienia dodatkowych kryteriów" stanowiący załącznik nr 1 do Formularza ofertowego.
3. Oferta może być złożona w zamkniętym, nieprzejrzystym opakowaniu, na którym należy napisać:
    a) nazwę i adres Zamawiającego:
    b) nazwę zamówienia,
    c) nazwę i dokładny adres Wykonawcy,
    d) napis o treści: „Nie otwierać przed upływem terminu składania ofert"
4. Ofertę należy złożyć Zamawiającemu w jeden z następujących sposobów:
    a) osobiście w siedzibie Zamawiającego,
    b) za pośrednictwem poczty/kuriera na adres Zamawiającego,
    c) w formie elektronicznej jako załączniki do emai'la w postaci skanu podpisanych dokumentów na adres email: informatyka@lubelskie.pl.
5. Termin składania ofert: **do dnia 1 grudnia 2017 r. do godziny 12.00**
6. Oferta musi być podpisana przez osobę/y upoważnioną/e do reprezentowania Wykonawcy.
7. Do oferty należy dołączyć opis ról i obowiązków osób związanych z realizacją przedmiotu zamówienia.
8. Do oferty należy dołączyć harmonogram poszczególnych faz realizacji projektu w formie wykresu Gantta zawierającego spis zadań opisanych datami względnymi.

9. Zaleca się dołączyć do oferty aktualny odpis z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej. W sytuacji gdy Wykonawca nie przedłoży ww. dokumentu, Zamawiający przed podpisaniem umowy może zwrócić się o jego przedłożenie.
10. Termin ważności oferty: 20 dni.
11. Osoby wyznaczone do kontaktów: Dariusz Kopyść, tel.: (81) 44 16 501;
12. e-mail: informatyka@lubelskie.pl

X. WYBÓR OFERTY

1. Złożone oferty muszą być zgodne z opisem zamówienia i warunkami zawartymi w punkcie IX. Oferty niezgodne z w/w punktem podlegają odrzuceniu.
2. Oferty złożone po terminie określonym w punkcie IX. ust. 5 podlegają odrzuceniu.
3. Oferty przekraczające wartością równowartość kwoty, określonej w Ustawie z dnia 29 stycznia 2004 r. z późn. zm. Prawo zamówień publicznych art. 4 pkt. 8., wyliczonej wg aktualnego kursu podawanego w Rozporządzeniu wymienionym w art. 35 pkt. 3 Ust. z dnia 29 stycznia 2004 r. z późn. zm. Prawo Zamówień Publicznych, będą odrzucone.
4. Przy wyborze najkorzystniejszej oferty, Zamawiający będzie się kierował następującymi kryteriami (podanymi poniżej w kolejności zgodnej z ich znaczeniem). Wszystkie oferty będą oceniane na podstawie następujących kryteriów:

60 pkt zostanie przyznanych ofercie zawierającej najniższą cenę brutto, pozostałe oferty zostaną ocenione wg następującego wzoru:

A/B*60=C

gdzie:

A - wartość najniższej oferty brutto,

B - wartość brutto oferty ocenianej,

C – wynik ofert cenowych,

40 pkt zostanie przyznanych ofercie, która spełni kryteria dodatkowo punktowane:

D - 30 pkt – otrzyma oferta, która spełni kryterium nr I zgodnie z treścią załącznika nr 1 do Formularza Ofertowego

E - 7 pkt – otrzyma oferta, która spełni kryterium nr II zgodnie z treścią załącznika nr 1 do Formularza Ofertowego

F - 3 pkt – otrzyma oferta, która spełni kryterium nr III zgodnie z treścią załącznika nr 1 do Formularza Ofertowego

Wybór oferty nastąpi wg wzoru:

S=C+D+E+F

S – suma uzyskanych punktów

5. Zamawiający udzieli niniejszego zamówienia temu Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą, tj. złożona została z największą liczbą punktów S
6. Jeżeli Zamawiający nie będzie mógł wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert będzie posiadało taką samą (równą najwyższej) liczbą punktów S, Zamawiający spośród tych ofert wybierze ofertę z najniższą ceną brutto oferty.
7. Wszystkie obliczenia będą prowadzone z dokładnością do dwóch miejsc po przecinku.
8. W celu oceny oferty, której wybór prowadziłby do powstania obowiązku podatkowego Zamawiającego zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, zamawiający dolicza do ceny przedstawionej w ofercie podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.
9. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zawiadamia Wykonawcę, który złożył najkorzystniejszą ofertę.
10. Cena ofertowa winna obejmować wszystkie koszty związane z realizacją zamówienia. Za cenę oferty uważać się będzie cenę brutto (łącznie z należnym podatkiem VAT).
11. Cena ofertowa musi być ostateczną ceną obejmującą wycenę realizacji wszystkich elementów składających się na przedmiot zamówienia, tj. produktów zawartych w pkt. 1 - PRODUKTY ZAMÓWIENIA.

XI. INFORMACJE DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Dokumentacja / przedmiot zamówienia:
   a) Formularz „Zobowiązanie Wykonawcy do spełnienia dodatkowych kryteriów", stanowiący załącznik nr 1 do Formularza ofertowego;
   b) Wzór umowy (Załącznik nr 2 do Zapytania Ofertowego);
   c) Dokumenty potwierdzające doświadczenie oraz kwalifikacje osób biorących udział ze strony Wykonawcy w zakresie realizacji podobnych projektów.
2. Zamawiający wraz z zapytaniem ofertowym przekazuje „Formularz ofertowy" - Załącznik nr 1 do Zapytania ofertowego z załącznikami oraz Wzór Umowy – Załącznik nr 2 do Zapytania ofertowego.
3. W siedzibie Zamawiającego udostępnione zostaną do wglądu niezbędne dokumenty potrzebne do realizacji przedmiotu zamówienia przez Wykonawcę.
4. Do czasu zawarcia umowy Zamawiający zastrzega sobie prawo do zakończenia postępowania na każdym etapie bez wyłonienia Wykonawcy oraz bez podania przyczyny.
5. Wykonawca może złożyć tylko jedną ofertę.