Szczegółowy Opis Przedmiotu Zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. zaprojektowanie, wykonanie i wdrożenie strony intranetowej GDOŚ (również jako „**Strona**" lub „**Intranet**"),
2. przeprowadzenie szkolenia dla administratorów/redaktorów Strony („**Szkolenia**"),
3. świadczenie usługi wsparcia (przez okres 12 miesięcy od dnia podpisania protokołów zdawczo-odbiorczych zadań , o których mowa w pkt. 1 i 2 powyżej) polegającego na pomocy administratorom/redaktorom Strony oraz prowadzenia płatnych prac rozwojowych, powdrożeniowych na zlecenie Zamawiającego („**usługa wsparcia**").

II. Założenia

Intranet powinien być nowoczesnym, przejrzystym oraz intuicyjnym w obsłudze serwisem informacyjno-integracyjnym dedykowanym pracownikom zatrudnionym w Generalnej Dyrekcji Ochrony Środowiska. Wykonawca zainstaluje przygotowaną Stronę w oparciu o infrastrukturę własną GDOŚ.

III. Termin realizacji Zamówienia:

Zadania opisane w pkt I ppkt 1 i 2 – **do 17 grudnia 2020 r.**

Zadanie opisane w pkt I ppkt 3 – **12 miesięcy** od dnia podpisania protokołów zdawczo-odbiorczych zadań opisanych w pkt. I ppkt. 1-2.

IV. Wymagania Zamawiającego dot. realizacji zamówienia:

1. Wymagania pozafunkcjonalne (ogólne)

1.1. Intranet musi być dostępny za pomocą logowania poprzez konto domenowe z integracją Active Directory.

1.2. Intranet musi być dostępny w sieci Internet dla zalogowanego użytkownika.

1.3. Intranet musi być responsywny.

1.4. Intranet musi mieć przygotowaną wersję desktopową oraz wersję mobilną automatycznie dostosowującą wyświetlanie do rodzielczości urządzeń.

1.5. Intranet musi być przystosowany do obsługi conajmniej jednocześnie zalogowanych 200 użytkowników.

1.6. Intranet musi być przygotowany w szacie graficznej zgodnej z Księgą Identyfikacji Wizualnej Generalnej Dyrekcji Ochrony Środowiska.

1.7. Podstawowym językiem systemu Intranetu musi być język polski (portal, panel administracyjny, dokumentacja/pomoc dla użytkowników i administratorów).

1.8. Dokumentacja Intranetu musi zawierać wszelkie informacje niezbędne, by umożliwić Zamawiającemu jego dalszy rozwój i/lub modyfikację bez udziału Wykonawcy.

1.9. Wykonawca zobowiązany jest udostępnić co najmniej dwa środowiska systemu Intranetu w infrastrukturze sieciowo-sprzętowej Zamawiającego: Środowiska produkcyjnego, Środowiska testowo - szkoleniowego.

2. Ogólna struktura Intranetu

2.1. System Intranetu musi posiadać konstrukcję modułową.

2.2. System Intranetu musi mieć możliwość rozbudowy dowolnego modułu (również modułów niezależnie od siebie).

2.3. System Intranetu musi mieć możliwość rozbudowy wewnętrznej architektury modułowej o kolejne moduły.

2.4. System Intanetu musi mieć możliwość w przyszłości poszerzenia liczby użytkowników o pracowników jednostek podległych (regionalne dyrekcje – ok. 1700 osób).

2.5. System Intranetu musi posiadać narzędzia służące do zarządzania strukturą Intranetu z poziomu panelu administratora wraz z możliwością samodzielnej budowy wielopoziomowych menu oraz konfiguracji sposobu wyświetlania.

2.6. System Intranetu musi umożliwiać łatwą zmianę kolejności pozycji menu w danej kategorii oraz położenia kategorii względem siebie.

2.7. System Intranetu musi posiadać narzędzia umożliwiające pełne zarządzanie wszystkimi modułami z poziomu graficznego interfejsu administratora dostępnego z poziomu przeglądarki internetowej.

2.8. System Intranetu musi być tak wewnętrznie powiązany, aby wprowadzone dane do jednego modułu były automatycznie publikowane w module powiązanym we wskazanym miejscu.

2.9. System Intranetu musi umożliwiać wydruk oraz możliwość wygenerowania PDF dowolnej strony z poziomu opublikowanej treści.

2.10. System Intranetu musi mieć możliwość podłączenia Really Simple Syndication (RSS).

2.11. System Intranetu musi zapewniać ciągły dostęp do wszystkich danych gromadzonych w Portalu, w okresie jego eksploatacji zgodnie z przypisanymi prawami dostępu.

2.12. Architektura systemu Intranetu musi uwzględniać niezawodność, skalowalność, wysoką dostępność (ang. High Availability) oraz wydajność.

2.13. Użytkownik na każdej stronie/podstronie Intranetu musi mieć możliwość zgłoszenia uwag dot. nieaktualnych treści – poprzez przycisk ZGŁOŚ NIEAKTUALNĄ TREŚĆ musi otworzyć się formularz kontaktowy, zgłoszenie na wskazany przez Zamawiającego adres email.

3. Zarządzanie uprawnieniami

3.1. System Intranetu musi umożliwiać definiowanie różnych poziomów dostępu dla administratorów IT oraz definiowanie zakresów dostępów do danych, którymi mogą zarządzać.

3.2. System Intranetu musi umożliwiać definiowanie różnych poziomów dostępu dla administratorów (głównych, wydziałowych i IT) oraz zakresy treści, którymi mogą zarządzać.

3.3. System Intranetu musi umożliwiać definiowanie różnych poziomów dostępu dla administratorów modułowych (administratorów wydziałowych), oraz określenia zakresu treści, którymi mogą zarządzać.

3.4. System Intranetu musi posiadać funkcjonalność nadawania i kontroli uprawnień użytkownikom.

3.5. System Intranetu musi umożliwiać tworzenie dowolnych grup użytkowników i przypisywać uprawnienia grupom. Grupy mogą być tworzone na podstawie stanowisk czy realizowanych funkcji, np. grupy dyrektorów / dana grupa projektowa.

3.6. System Intranetu musi uwzględniać co najmniej następujące typy uprawnień:

3.6.1. administrator główny – możliwie najszersze uprawnienia i dostęp do wszystkich publikowanych treści,

3.6.2. administrator wydziałowy – dostęp i administrowanie określonym zakresem treści – poszczególne części modułów wydziałowych,

3.6.3. administrator IT – osoba odpowiedzialna za ogólne działanie systemu, realizująca czynności związane z wgrywaniem poprawek do systemu, obsługę interfejsu, monitorująca pracę systemu, konfigurująca aplikacje,

3.6.4. użytkownik – osoba korzystająca z Intranetu z uprawnieniami zgodnie z dopisanymi grupami.

3.7. System Intranetu musi umożliwiać nadawanie takich samych uprawnień co do tego samego zakresu kilku administratorom.

3.8. Definiowanie i nadawanie uprawnień musi odbywać się z poziomu zaplecza administracyjnego systemu Intranetu i być niezależne od Wykonawcy.

3.9. System Intranetu musi umożliwiać utworzenie co najmniej 50 kont o uprawnieniach administracyjnych bez potrzeby zmian w architekturze systemu Intranetu.

4. Wymagania dot. modułu „Kontakty / struktura organizacyjna”

Skrótowy opis modułu:

Po kliknięciu w przycisk „**Kontakty / struktura organizacyjna**” (nazwa robocza, co do której musi być możliwość zmiany) ze strony głównej otwiera się strona ze skróconą wersją wizytówek/identyfikatorów pracowników.

Skrócona wersja wizytówek to tabela zawierająca rekordy ułożone domyślnie w kolejności alfabetycznej zawierająca co najmniej: zdjęcie, imię, nazwisko, nazwę jednostki, stanowisko, komórka organizacyjna (referat i wydział pracownika). Po kliknięciu w którekolwiek pole przechodzimy do wizytówki pełnej.

4.1. Moduł musi mieć możliwość zmiany nazwy. Nazwę „**Kontakty / struktura organizacyjna**" Wykonawca potraktuje roboczo.

4.2. Moduł musi posiadać co najmniej dwie wersje: skróconą wersję wizytówek, wizytówkę pełną.

4.3. Moduł umożliwia proste przełączenie między wersją skróconą a wersjami pełnymi wizytówek.

4.4. **Skrócona wersja wizytówki** musi zawierać rekordy ułożone domyślnie w kolejności alfabetycznej zawierające określone przez Zamawiającego elementy, co najmniej: zdjęcie pracownika (lub zamarkowane domyślnie miejsce z przykładową grafiką oznaczającą miejsce na zdjęcie), nazwisko, imię, nazwę jednostki, stanowisko I komórka organizacyjna.

4.4.1. Administrator główny ma możliwość dostosować widok skróconej wersji wizytówek w obrębie elementów zawartych w pełnej wersji wizytówek.

4.4.2. Moduł umożliwia użytkownikom sortowanie rekordów skróconej wersji wizytówki po dowolnym parametrze, którym opisywany jest rekord pracownika.

4.5. **Wersja pełna wizytówki** musi zawierać co najmniej następujące elementy:

4.5.1. zdjęcie pracownika – zdjęcie pracownika bądź zamarkowane miejsce na to zdjęcie; pracownik, który jest zalogowany, musi mieć możliwość poprzez przycisk DODAJ/ZMIEŃ ZDJĘCIE, dodać plik ze zdjęciem; usunąć zdjęcie mogą wyznaczeni administratorzy;

4.5.1.1. Moduł musi mieć możliwość ustawienia zatwierdzania przez administratora wydziałowego wgranego zdjęcia przed publikacją;

4.5.1.2. Miniatura zdjęcia wgranego poprzez pełną wersję wizytówki jest udostępniona w innych modułach: Wizytówka wydziałowa oraz Narzędzie wspierania pracy grupowej w projektach;

4.5.1.3. Wykonawca w porozumieniu z Zamawiającym określi formaty i maksymalną wielkość plików;

4.5.2. Nazwa jednostki – domyślnie Generalna Dyrekcja Ochrony Środowiska; powinna być zachowana możliwość edycji tego pola;

4.5.3. Imię/imiona;

4.5.4. Nazwisko;

4.5.5.Stanowisko;

4.5.6. Referat i wydział – link do wyszukiwania innych pracowników w referacie i wydziale;

4.5.7. Siedziba – czyli adres siedziby, gdzie pracuje dana osoba;

4.5.8. Pokój – czyli nr pokoju, w którym pracuje dana osoba;

4.5.9. Telefon komórkowy (nr telefonu);

4.5.10. Telefon stacjonarny (nr telefonu);

4.5.11. Adres e-mail – link, po naciśnięciu którego użytkownik zostanie przekierowany do pisania nowego e-maila z domyślnie wypełnionym polem adresata;

4.5.12. Bezpośredni przełożony – link do wizytówki pracowniczej przełożonego;

4.5.13. Wersja pełna wizytówki musi mieć możliwość dodania i zdefiniowania kolejnych pól wizytówki przez administratora głównego.

4.6. Treść wyświetlana w module musi być dostępna dla wszystkich zalogowanych użytkowników.

4.6.1. Po kliknięciu np. w przycisk WYDZIAŁY (nazwa robocza) powinna pojawić się struktura Generalnej Dyrekcji Ochrony Środowiska (lub rozwinąć się jako lista z odnośnikami do poszczególnych wydziałów). Po kliknięciu w nazwę danego wydziału powinna pojawić się publiczna część wizytówki wydziału. Zalogowani pracownicy przypisani do danego wydziału mają wgląd w pełną wersję wizytówki.

4.7. Moduł musi umożliwiać edycję treści w poniższych zakresach:

4.7.1. Administrator główny – edycja dowolnej treści,

4.7.2. Administrator wydziałowy oraz opiekun merytoryczny – edycja wizytówek pracowników przypisanych do danego wydziału,

4.7.3. Użytkownik – możliwość dodania i zmiany zdjęcia w swojej wizytówce.

4.7.3.1. Wykonawca musi określić parametry, jakie powinien spełniać wgrany plik, aby wyświetlał się poprawnie na stronach modułów.

5. Inne moduły

5.1. Moduły opisane poniżej zostaną zaprojektowane w oparciu o moduły z obecnego Intranetu GDOŚ:

5.1.1. Aktualności - moduł wykorzystywany w celu publikacji aktualnych informacji. Moduł publikuje treści w następujących odsłonach: widok pierwszy to skrót informacji wraz z fotografią; widok drugi to pełna treść informacji wraz z pozostałymi zdjęciami, plikami, tabelami itp.;

5.1.2. Komunikaty - komunikaty jako artykuły publikowane w aktualnościach,

5.1.3. Mapa intranetu - moduł służący do generowania na bieżąco mapy całego serwisu intranetowego. Przy aktualizacjach działów moduł automatycznie dodaje/usuwa/modyfikuje kolejne elementy do struktury strony zobrazowanej na mapie strony.

5.1.4. Struktura organizacyjna zintegrowana z książką adresową -możliwość graficznego przedstawianie struktury; wykorzystanie tej funkcji jako „książki adresowej” zawierającej kluczowe informacje o pracownikach;

5.1.5. Wyszukiwarka -dodanie mechanizmów umożliwiających wyszukiwanie pracowników po różnego rodzaju atrybutach;

5.1.6. Pliki do pobrania - repozytorium plików (formularze, wnioski) w podziale na kategorie, możliwość hierarchizowania grup dokumentów oraz pobieranie plików.

5.2. Wymagana jest migracja danych z obecnego Intranetu GDOŚ, w zakresie modułów:

5.2.1. Biblioteka i materiały do pobrania,

5.2.2. Zarządzenia Generalnego Dyrektora Ochrony Środowiska,

5.2.3. Zarządzenia Generalnego Dyrektora Ochrony Środowiska - Zamówienia publiczne,

5.2.4. Zarządzenia Dyrektora Generalnego GDOŚ,

5.2.5. Zarządzenia Dyrektora Generalnego GDOŚ - Zamówienia publiczne,

5.2.6. Kontrola zarządcza,

5.2.7. Bezpieczeństwo Informacji i Ochrona Informacji Niejawnych,

5.2.8. Ochrona danych osobowych,

5.2.9. Inspektor Ochrony Danych,

5.2.10. BHP/PPOŻ,

5.2.11. Zamówienia Publiczne.

5.3. Pozostałe moduły, przedstawione poniżej, zostaną dopracowane przy zapewnionych konsultacjach z Zamawiającym:

5.3.1. Komunikator / Chat:

5.3.1.1. Moduł typu messenger – umożliwia korespondencję pisemną oraz wymianę plików (do 5 Mb),

5.3.1.2. Moduł umożliwia tworzenie grup tematycznych,

5.3.1.3. Moduł umożliwia identyfikację zalogowanych użytkowników poprzez odpowiednie oznaczenie zalogowanego (aktywnego) użytkownika,

5.3.1.4. Moduł jest zintegrowany z modułem “wizytówki” – wyświetla zdjęcie użytkownika, umożliwia szybkie przejście z profilu użytkownika komunikatora do jego wizytówki.

5.3.2. Galeria zdjęć:

5.3.2.1. Moduł umożliwia administratorom każdego poziomu dodawanie zdjęć do zbioru głównego,

5.3.2.2. Moduł umożliwia tworzenie galerii tematycznych (podział np. ze względu na strukturę organizacyjną GDOŚ lub tematykę zdjęć),

5.3.2.3. Główna galeria wyposażona jest w tryb pokazu slajdów (włączony domyślnie),

5.3.2.4. Moduł umożliwia opisanie każdego zdjęcia: temat, autor zdjęcia, czas zrobienia zdjęcia (miesiąc, rok), miejsce zrobienia zdjęcia, osoba publikująca zdjęcie.

5.3.3. Baza przydatnych linków:

5.3.3.1. Linki stanowić będą aktywne odnośniki graficzne w formie ikon lub banerów po kliknięciu, w które nastąpi przekierowanie użytkownika do dedykowanej treści (np. na stronę ministerstwa).

6. Zasady bezpieczeńswa

6.1. System musi zapisywać historię logowania z uwzględnieniem co najmniej następujących parametrów: użytkownik, czas logowania, status powodzenia logowania.

6.2. System musi zapisywać historię zmian treści, z uwzględnieniem co najmniej następujących parametrów: użytkownik, czas zmiany, zmiany treści.

6.3. System musi automatycznie blokować konto użytkownika po określonej liczbie nieudanych prób logowania. Liczba nieudanych prób logowania powodująca blokadę konta musi być parametryzowana.

6.4. System musi umożliwiać definiowanie zakresów IP, z których możliwy jest dostęp do panelu administracyjnego.

6.5. System musi posiadać funkcję automatycznego wylogowania użytkownika po określonym okresie bezczynności. Czas bezczynności powodujący automatyczne wylogowanie użytkownika musi być parametryzowany.

6.6. System musi przechowywać hasła w sposób zaszyfrowany z zastosowaniem jednego z algorytmów: SHA2 lub BCRYPT.

6.7. System musi umożliwiać bezpieczne połączenie zdalnych użytkowników z użyciem protokołu TLS 1.2.

6.8. System musi posiadać możliwość rejestracji następujących informacji: historia operacji, logi transakcji oraz historia dostępu do aplikacji i danych dla wybranych ról.

6.9. System musi mieć mechanizm automatycznego prowadzenia dziennika systemu.

6.10. System musi umożliwiać pełną rozliczalność działań prowadzonych przez użytkowników w Intranecie. Musi w tym celu zapewnić administratorowi wgląd do rejestru co najmniej następujących zdarzeń: udane i nieudane logowanie, wszystkie operacje na artykułach i stronach (dodanie, edycja, usunięcie), wszystkie operacje na dokumentach (dodanie, edycja, usunięcie). System musi posiadać funkcję wersjonowania artykułów i dokumentów oraz przechowywać informacje, kto i kiedy dokonał modyfikacji danego elementu.

16.11. System musi posiadać skuteczne rozwiązania w zakresie bezpieczeństwa danych i tworzenia kopii bezpieczeństwa oraz sterowania uprawnieniami poszczególnych użytkowników w zakresie dostępu do danych, konkretnych ekranów I opcji. System musi zapewnić przypisanie uprawnień do poszczególnych funkcjonalności do użytkownika oraz grup użytkowników. Dodatkowo w przypadku dostępu do danych system musi zapewnić różne typy dostępu (wprowadzanie, podgląd i akceptację).

6.12. System musi zapewniać mechanizm zarządzania transakcjami gwarantujący integralność i spójność danych.

6.13. System musi zawierać mechanizm(y) automatycznego wykrywania zdarzeń niepożądanych, w szczególności takich jak:

6.13.1. Anomalie protokołów,

6.13.2. Anomalie ruchu,

6.13.3. Ataki typu backdoor,

6.13.4. Ataki DoS, DDoS,

6.13.5. Ataki typu IP Spoofing,

6.14. System musi być odporny na znane metody uzyskania nieautoryzowanego dostępu, w tym:

6.14.1. Ataki semantyczne na adres URL,

6.14.2. Ataki związane z ładowaniem plików,

6.14.3. Ataki typu cross-sitescripting,

6.14.4. Ataki typu CSRF,

6.14.5. Podrabianie zatwierdzenia formularza,

6.14.6. Sfałszowanie żądania HTTP,

6.14.7. Ujawnienie uwierzytelnień dostępu,

6.14.8. Wstrzykiwanie kodu SQL,

6.14.9. Ujawnienie danych przechowywanych w bazie,

6.14.10. Kradzież cookies,

6.14.11. Przechwytywanie sesji,

6.14.12. Wstrzykiwanie sesji,

6.14.13. Zafiksowanie sesji,

6.14.14. Trawersowanie katalogów,

6.14.15. Wstrzykiwanie poleceń Intranetu,

6.14.16. Ujawnianie kodu źródłowego, np. plików.inc, „template”, itp.

6.15. System musi zapewniać możliwość audytowania wszystkich prób dostania się do Intranetu w logach. Log musi zawierać co najmniej następujące informacje: opis zdarzenia (próby udane i nieudane), nazwa użytkownika, nazwa hosta, data zdarzenia, godzina zdarzenia.

6.16. System musi zapewniać rejestrowanie stanów niesprawności Intranetu i ich przyczyn w logach. Log musi zawierać co najmniej następujące informacje: data i godzina zdarzenia, identyfikator błędu, opis błędu itp.

6.17. System musi zawierać mechanizmy parametryzowania czasu przechowywania plików logów wraz z mechanizmem archiwizowania tych plików.

6.18. System musi zawierać mechanizmy uniemożliwiające nieuprawnionym użytkownikom edycję i usuwanie plików logów oraz mechanizmy chroniące przed przepełnieniem.

6.19. System musi posiadać możliwość dostosowania stron błędów (np. 404).

6.20. System musi uniemożliwiać dostęp do funkcji i zgromadzonych w nim danych z pominięciem mechanizmów bezpieczeństwa.

6.21. Wykonawca zobowiązany jest do wprowadzenia poprawek i aktualizacji w mechanizmach bezpieczeństwa Systemu w przypadku pojawienia się nieznanych wcześniej technik włamań, w taki sposób, aby zapewnić jego maksymalne bezpieczeństwo w ramach świadczonej pomocy technicznej.

6.22. System musi posiadać funkcję walidacji wszelkich danych wprowadzanych do systemu w celu zminimalizowania ryzyka naruszenia integralności systemu bądź danych.

6.23. Warstwa kodowa Systemu musi być jawna i dostarczona w takiej postaci, aby Zamawiający mógł w pełni prześledzić ich działanie, bez użycia mechanizmów szyfrujących (np. ioncube).

6.24. Dostęp do systemu musi odbywać się za pomocą bezpiecznego połączenia SSL z kluczem o długości co najmniej 128 bitów dla wszystkich administratorów i redaktorów serwisu.

6.25. System musi zawierać mechanizm uniemożliwiający kilkukrotne jednoczesne logowanie się tego samego użytkownika.

6.26. System musi zawierać mechanizm automatycznego tworzenia kopii bezpieczeństwa wszystkich elementów składających się na serwis (baza danych, aplikacje, pliki). Częstotliwość tworzenia kopii bezpieczeństwa musi być określana parametrem poprzez panel administratora.

6.27. System musi dawać możliwość ustalenia przez administratora miejsca, gdzie zapisywane będą kopie bezpieczeństwa. Możliwe musi być zapisywanie kopii bezpieczeństwa na innym serwerze.

6.28. System musi umożliwiać przeszukiwanie oraz filtrowanie historii i logów co najmniej takich atrybutów jak: data i czas operacji z dokładnością do minuty, nazwa użytkownika, rodzaj operacji, miejsce wykonania operacji lub nazwa pliku, na którym wykonano operację.

6.29. System musi raportować administratorowi wszelkie błędy w działaniu systemu CMS, w tym także kody błędów HTTP (np. 404).

6.30. Generowane przez system kody błędów muszą być prawidłowo rozpoznawane przez obsługiwane wyszukiwarki internetowe.

7. Wymagania związane z infrastrukturą

7.1. Generalna Dyrekcja Ochrony Środowiska zapewnia i dostarcza:

7.1.1. Serwer wirtualny oparty na środowisku Vmware o z góry ustalonych parametrach, to jest: CPU max. 8 VC, RAM max. 32 GB,

7.1.2. Niezbędne zasoby dyskowe o z góry ustalonej wielkości maksymalnie 1 TB,

7.1.3. Codzienną kopię zapasową całej maszyny wirtualnej o retencji max. 14 dni,

7.1.4. Wykonawca otrzyma zdalny dostęp do konsoli administracyjnej systemu operacyjnego na z góry ustalonych zasadach zgodnych z polityką bezpieczeństwa Urzędu.

7.2. Wykonawca zrealizuje:

7.2.1. Konfigurację systemu operacyjnego na wskazanym serwerze,

7.2.2. Instalację i konfigurację aplikacji,

7.2.3. Wdrożenie aplikacji i uruchomienie funkcjonalności, jakich oczekujemy,

7.2.4. Wykonawca dostarcza prawa licencyjne dla nas dla wdrożonych produktów.

7.3. Wykonawca jest odpowiedzialny za zachowanie sprawności i ciągłości działania wdrożonego środowiska na poziomie określonego SLA w zakresie:

7.3.1. Aplikacji Intranetu,

7.3.2. Innych elementów składowych aplikacji Intranetu.

8. Szkolenia

8.1. W ramach wdrożenia zostaną przeprowadzone w języku polskim następujące rodzaje Szkoleń:

8.1.1. Administracyjne – obejmujące m.in. ogólne działanie systemu, zarządzanie systemem, opisujące wszystkie funkcjonalności systemu, opisujące czynności okresowe związanych z administracją systemu (np. wgrywanie poprawek do systemu), procedury postępowania w przypadkach wystąpienia nieprawidłowości w działaniu systemu, najczęściej występujące zagadnienia i sposoby ich rozwiązywania,

8.1.2. Funkcjonalne – obejmujące m.in. funkcjonalności standardowe systemu Intranetu w ramach poszczególnych modułów.

8.2. Liczba osób objętych Szkoleniami:

8.2.1. Administrator główny – 3 osoby,

8.2.2. Administrator wydziałowy – około 20 osób,

8.2.3. Administrator IT – 3 osoby.

8.3. Wszystkie Szkolenia zostaną przeprowadzone w formie tradycyjnej, tzn. z wykorzystaniem systemu Intranetu (docelowe środowisko testowo-szkoleniowe) i oddzielnych stanowisk dostępowych dla każdego z uczestników w siedzibie Zamawiającego.

8.4. Formuła Szkolenia w formie „e-learning” dopuszczalna jedynie, jako uzupełnienie Szkolenia w formie warsztatów.

8.5. Liczba uczestników każdego pojedynczego Szkolenia nie przekroczy 10 osób.

8.6. Wykonawca dostarczy dla każdego uczestnika Szkolenia materiały szkoleniowe w języku polskim w postaci elektronicznej (w postaci plików utworzonych w popularnych formatach – doc, pdf), tj. podręcznika lub skryptu spójnego z zakresem i przebiegiem Szkolenia (wykład, ćwiczenia i miejsce na notatki).

8.7. Szczegółowy plan, zakres oraz terminy każdego Szkolenia zostaną uzgodnione przez Wykonawcę z Zamawiającym.

8.8. Użytkownicy zostaną przeszkoleni wewnętrznie przez Zamawiającego. Wykonawca zapewni pomoc w przygotowaniu Szkolenia, a w szczególności w opracowaniu materiałów szkoleniowych, programu i scenariuszów szkoleniowych, a także konfiguracji modułów i danych szkoleniowych.

9. Pozostałe wymagania techniczne

9.1. Intranet dostosowany do ustawy o dostępności cyfrowej stron internetowych i aplikacji mobilnych" (WCAG 2.1.) i zgodny z aktualnie obowiązującymi wymaganiami i standardami dla serwisów w administracji rządowej.

9.2. Narzędzia użyte w systemie muszą być oparte na usługach i oprogramowaniu open source.

9.3. Narzędzie nie może wymuszać kontynuacji wsparcia od dostawcy oprogramowania.

9.4. Wymagane jest przekazanie pełnego kodu źródłowego. Przeniesienie pełni praw (poza dalszą dystrybucją) na Zamawiającego.

9.5. Zapewnienie wysokiego poziomu bezpieczeństwa przetwarzania danych w trakcie uruchamiania i użytkowania oprogramowania.

9.6. Możliwość integracji użytkowników (obu środowisk: produkcyjnego i testowo–szkoleniowego) z AD jak również dopisywanie ich spoza AD.

9.7. Logowanie do intranetu za pomocą SSO lub alternatywnie.

10. Gwarancja, wsparcie i prace rozwojowe

10.1. W ramach gwarancji Wykonawca zobowiązuje się do nieodpłatnej:

10.1.1. analizy wykrytych usterek, błędów i błędów krytycznych; usuwania przyczyn oraz skutków wykrytych usterek, błędów i błędów krytycznych;

10.1.2. dokonywania aktualizacji zmian (po uzyskaniu zgody Zamawiającego) oraz zapewnienia prawidłowego działania Strony, a także związanych z tym aktualizacji dostarczonej dokumentacji i kodów źródłowych;

10.1.3. zgłoszenia usterek, błędów i błędów krytycznych przyjmowane będą przez Wykonawcę pod podanym w umowie numerem faksu lub adresem e-mail;

10.1.4. czas reakcji na zgłoszenie usterki, błędu lub błedu krytycznego nie może być dłuższy niż 4 godziny (brak reakcji Wykonawcy we wskazanym czasie oznacza automatycznie

rozpoczęcie - po upływie 4 godzin od wysłania zgłoszenia przez Zamawiającego - biegu terminu skutecznej naprawy);

10.1.5. przyjęcie zgłoszenia musi zostać potwierdzone przez Wykonawcę faksem lub e-mailem. Wykonawca niezwłocznie po przyjęciu zgłoszenia przystąpi do analizy zaistniałej sytuacji i podejmie działania zmierzające do usunięcia zgłoszonych nieprawidłowości;

10.1.6. termin skutecznej naprawy błędu to 2 dni robocze od momentu potwierdzenia przyjęcia zgłoszenia błędu (lub po upływie 4 godzin od wysłania zgłoszenia przez Zamawiającego –w przypadku kiedy Wykonawca przekaże z opóźnieniem potwierdzenie przyjęcia zgłoszenia). Wykonawca udzieli Zamawiającemu 12-miesięcznego wsparcia polegającego na świadczeniu pomocy administratorom/redaktorom strony, rozumianego jako: konsultacje dotyczące funkcjonowania, analiza problemów zgłaszanych przez administratorów/redaktorów strony oraz asysta przy ich rozwiązywaniu.

10.2. Wsparcie świadczone będzie w dni robocze, w godzinach 8.00-16.00.

10.3. Wykonawca w ramach usługi wsparcia wykona prace rozwojowe dodatkowo płatne, na podstawie zaakceptowanego kosztorysu. W zakres prac rozwojowych wchodzą projektowanie, wykonywanie i wdrażanie nowych funkcjonalności; dostosowanie strony intranetowej do zmian aktów prawnych, mających wpływ na dostarczony serwis i realizowane przez niego funkcjonalności; projektowanie i wykonywanie grafik itp.

10.4. Zlecanie prac rozwojowych odbywa się zgodnie z następującą procedurą:

10.4.1. Zamawiający przekaże Wykonawcy e-mailem lub faksem prośbę o oszacowanie czasochłonności prac rozwojowych, zawierającą opis produktu zlecanych prac rozwojowych;

10.4.2. Wykonawca niezwłocznie, nie później jednak niż w terminie 3 dni roboczych od otrzymania prośby, przedstawi Zamawiającemu e-mailem lub faksem oszacowanie czasochłonności prac rozwojowych wraz z ich harmonogramem i kosztorysem.

10.4.2. Po akceptacji oszacowania przez Zamawiającego, rozumianej jako zlecenie wykonania prac rozwojowych, Wykonawca niezwłocznie przystąpi do wykonania prac rozwojowych, nie później jednak niż w ciągu 3 dni roboczych, chyba że Strony e-mailem lub faksem ustalą inny termin.

10.5 Wykonawca po wykonaniu prac rozwojowych niezwłocznie, nie później jednak niż w momencie upływu roboczogodzin wskazanych w oszacowaniu, przekaże produkt do akceptacji Zamawiającego.

10.6 Zamawiający niezwłocznie, nie później jednak niż w terminie 3 dni roboczych, zaakceptuje produkt prac rozwojowych lub zgłosi Wykonawcy swoje do niego zastrzeżenia wynikające z rozbieżności między przekazanym przez Wykonawcę produktem a opisem produktu podanym w prośbie, o której mowa w pkt 10.5.

10.7 W przypadku zgłoszenia zastrzeżeń Wykonawca niezwłocznie poprawi produkt, po czym przekaże go Zamawiającemu do akceptacji. Wprowadzanie poprawek przez Wykonawcę wlicza się w sumę roboczogodzin przedstawionych w zaakceptowanym oszacowaniu, tzn. podlega wynagrodzeniu. Jeśli wprowadzanie poprawek przekracza sumę roboczogodzin przedstawionych w zaakceptowanym oszacowaniu, Wykonawca wprowadza je na własny

koszt, tzn. nadliczbowe roboczogodziny nie podlegają wynagrodzeniu.

10.8 Odbiór produktu prac rozwojowych następuje po jego akceptacji przez Zamawiającego, wdrożeniu oraz przekazaniu zaktualizowanej dokumentacji (w tym głównie: instrukcji obsługi, procedury wykonywania kopii środowisk, procedury odtwarzania po awarii) i kodów źródłowych.