Załącznik nr 1 do OPZ

wymaganie	opis
Oprogramowanie e-Zamówienia-UMŁ- Ogólne	
Ogólne.1.	Powiadamianie użytkowników (np. mailowe) i włączanie poszczególnych użytkowników w procesy.
Ogólne.2.	System musi mieć możliwość ograniczania dostępu do widoków i edycji pól dla poszczególnych użytkowników (nadawanie uprawnień użytkownikom).
Ogólne.3.	Zarządzanie/administrowanie systemem będzie realizowane przez Wykonawcę na podstawie informacji otrzymanych od Zamawiającego. Zamawiający nie będzie samodzielnie konfigurował systemu, chyba że w trakcie analizy przedwdrożeniowej zostaną podjęte inne decyzje.
Ogólne.4.	System musi mieć opcję auto zapisu danych, w określonym czasie definiowanym w Systemie w trakcie pracy użytkownika, co zabezpieczy przed ich utratą w czasie pracy.
Ogólne.5.	System musi uwzględniać wyszukiwanie proste i zaawansowane.
Ogólne.6.	System musi zostać wykonany w architekturze 3-warstwowej, w której klient łączy się z serwerem aplikacji poprzez przeglądarkę internetową, a procesy związane z przetwarzaniem danych są realizowane przez serwer aplikacyjny. Zamawiający nie uzna, że System został wykonany w architekturze 3-warstwowej, jeżeli użytkownik będzie łączyć się z serwerami aplikacji z wykorzystaniem rozwiązań terminalowych jako metody dostępu użytkownika do serwera aplikacji.
Ogólne.7.	System musi posiadać interfejsy WebService do komunikacji z innymi systemami jako podstawowy model integracji z innymi systemami.
Ogólne.8.	Poprzez interfejsy WebService System musi realizować funkcjonalność aktualizacji własnych danych oraz udostępniać dane do innych systemów. Zakres integracji w ramach zamówienia podstawowego jest opisany w treści OPZ.
Ogólne.9.	Interfejsy WebService muszą zapewniać funkcjonalność szyfrowania transmisji danych przy wykorzystaniu certyfikatów X.509.
Ogólne.10.	Zakres danych wymienianych do i z Systemu poprzez WebService-y zostanie uzgodniony w Projekcie Rozwiązania.

Ogólne.11.	Komunikaty o ostrzeżeniach, błędach, informacjach w Oprogramowaniu Aplikacyjnym Standardowym i Oprogramowaniu Dedykowanym prezentowane muszą być w języku polskim.
Ogólne.12.	System musi zapewnić pełną spójność danych we wszystkich Modułach.
Ogólne.13.	Oprogramowanie Aplikacyjne nie może przechowywać loginów i haseł w plikach konfiguracyjnych.
Ogólne.14.	System musi zapewniać jednolity interfejs użytkownika dla wszystkich obszarów funkcjonalnych, a funkcje powtarzające się w różnych Modułach powinny być dostępne dla użytkownika pod taką samą nazwą w menu i pod takim samym klawiszem skrótu, zapewniając w maksymalny sposób jednolitość obsługi.
Ogólne.15.	System musi zapewnić dostęp do wszystkich danych Systemu transakcyjnego w czasie rzeczywistym.
Ogólne.16.	Porządek sortowania musi uwzględniać alfabet polski (A, Ą, B, C, Ć… a nie A, B, C … Z, Ą, Ę, Ć). Porządek sortowania (w kolejności od najmniejszej do największej lub odwrotnie) numerów liczb zapisanych jako tekst musi być identyczna jak w przypadku liczb.
Ogólne.17.	Musi być zachowana jednolitość i jednoznaczność ikon, przycisków itp. w całym Systemie.
Ogólne.18.	Oprogramowanie powinno uniemożliwiać jednoczesną edycję tych samych danych przez więcej niż jednego użytkownika. W przypadku próby edycji danych przez kolejnego użytkownika powinien być wyświetlany odpowiedni komunikat, w tym może być wyświetlana informacja o użytkowniku, który aktualnie dokonuje ich edycji.
Ogólne.19.	Pola wymaganych danych muszą być oznaczone w sposób wyraźny i jednolity dla całego Oprogramowania oraz wyraźnie oddzielone od pól opcjonalnych.
Ogólne.20.	Pola danych nieedytowalnych powinny być oznaczone w sposób wyraźny i jednolity dla całego Oprogramowania. Informacje w nich wyświetlane nie mogą podlegać edycji.
Ogólne.21.	Oferowane Rozwiązanie musi poprawnie funkcjonować na stacjach roboczych użytkowników, którzy pracują w profilu indywidualnym bez uprawnień administratora stacji roboczej. Żaden z elementów oferowanego Systemu nie może wymagać do swojej poprawnej pracy, posiadania uprawnień administratora na stacji roboczej użytkownika.
Ogólne.22.	System musi mieć walidację poszczególnych pól w formularzach (tych, których jest możliwość i zasadność).

Ogólne.23.	System musi zapewnić możliwość parametryzacji tworzonych raportów i analiz poprzez zastosowanie filtrów ograniczających, agregatów oraz innych mechanizmów.
Ogólne.24.	System musi zapewnić możliwość wykorzystania predefiniowanych wzorców raportów/analiz/zestawień.
Ogólne.25.	Słowniki w Systemie muszą być wspólne dla wszystkich modułów oraz komponentów. System musi zapewniać, że modyfikacja słownika następuje tylko w jednym miejscu, a synchronizacja do pozostałych miejsc jest automatyczna, on-line i synchroniczna.
Ogólne.26.	System musi zabezpieczać dane przed przypadkowym usunięciem – generowanie ostrzeżenia o nieodwracalnym usunięciu danych.
Ogólne.27.	System musi uniemożliwiać usunięcie danych np. słownikowych, jeśli zostały one już przypisane do innych danych.
Ogólne.28.	System musi zapewniać automatyczne sprawdzanie poprawności wprowadzanych do Systemu danych typu NIP, REGON, numer konta bankowego razem ze sprawdzaniem sumy kontrolnej. Sprawdzanie poprawności numeru NIP dot. wszystkich krajów Unii Europejskiej. System musi być niewrażliwy na różne sposoby zapisu numerów NIP (np. z separatorami lub bez).
Ogólne.29.	System musi uwzględniać skróty klawiszowe funkcjonujące w środowisku Windows.
Ogólne.30.	System musi zapewnić możliwość eksportu wszystkich widoków ekranowanych i wygenerowanych raportów do następujących formatów: .txt, .xlsx, .docx, .pdf, .xml, .rtf oraz .csv.
Ogólne.31.	System musi zapewniać dostęp użytkownikowi do wbudowanej pomocy kontekstowej dostępnej z każdego ekranu w Systemie. Pomoc kontekstowa musi być w języku polskim i zawierać wszystkie informacje potrzebne przeszkolonemu użytkownikowi w celu poprawnej pracy w Systemie.
Ogólne.32.	Cała komunikacja pomiędzy klientem a serwerem musi być szyfrowana za pomocą certyfikatów SSL.
Ogólne.33.	Modyfikacje wierszy danych w Systemie nie mogą blokować niezależnych odczytów, odczyt wierszy nie może ich blokować do celów modyfikacji. Spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.
Ogólne.34.	System musi zapewniać funkcjonalność wklejania (ze schowka systemowego) treści do pól formularzy oraz kopiowania (do schowka systemowego) z pól na formularzu.

Ogólne.35.	Możliwość wprowadzania czcionek w innych niż łaciński alfabetach - musi istnieć łatwy dostęp do znaków specjalnych w każdym miejscu, gdzie wprowadzany jest jakikolwiek tekst.
Ogólne.36.	Historia wprowadzanych zmian powinna być zapisywana i możliwa do zobaczenia przez uprawnionych użytkowników.
Ogólne.37.	System musi zapewnić poprawną integrację z Systemem e-Zamówienia (kiedy zostanie on udostępniony przez Urząd Zamówień Publicznych) zarówno pod względem technicznym oraz zakresu udostępnianych danych.
Ogólne.38.	System umożliwi bezpieczne połączenie zdalnych użytkowników z użyciem protokołu SSL (TLS 1 i wyższa).
Ogólne.39.	System musi zapewnić audyt systemowy - udokumentowanie historii czynności związanych z zasobami i dostępów do zasobów – audyt systemowy musi odbywać się automatycznie. System musi zapewnić raporty o zmianach dokonywanych na danych osobowych wraz z informacją, kiedy i kto jej dokonał.
Ogólne.40.	System musi zapewnić generowanie raportu, o danych osobowych zgromadzonych dla danego kontrahenta.
Ogólne.41.	Serwery aplikacyjne muszą zapewniać ochronę co najmniej przed atakami: a. wstrzykiwanie poleceń Systemowych; b. ataki semantyczne na adres URL; c. ataki związane z ładowaniem plików; d. ataki typu cross-site scripting; e. ataki typu CSRF; f. podrabianie zatwierdzania formularza; g. sfałszowanie żądania HTTP; h. ujawnienie uwierzytelnień dostępu; i. wstrzykiwanie kodu SQL; j. ujawnienie danych przechowywanych w bazie; k. kradzież COOKIES; l. przechwytywanie sesji; m. wstrzykiwanie sesji; n. zafiksowanie sesji; o. trawersowanie katalogów;

Ogólne.42.	System oferowany przez Wykonawcę musi zapewniać: a. poufność – ochrona przed ujawnieniem nieuprawnionemu odbiorcy; b. integralność – ochrona przed nieuprawnioną modyfikacją lub zniekształceniem; c. dostępność – dostęp do zasobów informacyjnych; d. rozliczalność – określenie i weryfikowanie odpowiedzialności za wykorzystanie Systemu informacyjnego; e. autentyczność – weryfikacja tożsamości podmiotów i prawdziwości zasobów; f. niezawodność – gwarancja oczekiwanego zachowania Systemu i otrzymywanych wyników;
Wymagania funkcjonalne	
1. Sporządzenie planu zamówień publicznych i planu postępowań oraz dokonywanie jego zmian zgodnie z regulacjami wewnętrznymi Zamawiającego w tym możliwość zastosowania – art. 30 ust. 4 ustawy Prawo zamówień publicznych (Dz. U. 2019 r., poz. 2019 ze zm.) zwanej dalej „ustawą Pzp”, Plan powinien mieć wymienione funkcjonalności: – możliwość agregowania zamówień do odpowiednich grup rodzajowych stworzonych przez zamawiającego, – możliwość dodawania bądź likwidowania kolumn w planie (plan powinien posiadać co najmniej możliwość stworzenia kolumn takich jak: nr pozycji, komórka organizacyjna zamawiającego, grupa rodzajowa, opis przedmiotu zamówienia, kod cpv, wartość zamówienia podstawowego, wartość prawa opcji, wartość usług polegających na powtórzeniu podobnych usług lub robót budowlanych zgodnie z art. 214 ust. 1 pkt 7 ustawy Pzp bądź wartość dodatkowych dostaw zgodnie z art. 214 ust. 1 pkt 8 ustawy Pzp, przewidywany termin zawarcia umowy, termin złożenia wniosku do Wydziału, data złożenia wniosku do Wydziału, środki unijne, uwagi), – możliwość ograniczenia wpisywania konkretnych danych (np. tak, nie, data), – możliwość filtrowania każdej kolumny wg. wartości np. konkretną komórkę	

organizacyjną zamawiającego bądź nr pozycji,

- możliwość usuwania lub dodawania pozycji do planu,
- możliwość zwrotu planu komórki organizacyjnej do poprawy,
- możliwość odznaczania pozycji realizowanych, do których wpłynął wniosek o wszczęcie postępowania (np. poprzez wpisanie daty wpływu wniosku w kolumnie „data wpływu wniosku do Wydziału),
- możliwość monitorowania realizacji planu zamówień poprzez filtrowanie daty niezłożonych wniosków, w których minął termin wszczęcia postępowania.
- możliwość wpisania uwag przy każdej pozycji z planu;

2. Możliwość kierowania wniosków o przygotowanie i wszczęcie postępowania do procedowania;
3. Obsługę postępowań w trybach zgodnie z ustawą Pzp oraz ustawą o umowie koncesji na roboty budowlane lub usługi;
4. Obsługę postępowań w trybach zgodnie z regulacjami wewnętrznymi Zamawiającego w związku z art. 2 ust.1 pkt 1 ustawy Pzp (UMŁ i miejskie jednostki organizacyjne);
5. Sprawozdawczość zamówień publicznych zgodnie z ustawą Pzp;
6. System musi umożliwiać pobranie wszystkich dokumentów znajdujących się w systemie na dysk lokalny stacji roboczej użytkownika. Użytkownik będzie mógł pobierać każdy dokument pojedynczo lub wiele dokumentów lub paczkę dla całego postępowania (ZIP).
7. Uwzględnienie regulacji wewnętrznych Zamawiającego w związku z art. 2 ust.1 pkt 1 ustawy Pzp (przyszłościowo również procedurę na wzór licytacji elektronicznej) (UMŁ i miejskie jednostki organizacyjne);
8. Zamieszczanie postępowań zgodnie z ustawą Pzp w trybach: przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem, negocjacje bez ogłoszenia, zamówienie z wolnej ręki, dialog konkurencyjny, partnerstwo innowacyjne, tryb podstawowy z wyborem oferty: bez przeprowadzenia negocjacji, z możliwością negocjowania treści oferty, z negocjacjami treści oferty z wykorzystaniem: umowy ramowej, dynamicznego systemu zakupów, konkursu, aukcji elektronicznej odpowiednio dla danego trybu udzielania zamówień, wstępne konsultacje rynkowe oraz zamówienia na usługi społeczne i inne szczególne usługi w trybach przewidzianych ustawą o umowie

koncesji na roboty budowlane lub usługi;

9. System musi umożliwiać Zamawiającemu tworzenie dokumentacji postepowania na wzorach własnych Zamawiającego i dodawania ich do systemu przez jednego pracownika, bądź wzorach stworzonych w systemie zgodnie z wyborem Zmawiającego (m.in. SWZ, zaproszenia do negocjacji, wezwania, OPZ, oświadczeń, informacji z otwarcia oferta)
10. Zamieszczanie postępowań innych niż postępowania prowadzone na podstawie ustawy Pzp lub regulacji wewnętrznych Zamawiającego np.: postępowań prowadzonych na podstawie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych;
11. Aktami wykonawczymi do ustawy Pzp oraz ustawy o umowie koncesji na roboty budowlane lub usługi;
12. Zamieszczania przez Zamawiającego na platformie dokumentów o maksymalnym rozmiarze (plików) 2 GB m.in. Opis Przedmiotu Zamówienia, Opis przedmiotu umowy koncesji oraz Wzór umowy celem oszacowania wartości zamówienia, zaś przez Wykonawców o maksymalnym rozmiarze 250 MB;
13. Zamieszczania przez Zamawiającego na platformie dokumentów o maksymalnym rozmiarze (plików) 2 GB dla zamówień zgodnie z regulacjami wewnętrznymi Zamawiającego w związku z art. 2 ust.1 pkt 1 ustawy Pzp, zaś przez Wykonawców o maksymalnym rozmiarze 250 MB;
14. Przekazania przez Zamawiającego ogłoszeń wymaganych ustawą Pzp Urzędowi Publikacji Unii Europejskiej *oraz* ustawą o umowie koncesji na roboty budowlane lub usługi;
15. Publikacji ogłoszeń wymaganych ustawą Pzp w Biuletynie Zamówień Publicznych oraz ustawą o umowie koncesji na roboty budowlane lub usługi;
16. Zamieszczania na platformie dokumentów zgodnie z ustawą Pzp przez Zamawiającego o maksymalnym rozmiarze (plików) 2 GB m.in. ogłoszeń, SWZ, załączników do SWZ odpowiedzi na pytania zadane przez Wykonawców, zmiany SWZ, zmiany załączników do SWZ, kopii odwołania (środki ochrony prawnej) , ogłoszeniem o koncesji, wstępne ogłoszenie informacyjne, zaproszenie do ubiegania się o zawarcie umowy koncesji, zaproszenie do składania ofert, opis przedmiotu umowy koncesji;

17. Zamieszczania przez Zamawiającego dokumentów na platformie o maksymalnym rozmiarze (plików) 2 GB m.in. dotyczących postępowań na usługi społeczne i inne szczególne usługi;
18. Zamieszczania na platformie dokumentów przez Zamawiającego na platformie dokumentów o maksymalnym rozmiarze (plików) 2 GB m.in. informacji o zamiarze przeprowadzenia wstępnych konsultacji rynkowych oraz ich przedmiotu;
19. Komunikacji między Zamawiającym a Wykonawcą zgodnie z ustawą Pzp. System musi zapewnić zgodnie z § 61 rejestr przesyłek wychodzących oraz zgodnie z § 40 rejestru przesyłek wpływających Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z dnia 20 stycznia 2011 r.) w zakresie m. in.:
    - składania/wycofania ofert/wniosków
    - wyjaśnienia treści dokumentów dotyczących oszacowania wartości zamówienia (koncesji),
    - wyjaśnienia treści dokumentów dla zamówień zgodnie z regulacjami wewnętrznymi Zamawiającego w związku z art. 2 ust.1 pkt 1 ustawy Pzp;
    - wyjaśnienia treści SWZ, zmiany SWZ, załączników do SWZ i ogłoszeń, przekazywania odwołań (środki ochrony prawnej), opisu przedmiotu umowy koncesji,
    - wyjaśnienia treści dokumentów koncesji, SWZ/Ogłoszenia, zmiana treści SWZ/Ogłoszenia, załączników do SWZ/Ogłoszenia w postępowaniach na usługi społeczne i inne szczególne usługi,
    - wezwania Wykonawcy przez Zamawiającego do złożenia dokumentów, złożenia wyjaśnień, uzupełnienia dokumentów,
    - złożenia przez Wykonawcę dokumentów, wyjaśnień, podpisanych kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym;
19. System musi zapewnić możliwość wygenerowania potwierdzenia tożsamego z urzędowym poświadczeniem przesłania i otrzymania ePUAP.
20. System musi umożliwiać za pomocą oprogramowania dostępnego w systemie bez zewnętrznego oprogramowania:
    – weryfikację podpisu kwalifikowanego, osobistego, zaufanego (ważność

certyfikatu oraz integralność dokumentu) każdego dokumentu zapisanego w systemie (przychodzącego, wychodzącego, wewnętrznego) i wyświetlać dla danego dokumentu informację o poprawnej bądź nie weryfikacji podpisu;

- umożliwiać pobranie certyfikatu, którym został podpisany dokument;
- zapewniać pobranie raportu z informacją o wynikach weryfikacji zawierającego co najmniej informację: podpis elektroniczny zweryfikowany w dniu ….[data]; wynik weryfikacji: ważny/nieważny/nieokreślony - brak możliwości weryfikacji (ze wskazaniem przyczyny).

Zakładane funkcjonalności weryfikatora:

1. **Weryfikacja – formaty podpisów**
   1) weryfikacja podpisu kwalifikowanego,
   2) weryfikacja podpisów zaawansowanych,
   3) weryfikacja podpisu zaufanego,
   4) weryfikacja podpisu osobistego,
   5) weryfikacja kwalifikowanego znacznika czasu.
2. **Walidacja – typy podpisów:**
   1) XAdES otaczający,
   2) XAdES zewnętrzny (w osobnym pliku),
   3) XAdES wewnętrzny (otoczony),
   4) PAdES,
   5) CAdES,
   6) ASiC.
3. **Weryfikacja – formaty plików – rozszerzenia:**

   .txt, .rtf, .pdf, .xps, .odt, .ods, .odp, .doc, .xls, .ppt, .docx, .xlsx, .pptx, .csv, .jpg, .jpeg, .tif, .tiff, .geotiff, .png, .svg, .wav, .mp3, .avi, .mpg, .mpeg, .mp4, .m4a, .mpeg4, .ogg, .ogv, .zip, .tar, .gz, .gzip, .7Z, .html, .xhtml, .css, .xml, .xsd, .gml, .rng, .xsl, .xslt, .TSL, .XMLsig, .XAdES, .PAdES, .CAdES, .ASIC, .XMLenc, .dwg, .dwf, .dxf, .dgn, .jp2, eml, .msg.
4. **Walidacja – zakres:**
   1) weryfikacja ważności certyfikatu,
   2) weryfikacja integralności dokumentu,
   3) weryfikacja pkt 1-2 wg ustawionej daty (weryfikuj na podany czas, weryfikuj wg czasu w znaczniku czasu, weryfikuj wg daty systemowej),

4) weryfikacja wg CRL,
5) weryfikacja wg OCSP o ile jest dodane do podpisu,
6) weryfikacja rodzaju certyfikatu (kwalifikowany, zaufany, osobisty).

5. Prezentacja dokumentu podpisanego:

1) możliwość wyświetlenia dokumentu podpisanego w aplikacji dostępnej na komputerze odpowiedniej do formatu pliku,
2) możliwość pobrania podpisanego dokumentu na dysk lokalny niezależnie od typu podpisu (pkt 2) oraz formatu podpisanego pliku (pkt 3).

6. Raporty – wyniki weryfikacji

1) raport z weryfikacji zawierający informację o wyniku weryfikacji:
   a) ważny, nieważny, nieokreślony (ze wskazaniem przyczyny),
   b) rodzaj podpisu: kwalifikowany, osobisty, zaufany,
   c) data weryfikacji podpisu na dzień …,
   d) data złożenia podpisu (czas deklarowany/czas ze znacznika czasu),
   e) data (okres) ważności certyfikatu,
   f) data unieważnienia certyfikatu,
   g) informacja o utracie integralności dokumentu,
   h) informacja o wystawcy certyfikatu,
   i) informacja o osobie fizycznej składającej podpis.

21. Złożenia przez Wykonawcę oferty/wniosku wraz z dokumentami opatrzonymi kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym;
22. Wycofania oferty/wniosku przez Wykonawcę do terminu składania ofert/wniosków opatrzonej/go kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym;
23. Złożenia w odrębnym pliku dokumentów stanowiących tajemnicę przedsiębiorstwa opatrzonych kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym;
24. Szyfrowania ofert/wniosków w celu zagwarantowania integralności i nienaruszalności do wyznaczonego czasu ich otwarcia (data i godzina otwarcia ofert/wniosków);
25. Otwarcia ofert/wniosków w wyznaczonym czasie (data i godzina otwarcia ofert/wniosków) przez jednego pracownika i/lub większą ilość pracowników

Zamawiającego po prawidłowym zalogowaniu się do systemu i bez wykorzystania dodatkowej weryfikacji (np. w postaci kodów) zgodnie z wyborem Zamawiającego;

26. Weryfikowania czy oferty/wnioski wraz z dokumentami złożonymi przez Wykonawców zostały podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
27. Zamieszczania informacji z otwarcia ofert przy wykorzystaniu danych wprowadzonych przez Wykonawców do oferowanego systemu wspierającego procedurę udzielania zamówień publicznych;
28. Weryfikowania czy złożone/uzupełnione przez Wykonawców dokumenty zostały podpisane kwalifikowanym podpisem elektronicznym, podpisów zaufanych lub podpisów osobistych;
29. Zamieszczania wyników postępowania np. poprzez automatyczne generowanie z danych w systemie (wybór najkorzystniejszej oferty/unieważnienie postępowania);
30. Przekazania Wykonawcom wyniku postępowania (wybór najkorzystniejszej oferty, unieważnienie postępowania, wykluczenie Wykonawców z postępowania, odrzucenie ofert, powodach odrzucenia oferty lub wniosku o dopuszczenie do udziału w postępowaniu o zawarcie umowy koncesji oraz o przysługujących wykonawcy środkach odwoławczych, unieważnieniu postępowania o zawarcie umowy koncesji, ponownym wszczęciu postępowania o zawarcie umowy koncesji);
31. Możliwość zatwierdzania dokumentacji związanej z procedurą o udzielenie zamówienia publicznego i koncesji na roboty budowlane lub usługi przez kierownika Zamawiającego lub osoby upoważnionej);
32. Zamieszczania i przesyłania plików z rozszerzeniami w szczególności: txt, rtf, pdf ,xps, odt, ods, odp, doc, xls, ppt, docx, xlsx, pptx, csv, jpg, jpeg, tif, tiff, geotiff, png, svg, wav, mp3, avi, mpg, mpeg, mp4, m4a, mpeg4, ogg, ogv, zip, tar, gz, gzip, 7z, html, xhtml, css, xml, xsd, gml, rng, xsl, xslt, TSL, XMLsig, XAdES, CAdES, ASIC, XMLenc
33. Bezpieczeństwo w zakresie ochrony ofert/wniosków przed dostępem osób niepożądanych;
34. Weryfikację daty i godziny złożenia oferty/wniosku;

35. Weryfikację daty i godziny złożenia dokumentów na wezwanie Zamawiającego;
36. Weryfikację daty i godziny uzupełnienia dokumentów na wezwanie Zamawiającego;
37. Weryfikację daty i godziny złożenia wyjaśnień na wezwanie Zamawiającego;
38. Personalizację do potrzeb Zamawiającego poprzez umieszczenie logo Zamawiającego, przygotowanie interfejsu graficznego Zamawiającego;
39. Personalizację do potrzeb Zamawiającego poprzez umieszczenie logotypów projektu/programu finansowanego ze środków Unii Europejskiej lub z innych środków niż pochodzące z budżetu Unii Europejskiej, przygotowanie interfejsu graficznego;
40. Możliwość powoływania komisji przetargowej, zmiany jej składu, odwoływania poszczególnych członków.;
41. System musi zapewniać możliwość przeprowadzenia aukcji elektronicznej w formie, jaką przewiduje ustawa Pzp;
42. Zamieszczanie wstępnych ogłoszeń informacyjnych na profilu nabywcy.
43. Elektroniczne przetwarzanie i przechowywanie dokumentów i danych zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. Nr 206, poz. 1518 ze zm.);
44. Monitorowanie, kontrolę i sprawozdawczość: przegląd i wyszukiwanie informacji dotyczących konkretnych postępowań o udzielenie zamówienia publicznego i koncesji na roboty budowlane lub usługi oraz udostępnienie funkcjonalności pozwalających na przetwarzanie danych dotyczących wszystkich zamówień publicznych i koncesji na roboty budowlane lub usługi w celach statystycznych, analitycznych oraz kontrolnych (np. wpisując nazwę postępowania, nr referencyjny postępowania, tryb, wartości o których mowa w art. 359 ustawy Pzp, CPV);
45. Kontrolę realizacji zamówień publicznych i koncesji na roboty budowlane lub usługi;
46. Wykorzystywanie katalogów elektronicznych;
47. Wspomaganie przygotowania i prowadzenia oraz dokumentowania zamówień i koncesji od momentu wszczęcia postępowania, poprzez złożenie ofert, ocenę, dokumentację przeprowadzonego postępowania, kończąc na odnotowaniu

postępu realizacji zamówienia;

48. Posiadanie wbudowanego Wspólnego Słownika Zamówień (CPV) – możliwość powiązania numeru z prowadzonym postępowaniem. Lista kodów CPV winna być rozwijana jak na stronie Urzędu Zamówień Publicznych np. posiadać widok drzewiasty, z możliwością wyszukiwania po wpisaniu minimum 3 znaków alfanumerycznych,
49. Usprawnienie kontroli przedmiotowej i finansowej na różnych poziomach uprawnień;
50. Zapewnienie ochrony dostępu do danych,
51. Tworzenie archiwum dokumentów,
52. Umożliwienie ewidencji prowadzonych postępowań,
53. Umożliwienie automatycznego tworzenia dokumentów na podstawie informacji z bazy danych (pisma użytkownika, protokoły) i wzorów dokumentów włączonych do systemu oraz definiowanie własnych wzorów wynikających z indywidualnych wymagań/potrzeb Zamawiającego,
54. Przeprowadzenie oceny złożonych ofert – funkcje automatycznego przeliczania punktacji, również po przeprowadzeniu aukcji elektronicznej.
55. Sygnalizowanie o upływających terminach - sygnalizacja pewnych możliwych do uchwycenia niezgodności wynikających z wewnętrznych regulacji Zamawiającego (np. terminowe składanie wniosków o wszczęcie postępowania wynikające z daty zawartej w Planie Udzielania Zamówień),
56. Przeszukiwanie zamówień, Wykonawców (baza Wykonawców), ofert i dokumentów według różnych kryteriów,
57. Tworzenie różnego rodzaju statystyk oraz zestawień, raportów z przeprowadzonych postępowań na podstawie wprowadzonych do systemu danych w tym m.in. możliwość filtrowania:
    - unieważnionych postępowań,
    - postępowań, w których został dokonany wybór oferty,
    - postępowań, w których została zawarta umowa,
    - postępowań prowadzonych w danym progu (np. poniżej 130 000 PLN, próg krajowy, próg unijny),
    - postępowań dla danego rodzaju zamówienia (dostawy, usługi, roboty

budowlane).	
Generator.1	Moduł musi posiadać możliwość generowania dokumentów na podstawie wcześniej zdefiniowanych szablonów.
Generator.2	Moduł musi mieć możliwość listowania, wyświetlania, filtrowania i sortowania dokumentów po: numerze, typie, dacie, twórcy i innych polach - szczegóły pól zostaną ustalone przez Zamawiającego.
Generator.3	Jeżeli użytkownik posiada takie uprawnienia to musi mieć możliwość, dodawania, edycji, usuwania dokumentów.
Generator.4	Dokumenty w ruchu wewnętrznym mogą być przypisywane do użytkownika tj. twórca dokumentu może przypisać inną osobę w systemie do której dokument powinien dotrzeć.
Generator.5	Dokumenty muszą posiadać historię swojej modyfikacji.
Moduł Słowników	
Słowniki .1	Za konfigurację i uzupełnianie treści słowników odpowiada Wykonawca, chyba że w trakcie analizy przedwdrożeniowej zostaną podjęte inne decyzje.
Słowniki.2	Moduł musi umożliwiać tworzenie słowników (płaskich i hierarchicznych), dodawania tłumaczeń do słowników, scalania haseł słownikowych, dodawania nowego hasła słownikowego lub edycja już dodanego.
Słowniki.3	Moduł musi mieć możliwość dokonywania zmian w słownikach z poziomu robienia rekordu (bez konieczności zamykania okna rekordu i wchodzenia do słownika).
Słowniki.4	Moduł musi we wszystkich miejscach, gdzie używane są terminy skrócone użytkownik dokonując wyboru terminu skróconego musi widzieć pełny termin np. za pomocą pop-up'u.
Słowniki.5	Do wszelkiego rodzaju danych słownikowych muszą zostać przygotowane narzędzia/funkcje umożliwiające wykonywanie edycji, a także porządkowanie haseł, scalanie, hierarchizacja, edycja dodawania i modyfikowanie terminów, ich wyszukiwanie, usuwanie itd.
Słowniki.6	Słowniki w module muszą być wspólne dla pozostałych modułów oraz komponentów. Moduł musi zapewniać, że modyfikacja słownika następuje tylko w jednym miejscu, a synchronizacja do pozostałych miejsc jest automatyczna, on-line i synchroniczna.
Słowniki.7	Uprawnienia do edycji i podglądu słowników powinny wynikać z przyznanej roli.

Słowniki.8	Moduł musi weryfikować poprawność wprowadzanych danych pod kątem ich kompletności i spójności oraz zgodności ze zdefiniowanymi słownikami, wspomagać użytkownika poprzez oferowanie list wyboru i wyszukiwania kontekstowego przy wprowadzaniu danych.
Moduł RBAC Zarządzanie użytkownikami	
RBAC.1	Zarządzanie/administrowanie rolami i uprawnieniami w systemie będzie realizowane przez Wykonawcę na podstawie informacji otrzymanych od Zamawiającego. Zamawiający nie będzie samodzielnie konfigurował systemu, chyba że w trakcie analizy przedwdrożeniowej zostaną podjęte inne decyzje.
RBAC.2	Moduł nie może posiadać ograniczenia co do liczby użytkowników ani co do liczby użytkowników zalogowanych w tym samym czasie.
RBAC.3	Warunkiem korzystania z systemu jest utworzenie konta w systemie przez administratora systemu.
RBAC.4	Użytkownik nie może pracować w systemie bez zalogowania się do niego.
RBAC.5	Moduł musi posiadać możliwość blokowania użytkowników przez konto użytkownika o określonych prawach (dezaktywowania konta bez możliwości jego usunięcia).
RBAC.6	Administrator ma mieć możliwość wyświetlania nieaktywnych i dezaktywowanych użytkowników, użytkownik taki powinien być oznaczony.
RBAC.7	Administrator musi mieć możliwość edycji konta użytkownika, wprowadzenia nowego hasła, zresetowania hasła użytkownika itp. nie może mieć jednak wglądu do hasła użytkownika.
RBAC.8	Hasła użytkowników w Systemie nie mogą być zapisywane plain tekstem – muszą być szyfrowane np. metodą Scrypt, bcrypt, argon2 lub innym nowoczesnym sposobem szyfrowania. Zamawiający nie dopuszcza szyfrowania haseł algorytmem MD5.
RBAC.9	Uprawnienia i profile użytkowników - funkcjonalność umożliwiająca przydzielanie praw i przydzieleniu ról użytkownikom. Typy kont, role oraz prawa zostaną określone podczas tworzenia systemu z Zamawiającym.
RBAC.10	Moduł musi umożliwiać wydajne wyszukiwanie użytkowników w systemie. Powinna istnieć lista użytkowników dostępna użytkownikom z rolą Administratora.
RBAC.11	Moduł musi wymuszać zmianę hasła po utworzeniu konta przez Administratora.

RBAC.12	Moduł musi umożliwiać przypisanie użytkownika do grup użytkowników np. działu.
RBAC.13	Moduł musi umożliwiać nadawanie uprawnień i przydzielanie ról każdemu użytkownikowi.
RBAC.14	Moduł musi posiadać funkcjonalność hurtowego nadawania uprawnień.
RBAC.15	Moduł musi umożliwiać tworzenie dowolnej liczby ról dla jednego użytkownika.
RBAC.16	Moduł musi umożliwiać edycję profilu użytkownika – ustawienie hasła, opisu, preferowanego widoku listy i szablonu obiektu.
RBAC.17	Dostęp użytkowników do poszczególnych funkcji Systemu musi być regulowany przez Administratora z odpowiednimi uprawnieniami z wykorzystaniem Ról.
RBAC.18	Role powinny być zdefiniowane w zależności od czynności wykonywanych przez użytkowników Systemu.
RBAC.19	System musi umożliwić całkowite lub częściowe ograniczenie dostępu do wybranych danych poszczególnym użytkownikom bądź grupom użytkowników.
RBAC.20	W momencie Startu Produkcyjnego, System musi mieć zdefiniowane Role uprawnień, określające dostęp do Modułów Systemu dla użytkowników.
RBAC.21	System zarządzania uprawnieniami użytkowników (Rolami) musi umożliwiać m.in.: kopiowanie definicji Ról, grupowe nadawanie uprawnień do Roli (np. po wyborze Roli wskazuje się użytkowników mających mieć do niej uprawnienie), modyfikowanie Ról itp.
RBAC.22	Autentykacja i autoryzacja użytkowników w Systemie będzie realizowana poprzez moduł RBAC.
RBAC.23	Każdy użytkownik w Systemie musi mieć niepowtarzalny identyfikator w systemie (Login).
RBAC.24	Każdy użytkownik musi mieć zdefiniowane hasło w systemie.

RBAC.25	System musi zapewniać dla każdego hasła możliwość zdefiniowania stopnia złożoności hasła co najmniej w zakresie: • minimalnej długości hasła • Poziom złożoności hasła - umożliwia określenie stopnia skomplikowania hasła poprzez zaznaczenie pól wyboru: wymagaj liter - hasło musi zawierać przynajmniej jedną literę od A do Z, wymagaj cyfr - hasło musi zawierać przynajmniej jedną cyfrę od 0 do 9, wymagaj znaków specjalnych - hasło musi zawierać przynajmniej jeden znak spoza grupy znaków alfanumerycznych np. "#", "$", "%", ● wymagaj wielkich i małych liter - hasło musi zawierać przynajmniej jedną literę wielką oraz małą.
RBAC.26	Użytkownik Systemu musi mieć możliwość samodzielnej zmiany hasła w dowolnym momencie po podaniu dotychczas ustawionego hasła.
RBAC.27	Uprawnienia do usuwania/kasowania rekordów obiektów w module winny być reglamentowane. Podobnie nadawania im statusu obiektów niepodlegających podliczeniu.
RBAC.28	W module musi być możliwość zablokowania logowania się do Systemu wszystkich lub wybranych użytkowników (np. w trakcie prowadzonych prac konserwacyjnych).
RBAC.29	W module musi być możliwość wylogowania wszystkich lub wskazanych użytkowników pracujących aktualnie w Systemie.
Moduł Konfiguracji systemowych	
Konfiguracja.1	Konfigurowanie systemu będzie realizowane przez Wykonawcę na podstawie informacji otrzymanych od Zamawiającego. Zamawiający nie będzie samodzielnie konfigurował systemu, chyba że w trakcie analizy przedwdrożeniowej zostaną podjęte inne decyzje.
Konfiguracja.2	Moduł ma umożliwić definiowanie przez Administratora okresu czasu jaki system musi wymuszać na użytkowniku zmianę hasła.
Konfiguracja.2	Administrator musi mieć możliwość tworzenia szablonów widoków dostępnych w całym systemie.
Konfiguracja.3	Moduł musi umożliwiać konfiguracja: 1. Częstotliwości zmiany hasła 2. Ustawienia trudności hasła 3. Danych instytucji 4. Adresów e-mail powiadamiania o zdarzeniach i logach

Konfiguracja.4	Administrator musi mieć możliwość wglądu do modułów logów (historii logowań użytkowników, zdarzeń w systemie).
Konfiguracja.5	Inne wymagania dot. możliwości Administratora systemu zostaną doprecyzowane wraz z Zamawiającym.
Moduł LOGI	
Logi.1	W kontekście użytkowników: funkcję zapisu zdarzeń typu data i czas założenia konta, logowania do systemu (w tym login użytkownika), przeglądania zasobów, modyfikacji danych i udostępniania. Każdy użytkownik powinien mieć możliwość uzyskania raportu dotyczącego własnej aktywności.
Logi.2	W module wszystkie operacje (a w szczególności operacje zmiany konfiguracji, zmiany modelu uprawnień oraz zmiany uprawnień) muszą być audytowane i zapisywane w logach, możliwych do odczytania poprzez Standardowe Oprogramowanie Aplikacyjne na poziomie co najmniej kto, kiedy i co.
Logi.3	Moduł musi zapewniać monitorowanie aktywności użytkowników w Systemie.
Logi.4	Moduł musi wyświetlać listę aktualnie zalogowanych użytkowników.
Logi.5	Moduł musi umożliwiać wyświetlenie listy nieudanych prób logowania do Systemu.
Logi.6	Moduł musi zapewniać możliwość raportowania aktualnie przydzielonych uprawnień.

Wymagania dla funkcjonalności kopii zapasowych	
	Zaoferowane rozwiązania w zakresie wykonywania kopii zapasowych musi zapewnić tworzenie kopii zapasowej danych oraz wszystkich elementów aplikacji w czasie normalnej pracy Systemu.
	Zaoferowane rozwiązania w zakresie wykonywania kopii zapasowych musi zapewnić kopie obiektów bezpośrednio w bazie danych, np. tabel oraz otwartych plików, plików systemowych, itp.
	Zaoferowane rozwiązania w zakresie wykonywania kopii zapasowych musi zapewnić wykonywania kopii zapasowych w trybie kopii pełnej oraz kopii przyrostowej lub różnicowej.
	Zaoferowane rozwiązania w zakresie wykonywania kopii zapasowych musi zapewnić skuteczne mechanizmy odtwarzania danych z wykonanych kopii zapasowych.