Badanie rynku - Zapytanie o informację cenową

Elektroniczna Platforma Zakupowa (EPZ) na potrzeby Spółek Grupy Enea

1. **Przedmiot zamówienia**
   1. przedmiot zamówienia obejmuje:

* udostępnienie skonfigurowanej i dostosowanej do wymagań funkcjonalnych określonych w niniejszym zapytaniu Elektronicznej Platformy Zakupowej na potrzeby prowadzenia postępowań i aukcji,
* udzielenie licencji w celu korzystania z tej platformy przez Spółki Grupy Enea,
* świadczenie usług utrzymaniowych,
* realizacja szkoleń i świadczenie usług rozwojowych,
  1. warianty wdrożenia:
* on-premises,
* Saas.

1. **Planowany termin realizacji przedmiotu zamówienia, czas trwania umowy**
   1. planowane udzielenie zamówienia (podpisanie umowy) – czerwiec 2023,
   2. czas korzystania z licencji i świadczenia usług ATIK– 36 mies. od daty realizacji przedmiotu zamówienia (zakończenia wdrożenia).
2. **Szkolenia/instrukcje**

Na potrzeby zapytania o informację cenową Zamawiający prosi o wycenę 1 dnia (6h) zdalnego szkolenia dla max. 30 użytkowników końcowych Grupy ENEA (na jednym szkoleniu) – szkolenia realizowane będą w terminie do 6 mies. od zawarcia umowy.

Wykonawca przygotuje i udostępni instrukcje dla użytkowników końcowych Enea, a także użytkowników Wykonawców obejmujących procesy prowadzone na Platformie.

1. **Szacunkowe dane ilościowe dot. Platformy**

W ramach przedmiotu zamówienia Zamawiający zakłada konfigurację i udostępnienie Platformy dla Spółek Grupy Enea zgodnie z poniższymi danymi ilościowymi.

|  |  |
| --- | --- |
| **Ilość Spółek GK Enea, którym na etapie wdrożenia udostępniana jest Platforma** | **3** |
| **Szacowana ilość postępowań prowadzonych w EPZ rocznie** | **3000** |
| **Szacowana ilość kont użytkowników ENEA** | **1500** |

Platforma zapewnia możliwość dołączenia również innych Spółek Grupy Enea (poza wskazanymi powyżej). Udostępnianie EPZ innym Spółkom będzie ewentualnie realizowane w ramach odrębnych zleceń.

1. **Dostępność + SLA**
2. Dostępność Platformy przez 24 godziny na dobę w dni robocze na poziomie nie niższym niż 95% w rozliczeniu miesięcznym. Przez dni robocze należy rozumieć dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w rozumieniu ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy („Dni Robocze”).
3. Wykonawca zobowiązuje się do świadczenia usług Wsparcia Technicznego w godzinach 8:00-16:00 w dni robocze. Przez dni robocze należy rozumieć dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w rozumieniu ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy („Dni Robocze”).
4. Wymagany czas przywrócenia pełni funkcjonalności platformy w przypadku błędów o kategoriach:
   1. w przypadku Błędu Krytycznego –2 (dwie ) godziny;
   2. w przypadku Błędu Istotnego – 16 (szesnaście) godzin;
   3. w przypadku Błędu Nieistotnego – 4 (cztery) dni robocze.
5. **Helpdesk dla użytkowników kontrahentów**

Wykonawca zapewni pierwszą linię wsparcia dla kontrahentów zewnętrznych. Wsparcie świadczone drogą telefoniczną obejmuje w szczególności kompleksową pomoc dla kontrahentów w zakładaniu i obsłudze kont na Platformie, a także wsparcie w zakresie uczestnictwa w procesach prowadzonych w EPZ oraz w poruszaniu się po Platformie. Zamawiający wymaga zapewnienia dostępności infolinii przynajmniej w godzinach 8-16 w dni robocze.

1. **Wymagania Infrastruktury**
2. techniczne warunki wdrożenia dla wariantu On-premises:

Na potrzeby wdrożenia systemu Zamawiający zapewni własną infrastrukturę informatyczną obejmującą cały obszar wdrożenia systemu

|  |
| --- |
| Zamawiający udostępni środowisko na serwerach z procesorami INTEL z oprogramowaniem VMware vSphere do wirtualizacji.  Dopuszczalne systemy operacyjne serwerów dla tego środowiska :   * system operacyjny Windows Server 64-bit * system operacyjny Oracle Linux 8 64-bit   Zamawiający wymaga aby Program działał na najnowszych wersjach systemów operacyjnych wymienionych powyżej. Zastosowanie innych wersji wymaga uzgodnienia z Zamawiającym. |
| Zamawiający udostępni jeden z następujących systemów bazodanowych:   * ORACLE Database 19 * Microsoft SQL Server 2019 * MariaDB Server 10 * Postgre SQL Server 9 |
| Środowisko stacji roboczych **Zamawiającego** jest objęte Domeną Windows z usługą Active Directory. Program będzie zintegrowany z AD i będzie miał zaimplementowany mechanizm SSO. |
| Specyfikacja standardowej stacji roboczej:   * Procesor min. Intel i5-5200U * Pamięć RAM min. 8GB * Dysk twardy min. 250 GB * System operacyjny  Windows 10 (64bit) * Pakiet biurowy MS Office * Przeglądarki EDGE, Chrome, FireFox |
| Zamawiający dopuszcza następujące serwery aplikacji:   * Oracle WebLogic Server * Microsoft IIS Server * Apache HTTP Server + PHP |
| **Wykonawca**, może prowadzić prace zdalnie poprzez zestawienie tunelu VPN pomiędzy Wykonawcą a Zamawiającym. W tym celu **Zamawiający** udostępni oprogramowanie klienta VPN dla systemów Windows i Linux oraz metodę uwierzytelniania sesji. W trakcie połączenia VPN, w systemie operacyjnym klienta zostaną wyłączone pozostałe połączenia sieciowe. Terminy sesji VPN poszczególnych klientów muszą być uzgadniane z **Zamawiającym**. |

1. **Wymagania funkcjonalne**

|  |  |  |
| --- | --- | --- |
| Opis wymagań funkcjonalnych/ modułów Elektronicznej Platformy Zakupowej | | |
| **l.p.** | **Wymaganie** | **Doszczegółowienie wymagań** |
| **1.** | **Rejestracja i obsługa kont kontrahentów oraz użytkowników kontrahentów** | * 1. Samodzielna rejestracja kont przez kontrahentów.   2. Zarządzanie bazą kontrahentów.   3. Możliwość przypisania kontrahenta do wybranych asortymentów/ branż (zgodnie z matrycą kategorii zakupowych GK ENEA);   4. Możliwość rejestracji kont w EPZ przez osoby fizyczne oraz podmioty zagraniczne nieposiadające NIP.   5. EPZ zapewnia możliwość wzięcia udziału w procesach prowadzonych w EPZ przez użytkowników ENEA również w roli kontrahentów.   6. Zabezpieczenie kont kontrahentów (potwierdzenie adresu e-mail, samodzielny reset hasła).   7. W ramach konta kontrahenta możliwość rejestracji kilku kont użytkowników (adresów e-mail). |
| **2.** | **Tworzenie i obieg wniosków zakupowych** | * 1. Platforma zapewnia możliwość tworzenia wniosków zakupowych/zapotrzebowań.   2. W zależności od Spółki postępowanie może być inicjowane na podstawie zaakceptowanego wniosku zakupowego lub bez wniosku zakupowego.   3. Wnioski podlegają procesowi akceptacji przez zdefiniowanych użytkowników.   4. Platforma zapewnia możliwość uwzględnienia na wniosku zakupowym dodatkowych wymaganych pól, a także załączników w tym m.in. * Jednostka org. która zleca postępowanie * Kategorie zakupowe * Nr planu zamówień * Szacowane wartości * Pola tekstowe   1. Platforma zapewnia możliwość powiązania wniosku zakupowego z RFI/RFP oraz z postępowaniem o udzielenie zamówienia.   2. Możliwość przypisywania użytkowników (kupców) do wniosku/postępowania przez zdefiniowanych użytkowników (menadżerów). |
| **3.** | **Prowadzenie postępowań o udzielenie zamówienia w trybach regulaminowych oraz zgodnie z ustawą PZP** | * 1. Realizacja postępowań PZP oraz w trybach otwartych i zamkniętych na podstawie regulaminów (tj. bez stosowania ustawy PZP);   2. Prowadzenie rozeznania rynku (RFI/RFP);   3. Możliwość przesłania zaproszenia do udziału w postępowaniu również do Dostawców nieposiadających konta w EPZ (np. wpisanie adresu mailowego ręcznie).   4. Komunikacja elektroniczna z kontrahentami w procesie prowadzenia postępowań, udzielanie odpowiedzi na pytania bez ujawnienia źródła, przekazywanie załączników;   5. Publikacja oraz modyfikacja ogłoszeń o postępowaniu i załączników;   6. Możliwość tworzenia wielu list wysyłkowych Wykonawców w celu zbiorczego informowania o postępowaniach otwartych i zbiorczego zapraszania do postępowań zamkniętych (na jednej liście wysyłkowej może być kilkuset wykonawców).   7. Określanie terminów w postępowaniu, w szczególności terminu publikacji postępowania, terminu składania ofert/wniosków, terminu zadawania pytań – system umożliwia przekazanie przez kontrahentów pytań do postępowania po upływie zdefiniowanego terminu zadawania pytań, jednoczenie sygnalizując (np. za pomocą komunikatu pop-up), że pytania mogą pozostać bez odpowiedzi.   8. Przesyłanie załączników przez kontrahentów (w tym JEDZ, oświadczeń, wniosków i ofert);   9. Szyfrowanie i zabezpieczenie ofert i wniosków, ochrona przed dostępem do treści ofert oraz wniosków o dopuszczenie do udziału w postępowaniu przed upływem wyznaczonych terminów ich otwarcia;   10. Zarządzanie rolami i uprawnieniami użytkowników Zamawiającego w postępowaniu (komisja przetargowa, kierownik zamawiającego)   11. Prowadzenie postępowania w podziale na produkty oraz na zadania/części.   12. Możliwość prowadzenia w różnym czasie niezależnych negocjacji na wybrane części (zadania) postępowania (np. kolejnej rundy składania ofert lub aukcji). Poszczególne części postępowania mogą być rozstrzygane niezależnie.   13. Możliwość określenia różnych kryteriów oceny ofert i ich wag, trendu i jednostek.   14. Możliwość określenia odrębnych lub tożsamych warunków udziału w postępowaniu i kryteriów oceny ofert dla każdej części (zadania) postępowania.   15. Automatyczne obliczanie punktacji i rankingu ofert w postępowaniu.   16. Możliwość wyboru oferty jednego lub wielu kontrahentów w ramach każdej części (zadania) postępowania.   17. Możliwość tworzenia ścieżek workflow w postępowaniu, czynności w ramach postępowania kierowane są do akceptacji przez użytkowników stanowiących komisję przetargową w danym postępowaniu i/lub kierownika zamawiającego w tym postępowaniu.   3.17.1. Akceptacji przez użytkowników z rolą Kierownik Zamawiającego lub Przewodniczący podlegają w szczególności następujące czynności:   * publikacja postępowania, * modyfikacja postępowania, * odpowiedź na pytania do postępowania, * wykluczanie kontrahentów, * odrzucanie ofert kontrahentów, * informacja o wyniku postępowania.   3.17.2. Proces wyboru najkorzystniejszej oferty w postępowaniu/zadaniu postępowania, oraz decyzja o unieważnieniu postępowania/ zadania postępowania podlega specyficznemu procesowi akceptacji:   * w pierwszej kolejności decyzja opiniowania jest przez członków komisji (rekomendacje komisji), każdy z członków może złożyć zdanie odrębne, * finalna decyzja podejmowana jest przez kierownika zamawiającego (nie musi być zgodna z rekomendacją komisji).   3.17.3. Platforma zapewnia możliwość przerwania procesu akceptacji (np. zatrzymanie procesu workflow w celu ponownej edycji dokumentu i akceptacji). EPZ zapewnia możliwość ponownego uruchomienia procesu akceptacji po zmianach.   * 1. Możliwość samodzielnego wygenerowania protokołu z postępowania (w formie raportu) szczegółowo odzwierciedlającego przebieg postępowania, a także proces akceptacji wyboru ofert w postępowaniu lub unieważnienia.   2. Platforma zapewnia możliwość unieważnienia postępowania w całości lub poszczególnych części (zadań), a także odrzucenia ofert kontrahentów na każdym etapie postępowania w ramach poszczególnych części (zadań), a także możliwość wykluczenia kontrahenta.   3. Możliwość importu produktów do postępowania z plików płaskich.   4. Możliwość uwzględnienia w EPZ wymaganych przez ENEA dodatkowych pól widocznych wewnętrznie lub również zewnętrznie dotyczących:   5. całego postępowania (np. pole wielokrotnego wyboru „Spółki objęte postępowaniem”, „Regulamin”, „Tryb postępowania”,   6. zadań postępowania (np. kody CPV)   7. poszczególnych produktów (np. kategoria zakupowa, indeks materiałowy, szacowana wartość);   8. EPZ zapewnia możliwość złożenia przez każdego z członków komisji, kierownika zamawiającego, a także biegłych oświadczenia o bezstronności na każdym etapie postępowania (standardowy moment złożenia oświadczenia jest inny w przetargach zamkniętych i otwartych).   9. Możliwość dokonywania zmian/zastępstw wśród użytkowników stanowiących komisję przetargową kierownika zamawiającego. |
| **4.** | **Prowadzenie aukcji elektronicznych (regulaminowych i zgodnie z ustawą PZP)** | * 1. Prowadzenie aukcji jako etapu negocjacji w postępowaniu.   2. Prowadzenie aukcji niezależnie.   3. Tworzenie aukcji testowych.   4. Tworzenie szablonów aukcji.   5. Przenoszenie ofert kontrahentów do aukcji z etapu postępowania.   6. Prowadzenie aukcji w oparciu o różne reguły np. składana oferta musi być korzystniejsza od najlepszej oferty w rankingu lub oferta musi być lepsza od najlepszej oferty danego kontrahenta, możliwość określenia ceny maksymalnej (wywoławczej), ceny minimalnej oraz wysokości minimalnego postąpienia lub wysokości wymaganego przebicia ostatniej oferty kontrahenta lub oferty prowadzącej.   7. Możliwość ustawienia czy system dopuszcza remisy podczas aukcji (ewentualny remis obejmuje sumę punktów wyliczoną po uwzględnieniu wszystkich kryteriów oceny podlegających aukcji oraz kryteriów stałych, określonych przed aukcją)   8. Zarządzanie widocznością parametrów aukcji dla kontrahentów przez Zamawiającego.   9. Możliwość ustalenia czasu podstawowego oraz czasu i ilości dogrywek w ramach aukcji.   10. Aukcje mogą być prowadzone niezależnie na wybrane części (zadania) postępowania, w ramach każdego z zadań może być zdefiniowanych wiele produktów (linii) przetargu. Konstrukcja aukcji odzwierciedla konfigurację postępowania.   11. Kryteria oceny ofert w aukcjach powinny być skonstruowane w czytelny sposób, kryterium „cena” nie może być uwarunkowane od ustawienia zaokrągleń – zawsze powinna wygrywać oferta z korzystniejszą ceną bez względu na kolejność złożenia postąpień.   12. Możliwość wyboru przez kontrahenta przy aukcjach multiobiektowych pozycji, dla których kontrahent chce złożyć postąpienie. Pozycje, dla których nie dokonano postąpień automatycznie zostaną zaczytane niezmienionymi kwotami.   13. EPZ nie wymaga od kontrahenta aktywnego udziału w aukcji. W przypadku ofert złożonych na wcześniejszych etapach postępowania, oferty są przenoszone do prowadzonej aukcji elektronicznej. Kontrahent, który złożył ofertę w postępowaniu nie musi brać czynnego udziału w aukcji, a jego oferta jest podtrzymana.   14. Możliwość uwzględnienia kryteriów stałych w prowadzonej aukcji, które nie podlegają licytacji natomiast uwzględniane są w dynamicznym rankingu podczas aukcji.   15. Minimalne wymagania w zakresie obsługiwanych typów aukcji: * aukcja zniżkowa i zwyżkowa, * aukcja japońska, * aukcja multiobiektowa, * aukcja wielokryterialna, * aukcja multiobiektowa-wielokryterialna. |
| **5.** | **Generowanie raportów** | * 1. Zapewnienie konfiguracji i dostępu do standardowych raportów obejmujących procesy prowadzone w EPZ w szczególności raport z pojedynczego postępowania oraz aukcji, a także zbiorcze raporty z prowadzonych postępowań (Excel).   2. Możliwość zarządzania uprawnieniami w zakresie dostępu do raportów.   3. Opracowanie innych szczegółowych raportów zgodnie z wymogami zamawiającego (dodatkowe godziny programistyczne). Możliwość raportowania na podstawie wszystkich dostępnych pół w EPZ. |
| **6.** | **Zarządzanie uprawnieniami/**  **rolami** | * 1. Odzwierciedlenie w EPZ struktury wielospółkowej.   2. Zapewnienie możliwości nadawania, odbierania, a także tworzenia i zarządzania rolami i uprawnieniami użytkowników oraz grupami użytkowników przez Administratorów ENEA. Czynności te muszą być jednolite i scentralizowane dla wszystkich modułów/aplikacji składających się na System EPZ.   3. Uprawnienia „globalne” - możliwość zarządzaniem dostępem do modułów/funkcjonalności Platformy poprzez uprawnienia (widoczność/ukrycie: określonych opcji, widoków, okien, elementów procesu, elementów menu itp.).   4. Uprawnienia „indywidualne” - możliwość zawężenia dostępu, poprzez nadanie ról i uprawnień do prowadzonych postępowań/aukcji wyłącznie określonym użytkownikom stanowiącym np. komisję przetargową, kierownika zamawiającego, Administratora ENEA. Zakres czynności możliwych do wykonania w ramach postępowania różni się w zależności od nadanej roli.   5. Platforma zapewnia w szczególności możliwość utworzenia ról z uprawnieniami do tworzenia, modyfikacji, odczytu:   6. wszystkich postępowań prowadzonych w wybranej spółce/spółkach ENEA,   7. wszystkich postępowań prowadzonych na Platformie,   8. wybranych postępowań, w których użytkownik wskazany był w komisji przetargowej lub jako kierownik zamawiającego,   9. odczytu i modyfikacji ustawień systemu (dostęp administracyjny). |
| **7.** | **Pozostałe wymagania** | * 1. Zgodność z Ustawą PZP i przepisami wykonawczymi wydanymi na jej podstawie.   2. W przypadku zmian przepisów prawa obejmujących procesy prowadzone na EPZ Wykonawca wdroży te zmiany w ramach świadczonych usług, bez dodatkowych kosztów po stronie Zamawiającego.   3. Integracja z centralną platformą e-Zamówienia, w terminach i zakresie wynikającym z odpowiednich przepisów prawa.   4. Interfejs użytkownika kontrahenta w co najmniej dwóch językach – polskim oraz angielskim.   5. Platforma korzysta z zaufanego serwera czasu – możliwe jest ustalenie dokładnego czasu wystąpienia istotnych zdarzeń w postępowaniach.   6. Platforma zapewnia funkcjonalności monitorowania przebiegu procesu workflow z możliwością informowania o przekroczeniach terminów.   7. EPZ zapewnia możliwość przesyłania automatycznych powiadomień mailowych zarówno do użytkowników Kontrahentów jak i użytkowników Zamawiającego informujących o istotnych zdarzeniach w systemie dotyczących m.in. zbliżających się lub upływających terminów w postępowaniu, modyfikacji postępowania (zmiana terminu/opisu/dodanie załączników) czy przesłania pytań do postępowania.   8. W ramach umowy Wykonawca zapewni dostęp do historii postępowań zakupowych i aukcji, przeprowadzonych w okresie obowiązywania umowy, w szczególności do wszystkich raportów, konfiguracji, logów i załączników do tych postępowań i aukcji. Dostęp, o którym mowa w zdaniu poprzednim, powinien być zapewniony w formie bezpośredniego dostępu online przez okres przewidziany w Ustawie PZP, bądź poprzez przekazanie Zamawiającemu na elektronicznych nośnikach danych, w formacie umożliwiającym Zamawiającemu samodzielny odczyt danych. |

**9. Wymagania bezpieczeństwa IT**

1. **A. Dla wersji On-premises** :
   * 1. System musi umożliwiać pracę w sieci poddanej separacji i segmentacji poprzez firewalle. Dla ochrony aplikacji należy zastosować WAF, a dla ochrony baz danych DAM.
     2. System musi wykorzystywać protokół TSL (min. v1.2) oraz klucze i certyfikaty X.509, do zapewnienia integralności danych, niezaprzeczalności i poufności w kanałach transmisyjnych.
     3. System musi ograniczać uprawnienia technicznych użytkowników i administratorów do niezbędnego minimum.
     4. System musi uruchamiać tylko niezbędne usługi i aplikacje.
     5. System musi posiadać zdefiniowany mechanizm wgrywania poprawek oraz nowych wersji systemu.
     6. System musi posiadać wydzielone środowisko testowe i powinien posiadać środowisko deweloperskie, dla umożliwienia przetestowania zmian przed implementacją w środowisku produkcyjnym.
     7. System musi być wdrożony i utrzymywany na infrastrukturze teleinformatycznej GK ENEA.
     8. System dostępny za pośrednictwem protokołu http powinien być sprawdzony przez Wykonawcę pod kątem odporności na błędy określone w standardzie OWASP (najnowszym) https://www.owasp.org/.
     9. Wykonawca włączy wskazówki dotyczące cyberbezpieczeństwa do dokumentacji Systemu dostarczonego do Zamawiającego. Dokumentacja ta powinna zawierać wskazówki, jak skonfigurować System i/lub otaczające go środowisko teleinformatyczne, aby jak najlepiej zapewnić bezpieczeństwo. Obejmuje ona również wskazówki, które porty logiczne lub fizyczne są wymagane, aby System działał.
     10. Wykonawca stosuje praktykę, zgodnie z którą aplikacje internetowe na styku z Internetem znajdują się na serwerze innym niż ten, który zawiera bazę danych.
     11. Komunikacja IP między elementami Systemu musi być zaszyfrowana przy użyciu ogólnodostępnych algorytmów z wykorzystaniem mocnych szyfrów (niedopuszczalne jest korzystanie a nawet umożliwienie korzystania ze słabych skompromitowanych algorytmów i szyfrów np. SSL2, SSL3, RC4, DH mniejszych niż 2048 bitów itd.). Rekomenduje się korzystanie z TLS v1.2 lub wyższego. Można posiłkować się listą ze strony https://ciphersuite.info/cs/ .
     12. Wykonawca nie będzie wykorzystywał chmur publicznych (np. AWS, GCP, Azure) i publicznych zasobów plikowych (np. DropBox, Google Drive, OneDrive) do wykonywania powierzonych przez Zamawiającego zadań, które wymagają przetwarzania wrażliwych informacji (np. plików konfiguracyjnych, logów, danych osobowych).
     13. System musi umożliwiać integrację z Systemem Zarządzania Tożsamością Zamawiającego lub integrację z bazą ActiveDirectory lub OpenLDAP lub Cisco ACS Zamawiającego.
     14. Architektura Systemu musi uniemożliwiać współdzielenie kont (również administracyjnych).
     15. Należy stosować blokadę konta dla kolejnych nieudanych prób logowania na wszystkich urządzeniach końcowych obsługujących System.
     16. System musi automatycznie zamykać sesję zalogowanego użytkownika po określonym czasie nieaktywności konfigurowalnym przez administratora w tym Systemie.
     17. System nie może wyświetlać informacji nt. rzeczywistych przyczyn odrzucenia dostępu (np. czy było to z powodu błędnego loginu czy hasła).
     18. System musi zapewniać system uprawnień, który umożliwia ograniczenie dostępu wyłącznie do takich informacji oraz takiego zakresu funkcji, jaki jest niezbędny użytkownikowi.
     19. Należy ograniczyć dostęp do środowisk deweloperskich i testowych tylko dla uprawnionego personelu.
     20. Dostęp do Systemu jest poprzedzony identyfikacją i uwierzytelnieniem użytkownika (nie ma możliwości obejścia mechanizmów logowania).
     21. System zapewnia mechanizmy kontroli uprawnień oparte na rolach oraz umożliwia określanie ról i uprawnień.
     22. System umożliwia wylistowanie (lub splikowanie, lub wydrukowanie) raportów zawierających wszystkie/wybrane profile i uprawnienia użytkownika lub grupy użytkowników w określonym przedziale czasowym.
     23. Usługi systemowe (daemon) muszą pracować na specjalnie przygotowanym koncie z minimalnymi uprawnieniami niezbędnymi do pracy usługi. Nie dopuszczalne jest uruchamianie usług na kontach typu root i administrator.
     24. System zapewnia poprawną obsługę błędów i nie prezentuje informacji z wewnętrznych aplikacji (np. z baz danych, kodów źródłowych, plików konfiguracyjnych).
     25. Nie wykorzystuje się danych produkcyjnych zarówno do programowania, jak i do testowania.
     26. Dane wrażliwe muszą być przechowywane na serwerze w postaci zaszyfrowanej (np. dane uwierzytelniające, kody, nr kart).
     27. Dane wejściowe do Systemu podlegają mechanizmowi kontroli i filtracji, które zapewniają wykrywanie następujących błędów:

a. wartości spoza dopuszczalnego zakresu;

b. niewłaściwych znaków w polach danych;

c. brakujących, niepoprawnych lub niekompletnych danych;

d. przekraczania górnych i dolnych ograniczeń wielkości danych;

e. nieuprawnionych lub niespójnych danych kontrolnych.

* + 1. System zapewnia odpowiednie walidowanie wszystkich wprowadzonych danych uniemożliwiając uzyskanie nieautoryzowanego dostępu do danych:

a. nieautoryzowanego wywoływania poleceń/zapytań;

b. wykonania skryptu;

c. podmiany zawartości danych;

d. przekierowania użytkownika na inną stronę.

* + 1. System musi posiadać mechanizmy umożliwiające rozliczalność działań.
    2. System musi spełniać wymagania obowiązującej polityki haseł w GK ENEA (w chwili obecnej jest to hasło minimum 8 znakowe, zawierające przynajmniej jedną wielką literę, przynajmniej jedną małą literę, przynajmniej jedną cyfrę lub znak specjalny, wymuszona zmiana hasła co 30 dni, brak możliwości powtarzania używanych wcześniej haseł, system pamięta funkcje skrótu 24 ostatnio używanych haseł).
    3. System nie może przechowywać haseł tylko ich funkcje skrótu i nie może to być MD5 ani SHA1, tylko mocniejsze zabezpieczenie. Dopuszczona jest możliwość przechowywania zaszyfrowanych haseł, w takim przypadku klucz szyfrujący musi być przechowywany na systemie HSM Zamawiającego.
    4. Wykonawca zmienia lub wyłącza wszystkie domyślne hasła lub opublikowane kody dostępu do wszystkich zainstalowanych przez siebie komponentów IT (np. systemów operacyjnych, systemów zarządzania bazami danych, urządzeń sieciowych, pakietów aplikacji itp.).
    5. Wprowadzane przez użytkowników hasła nie mogą być zapisywane i przechowywane po stronie klienta.
    6. Wykonawca posiada wytyczne bezpiecznego kodowania dla języków programowania używanych w procesie programowania dla Zamawiającego.
    7. Wykonawca w okresie gwarancji musi zadbać o regularną aktualizację oprogramowania, a w przypadku błędów związanych z bezpieczeństwem dokona aktualizacji niezwłocznie po jej udostępnieniu przez producenta rozwiązania.
    8. Do aktualizacji należy stosować bezpieczne repozytoria.
    9. Wszystkie elementy Systemu wysyłają swoje logi do systemu SIEM Zamawiającego lub serwera SYSLOG Zamawiającego.
    10. Należy chronić informacje przechowywane w dziennikach zdarzeń (logach) przed manipulacją/usunięciem i nieautoryzowanym dostępem.
    11. System posiada mechanizmy audytu zdarzeń wraz z:

a. rejestracją daty i czasu;

b. adresu IP;

c. identyfikatora użytkownika;

d. opisu zdarzenia (np. wywołania klienta i odpowiedzi serwera, udanych i nieudanych prób logowania do systemu, wylogowania użytkownika, zerwania sesji, wykonanych działań, zmiany danych (w tym parametrów systemowych, uprawnień dostępu, zablokowania/odblokowania konta), błędów i awarii systemu, ataków na system).

* + 1. System umożliwia synchronizację czasu (np. w domenie AD lub z serwerem NTP).
    2. Należy wykorzystywać obowiązującą u Zamawiającego architekturę DMZ przy działaniu Systemu.
    3. Zamawiający okresowo będzie dokonywał testów bezpieczeństwa, głównie polegających na wykrywaniu podatności, a Wykonawca w okresie gwarancji/obowiązywania umowy jest zobowiązany do niezwłocznego usunięcia wskazanych przez Zamawiającego podatności i wykrytych luk.
    4. Wszystkie komponenty IT wykorzystywane przez System muszą posiadać wsparcie producenta (przynajmniej w zakresie dostarczania i instalowania poprawek bezpieczeństwa dla każdego komponentu przynajmniej w okresie obowiązywania umowy lub korzystania przez Zamawiającego z tego Systemu. Zalecane jest korzystanie z najnowszej stabilnej wersji). W szczególności :

- system operacyjny Windows Server 19 64-bit lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- system operacyjny Oracle Linux 8 64-bit lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- Microsoft SQL Server 2019 lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- MariaDB w wersji 10.11 lub wyższej posiadającej wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- PostgreSQL Server 12 lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- ORACLE Database w wersji 19c lub wyższej posiadającej wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- Oracle WebLogic Server 14.1.x lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- Microsoft IIS 10 on Windows Server 2019 lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- Apache HTTP Server 2.4 lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa;

- PHP 8.1 lub wyższy posiadający wsparcie producenta w zakresie aktualizacji luk bezpieczeństwa.

1. **B. Dla wersji SaaS :**
2. Takie same jak dla wersji on-premises z wyłączeniem punktów 7, 12, 13, 41;
3. Punkt 37 z wersji on-premises zmienia w tym przypadku swoją treść na: „Wszystkie elementy Systemu wysyłają swoje logi do systemu SIEM Dostawcy lub serwera SYSLOG Dostawcy”;
4. Punkt 31 z wersji on-premises zmienia w tym przypadku swoją treść na: „System nie może przechowywać haseł tylko ich funkcje skrótu i nie może to być MD5 ani SHA1, tylko mocniejsze zabezpieczenie. Dopuszczona jest możliwość przechowywania zaszyfrowanych haseł, w takim przypadku klucz szyfrujący musi być przechowywany na systemie HSM Dostawcy”;
5. Posiadanie przez Dostawcę aktualnych certyfikatów z zakresu bezpieczeństwa w chmurze np. CSA CCM (Cloud Control Matrix) lub CSA STAR lub ISO/IEC 27017.