Szczegółowy opis przedmiotu zamówienia

I. Tytuł zamówienia

Zaprojektowanie, wykonanie, wdrożenie i uruchomienie Portalu Intranetowego w środowisku Zamawiającego z wykorzystaniem subskrypcji MS Office 365 (MS SharePoint online) wraz z przeszkoleniem pracowników z Portalu Intranetowego

II. Sposób realizacji zamówienia

Zamówienie będzie realizowane etapowo, przy czym etapy mogą być realizowane równolegle. Realizacja będzie dokonywana poprzez sesje zdalne, każda sesja będzie monitorowana poprzez system PAM zamawiającego, sesje poza PAM będą zablokowane. W ramach każdego etapu przewidziana jest realizacja następujących zadań:

Etap I: Zaprojektowanie architektury graficznej Intranetu Grupy NCBR

Wykonawca przedstawi projekt schematu/mapy oraz szaty graficznej Intranetu Grupy NCBR zgodnej z logotypem i księgą identyfikacji wizualnej Grupy NCBR. Wykonawca przedstawi przynajmniej trzy alternatywne oferty szaty graficznej, z których zostanie wybrana jedna z możliwością modyfikacji w trakcie wdrożenia zgodnie z potrzebami Zamawiającego. Księga identyfikacji wizualnej Grupy NCBR zostanie przekazana Wykonawcy w dniu zawarcia Umowy.

Etap II: Wdrożenie Intranetu w środowisku informatycznym Zamawiającego

Uruchomienie i wdrożenie Portalu Intranetowego Grupy NCBR w środowisku Zamawiającego (chmura O365) wraz z wymaganymi funkcjonalnościami w wersji produkcyjnej. Portal będzie wykorzystywany na wewnętrzne potrzeby Zamawiającego przez maksymalnie 1000 użytkowników.

Etap III: Przeszkolenie redaktorów lokalnych oraz administratorów

W ramach szkoleń Wykonawca będzie zobowiązany do przeszkolenia wskazanych przez Zamawiającego redaktorów lokalnych oraz administratorów Portalu Intranetowego w liczbie nie przekraczającej 10 osób, oraz przygotowania materiałów szkoleniowych. Szkolenia odbędą się w formie online za pośrednictwem usługi MS Teams. Zamawiający zastrzega sobie możliwość nagrania szkoleń.
Łączny czas na realizację wszystkich etapów nie może przekroczyć okresu realizacji wskazanego w Umowie.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

III. Główne funkcjonalności Intranetu Grupy NCBR

1. **Biuletyn/Aktualności** – szybkie opublikowanie informacji wewnętrznej – aktualności dzienne w podziale na komunikaty tematyczne wraz z możliwościami wyszukiwania poszczególnych komunikatów. Treść komunikatów podzielona na skrót tekstu (lead), tytuł, temat, tekst główny oraz zdjęcie. Zapewnienie możliwości korzystania z gotowych szablonów określających strukturę wiadomości tj. umiejscowienie obrazka i tekstu. W treści aktualności musi być możliwość dodania artykułu na określony czas i automatyczne wygaszenie go po upływie określonego terminu. Możliwość formatowania tekstu (boldowanie, kursywa, podkreślenie, zmiana koloru czcionki, linkowania, przypisy itp.) bez konieczności znajomości języków programowania dzięki zastosowanemu Edytorowi HTML - edytor WYSIWYG (What You See is What You Get), oraz możliwość dodawania tabel (możliwość wklejania z Excela lub Worda), rysunków, filmów i zdjęć (z możliwością kadrowania i skalowania) do treści informacji. Portal musi umożliwiać ustawienie daty startu oraz zakończenia publikacji.

2. **Struktura Organizacyjna Grupy NCBR** - moduł pozwala: wizualizować strukturę organizacyjną Grupy NCBR w formie drzewa – Zamawiający wymaga, aby struktura była w pełni zintegrowana z Active Directory; szybko wyszukiwać pracowników według imienia, nazwiska; moduł pozwala na podgląd danych pracownika poprzez kliknięcie na daną osobę.
   Informacje o przynależności danego użytkownika do działu oraz sekcji są dostępne w AD.

3. **Książka adresowa** - moduł dotyczący pracowników, zawierający dane:

a. Imię i nazwisko
b. Stanowisko
c. Telefon stacjonarny, telefon komórkowy
d. Adres email
e. Miejsce w strukturze organizacyjnej – jednostka/departament/centrum/zespół, bezpośredni przełożony
f. Nr pokoju
g. Zdjęcie (wizerunku).

Zamawiający wymaga, aby książka adresowa miała możliwość wyszukiwania po imieniu i nazwisku.
Wszystkie wskazane powyżej dane znajdujące się w AD Zamawiającego.

4. **Fora wewnętrzne/dyskusyjne** - pozwalające na wymianę informacji pomiędzy pracownikami organizacji. Moduł pozwala: prowadzić dyskusje między pracownikami; wymieniać wiedzę i doświadczenia pomiędzy pracownikami; archiwizować dyskusje i dodać je do firmowej bazy wiedzy; w prosty sposób komunikować ze sobą pracowników; administrować forum dzięki narzędziom umożliwiającym: edycję, wycinanie/wklejanie, usuwanie dyskusji i postów. Moduł zapewnia również wyświetlenie powiadomienia z czatów o nadejściu wiadomości. Portal musi umożliwiać użytkownikom tworzenie grup otwartych lub zamkniętych:

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

a. Portal musi umożliwiać użytkownikom tworzenie grup zamkniętych, która ma swoją nazwę, zdjęcie w nagłówku, opis społeczności, lokalizację, dodatkowych właścicieli społeczności, możliwość ustawienia społeczności jako obowiązkowej, dodania członków społeczności, dołączenia do społeczności poprzez akceptację właściciela, widoczność tylko dla członków którzy są dodawani lub zapraszani przez właściciela grupy.
b. Portal musi umożliwiać użytkownikom tworzenie grup otwartych, która ma swoją nazwę, zdjęcie w nagłówku, opis społeczności, lokalizację, dodatkowych właścicieli społeczności, możliwość ustawienia społeczności jako obowiązkowej, dodania członków społeczności, ustawienia limitu członków społeczności, dołączenia do społeczności poprzez akceptację właściciela.

Portal musi posiadać mechanizm Newsfeed, który jest elementem społecznościowym na wzór tablicy (walli) z Linkedln. Wpisy do newsfeeda dodawane będą przez użytkowników (Czytelników) wykorzystując uproszczony edytor tekstowy. W tekście można zawrzeć tagi (stawiając przed wyrazem znak „#') oraz wskazywać osoby (@mentions) i dołączać pliki. Dla linków URL wpisy muszą wyświetlać podgląd, a dla plików graficznych wyświetlać grafikę po publikacji. Portal umożliwia dodawanie komentarzy pod każdym typem wpisów. Użytkownik może wspominać (@) innych użytkowników lub dodawać hasztagi (#)

5. **Repozytorium dokumentów** (wzory dokumentów wewnętrznych, wychodzących). Wszystkie dokumenty w module uporządkowane są według drzewa kategorii, które można dowolnie rozbudowywać i modyfikować. Moduł pozwalający efektywnie zarządzać dokumentami dzięki:

a) zamieszczaniu w Portalu plików z podziałem na kategorie i podkategorie;
b) możliwość dodawania plików: DOCX, PDF, XLSX, MPEG, PNG, JPG, MP4, PPTX.
c) dodawaniu załączników do dokumentów (DOCX, PDF, XLSX, MPEG, JPEG, PPTX, pliki audio/wideo, itd.);
d) możliwości wspólnej pracy nad dokumentem (dostępność dokumentu dla osób zaangażowanych w pracę nad nim);
e) historii zmian wraz z danymi osób ich dokonujących;
f) możliwości określenia prawa dostępu do poszczególnych materiałów dla określonych grup użytkowników;
g) zebraniu wszystkich materiałów i dokumentów tematycznych w jednej bazie;
h) wyszukiwaniu dokumentów wraz z załącznikami i innymi powiązanymi dokumentami przy użyciu zdefiniowanych filtrów (w tym wyszukiwanie z treści);
i) możliwości określania parametrów publikacji: data publikacji od-do, wersja robocza i zaakceptowana;
j) możliwości formatowania tekstu (hołdowanie, kursywa, podkreślenie, zmiana koloru czcionki, itp.) bez konieczności znajomości języków programowania dzięki zastosowanemu Edytorowi HTML;
k) możliwości wersjonowania dokumentów - każda modyfikacja dokumentu tworzy nową wersję z możliwością przywrócenia starej, dostępność śledzenia zmian w dokumencie oraz dodawania komentarzy;
l) możliwość dodawania metadanych do plików podczas ewidencjonowania ich w repozytorium.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

6. **Kalendarz** - moduł pozwalający zorganizować czas przez użytkowników, w tym: dodawać wydarzenia służbowe i firmowe; dodawać różne typy wydarzeń (spotkanie, rocznica, wyjazd, delegacja, szkolenia, itd.); przeglądać wydarzenia w widoku: dziennym, tygodniowym, miesięcznym; przeglądać wydarzenia z wybranego dnia dzięki opcji „Idź do daty"; dodawać wydarzenia dostępne dla wybranych pracowników lub grup pracowników; Moduł musi mieć możliwość synchronizacji z kalendarzem funkcjonującym w ramach poczty elektronicznej (outlook).

7. **Statystyki** - monitorowanie aktywności użytkowników Intranetu w sposób zagregowany. Moduł pozwala: monitorować czas spędzany przez użytkowników i aktywność w Intranecie; monitorować aktywność w poszczególnych działach intranetu; wyświetlać statystyki czytania i pobierania zamieszczanych treści i dokumentów; wyświetlać statystyki czytania biuletynu; tworzyć statystyki korzystania z Intranetu z możliwością generowania raportu i wydruku.

8. **Sondy, ankiety** - moduł do tworzenia ankiet na dowolny temat, pozwalający: budować dowolne sondy i ankiety, nieograniczone ilością i rodzaje pytań (testowe, otwarte, itp.) oraz liczbą odpowiedzi; określać parametry publikacji takie jak data od-do, temat, itp.; badać preferencje użytkowników; zbierać wiedzę o użytkownikach; archiwizować ankiety przeprowadzone w przeszłości; tworzyć sondy graficzne; generować wyniki ankiet (doc. xls. pdf.), raporty, z możliwością wydruku. Możliwość publikacji ankiet anonimowych (bez wyświetlania danych osoby biorącej udział) oraz ankiet z zapisem danych uczestników. Możliwość tworzenia zależności między pytaniami (wyświetlania kolejnego pytania w zależności od odpowiedzi na wcześniejsze). Rozwiązanie musi bazować na integracji z Microsoft Forms.

9. **Tablica ogłoszeniowa (ogłoszenia prywatne)** umożliwiająca dodanie, usunięcie i edycję prostych ogłoszeń wyświetlanych w danej podstronie wraz z możliwością dodania zdjęcia i linków zewnętrznych. Każdy z pracowników musi mieć możliwość zgłoszenia do publikacji, natomiast wszystkie ogłoszenia muszą być akceptowane przez Administratora.

10. **Banery** - moduł umożliwi używać banerów pop-up lub webparta SharePoint Online (News).

11. **Pasek ważnych informacji** - możliwość dodawania linków wewnętrznych i zewnętrznych lub napisów na pasku na stronie głównej.

12. **Rotator aktualności** - możliwość ustawiania najważniejszych treści w rotatorze na stronie głównej.

13. **Agregatory treści** - możliwość agregowania różnych treści w jednym miejscu. Np. Najnowsze wydarzenia, najnowsze dokumenty.

14. **Stopka** - portal musi zawierać stopkę z linkami do social media NCBR.

15. **Prezentacja materiałów video** - portal musi integrować się z YouTube w celu dynamicznego osadzania wideo w intranecie z tego portalu.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

16. **Pole/kafelki z odnośnikami do ważnych stron/zasobów** jak np. EZD, Jira, Portal benefitowy

17. **Ulubione linki użytkownika** - element agregujący i wyświetlający linki do stron, dokumentów, artykułów, wpisów forum, itp. oznaczonych przez użytkowników. Treść strony musi być budowana dynamicznie w zależności od oznaczeń wykonanych przez użytkownika. Na stronie musi być możliwość wyszukiwania linków. Linki muszą być wyświetlane w sposób skategoryzowany.

18. **Wyszukiwarka treści** - zintegrowana wyszukiwarka przeszukująca zarówno strony treściowe jak i dokumenty, w tym wyszukiwanie pełno tekstowe w treści plików o formatach .pdf, .docx, .xlsx, .pptx. Wybrane części serwisu muszą mieć możliwości zaawansowanego wyszukiwania informacji, uwzględniające filtrowanie.

19. **Funkcje społecznościowe** - portal musi mieć możliwość włączania oraz wyłączania możliwości polubień oraz komentowania treści aktualności przez użytkowników.

20. **Podstrony treściowe** - zgodnie z opracowaną przez Zamawiającego mapą komunikacyjną Grupy NCBR, kategorie do szczegółowego potwierdzenia na etapie realizacji projektu. Jako kategorie możemy rozumieć:

- O Grupie NCBR - struktura, najważniejsze dokumenty itp.
- Sprawy organizacyjne - zakupy, zamówienia itp.
- Dla Pracownika - sprawy kadrowe, socjalne, szkolenia itp.

Maksymalna liczba podstron: 250

21. **Polityka prywatności/ regulamin korzystania z Intranetu** zawierający zasady przetwarzania danych osobowych, informacji chronionych i praw autorskich, w którym zapoznaje się każdy użytkownik przed rozpoczęciem korzystania. Zapoznanie się z polityką prywatności jest odnotowywane w systemie Zamawiającego z możliwością rozliczalności i zapisem historii wyrażonych/wycofanych zgód.

22. **On-boarding pracownika** - w sekcji on-boardingu użytkownik musi mieć możliwość kontaktowania się z osobą odpowiedzialną za konkretny obszar, zapoznania się z treścią on-boardingu (video, grafiki, pliki, linki), wypełnić ankietę lub formularz.

23. **Zmiana pracownicza** - portal musi posiadać możliwość publikowania informacji o zmianach na kluczowych stanowiskach w organizacji.

24. **Zgłoszenia nieaktualnych treści** - Użytkownik na każdej stronie/podstronie Intranetu musi mieć możliwość zgłoszenia nieaktualnych treści - poprzez przycisk ZGŁOŚ NIEAKTUALNĄ TREŚĆ musi otworzyć się formularz kontaktowy do wskazanego przez Zamawiającego adresu.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

IV. Opis funkcjonalny Systemu zarządzania treścią

Panel administracyjny Portalu musi umożliwiać publikację materiałów typu: aktualności na stronie głównej Intranetu czy tematycznych stron treściowych będących częścią Intranetu bez konieczności wiedzy technicznej i informatycznej, a w szczególności znajomości języka HTML. Dostęp do Portalu będą posiadać redaktorzy lokalni w poszczególnych komórkach organizacyjnych oraz administratorzy Portalu, którzy będą mieli możliwość nadawania odpowiednich uprawnień. Panel administracyjny ma się charakteryzować wysokim poziomem wygody oraz intuicyjności. Edytor do formatowania treści wraz z zaimplementowanym standardem jednolitego formatowania wszystkich stron (jedynie ograniczony WYSIWYG) przy jednoczesnej możliwości przenoszenia treści z aplikacji MS Office, HTML/XHTML, TXT. System musi umożliwiać realizację następujących funkcjonalności:

a) Możliwość podstawowych funkcji formatowania tekstu, takich jak wyrównywanie i pogrubienie czcionki, wielostopniowe punktowanie, dodanie obrazka w ramach tekstu, dodawania odnośników do plików i linków belki podziału treści, formatowanie nagłówków, dołączanie tabel, możliwość zamieszczania plików w dowolnych formatach i tagowanie poszczególnych stron (zatwierdzający, kto zamieścił, data zamieszczenia, data modyfikacji).
b) Możliwość zastosowania technologii drag and drop w celu ułatwienia zamieszczania poszczególnych elementów na stronie (zdjęć, plików, treści).
c) Możliwość korzystania z szablonów w trakcie definiowania stron tematycznych (różne rodzaje rozmieszczenia tekstów i obrazków).
d) Niewielkie wymagania techniczne (wszystkie funkcje są dostępne z poziomu przeglądarki internetowej).
e) System dostępny w chmurze po zalogowaniu oraz poprzez połączenie szyfrowane minimum TLS 1.2 dla wszystkich zdefiniowanych użytkowników.
f) Ustalona konwencja zamieszczania aktualności na stronie głównej Intranetu polegająca na podziale treści na lead, tekst aktualności i zdjęć z możliwością dodania załączników w formie plików.
g) Możliwość zamieszczania plików różnego typu, także graficznych, oraz łącz (linków). Portal automatycznie rozpozna typ pliku i doda odpowiednią ikonkę.
h) Spójne zarządzanie wyglądem stron, głównie pod kątem formatowania tekstu: globalne definiowanie jednego kroju tekstu dla całego serwisu bez możliwości jego modyfikacji przez redaktorów lokalnych (krój czcionki i kolor), możliwość wklejania treści przy publikacji stron z plików tekstowych lub edytorów tekstu (np. MS Word) wraz z usunięciem formatowania oryginalnego.
i) Automatyczne dołączanie do publikowanych stron internetowych informacji o dacie publikacji i autorze, o którym znajdzie się informacja zintegrowana z książką adresową serwisu (po kliknięciu autora pojawi się jego profil). Możliwość ustawienia jako autora nazwy działu lub zespołu.
j) Wersjonowanie treści stron działających automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści i możliwość przywracania wcześniejszych wersji.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

k) Możliwość generowania struktury poszczególnych stron serwisu wraz z możliwością dodawania i przenoszenia podstron w ramach różnych sekcji. Możliwość łatwego ukrywania stron treściowych także po ich zatwierdzeniu i opublikowaniu.

l) Automatyczne generowanie stron do wydruku.

m) Zarówno interfejs użytkownika jak i panel administratora musi być w języku polskim oraz posiadać polskojęzyczne komunikaty.

V. Nawigacja i konstrukcja Intranetu Grupy NCBR

Konstrukcja Intranetu Grupy NCBR musi mieć wyraźną i czytelną strukturę. Zamawiający zakłada, że:

a) strona główna Intranetu Grupy NCBR musi posiadać menu główne oraz menu zawierające strony jednostek organizacyjnych (jednostek, działów/biur);

b) strona główna Intranetu Grupy NCBR musi wyświetlać i umożliwiać dostęp do wszystkich elementów i funkcjonalności opisanych w pkt. III;

c) na wyświetlanej stronie musi pojawiać się informacja dotycząca lokalizacji aktualnie przeglądanej strony, wraz z możliwością przeniesienia się do każdego z wyższych poziomów;

d) Portal Intranetowy musi być zgodny z wytycznymi WCAG 2.1 (zgodnie z ustawą z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych), w zakresie oferowanym przez platformę Microsoft 365;

e) Portal Intranetowy musi umożliwiać utworzenie kolorystyki żałobnej oraz świątecznej (bożonarodzeniowej, wielkanocnej, świętowanie jubileuszu powstania) wraz z możliwością łatwego przełączania stron;

f) Intranet Grupy NCBR musi posiadać mechanizm zaawansowanego wyszukiwania treści zamieszczonych na platformie, a w szczególności wyszukiwać według dowolnych słów, słów kluczowych, wszystkich słów lub wyrażenia z możliwością późniejszego filtrowania wyników. Wyniki wyszukiwania muszą zawierać informacje o liczbie odnalezionych pasujących pozycji/rekordów oraz umożliwiać wyświetlanie w zależności od preferencji użytkownika: 10, 20, 50, 100 wyników na 1 stronie.

VI. Zarządzanie uprawnieniami

1. Portal musi umożliwiać definiowanie różnych poziomów dostępu dla administratorów oraz definiowanie zakresów dostępów do danych, którymi mogą zarządzać.
2. Portal musi umożliwiać definiowanie różnych poziomów dostępu dla redaktorów (opiekunów merytorycznych) oraz zakresy treści, którymi mogą zarządzać.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

3. Portal musi umożliwiać definiowanie różnych poziomów dostępu dla administratorów modułowych (administratorów departamentalnych) oraz określenia zakresu treści, którymi mogą zarządzać.
4. Portal musi posiadać funkcjonalność nadawania i kontroli uprawnień użytkownikom.
5. Portal 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.
6. Portal musi uwzględniać typy uprawnień:
    a. administrator biznesowy / główny - możliwie najszersze uprawnienia i dostęp do wszystkich publikowanych treści,
    b. redaktor witryny / administrator departamentalny - dostęp i administrowanie określonym zakresem treści - poszczególne części modułów departamentalnych,
    c. użytkownik - osoba korzystająca z Intranetu z uprawnieniami zgodnie z dopisanymi grupami.
7. Portal musi umożliwiać nadawanie takich samych uprawnień co do tego samego zakresu kilku administratorom.
8. Definiowanie i nadawanie uprawnień musi odbywać się z poziomu zaplecza administracyjnego systemu i być niezależne od Wykonawcy.

VII. Wymagania techniczne i bezpieczeństwa Portalu Intranetowego

1. Portal musi być zbudowany z wykorzystaniem technologii i narzędzi zapewniających: stabilność, wydajność, skalowalność oraz bezpieczeństwo. Zamawiający wymaga integracji posiadanego i wykorzystywanego przez Zamawiającego oprogramowania Office 365 E5 (Azure Active Directory, SharePoint online) z oferowanym rozwiązaniem (na przykład poprzez Graph API, SharePoint API, PowerApps, nie dopuszcza się interfejsów pośredniczących (np. Zapier) pomiędzy MSOffice, a oferowanym oprogramowaniem).

2. W przypadku integracji oferowanego oprogramowania poprzez interfejsy API oferowane przez Microsoft (np. Graph API) nie dopuszcza się, aby rozwiązanie wymagało uprawnień globalnego administratora do funkcjonowania.
3. Portal musi zapewnić ochronę treści w nim przechowywanych, w taki sposób, aby trwałe usunięcie treści możliwe było tylko przy użyciu konta z uprawnieniami administratora.
4. Wykonawca zapewni mechanizmy wykorzystywane do:
    a. Logowania użytkowników
    b. Tworzenia, blokowania i usuwania kont użytkowników
    c. Zarządzania uprawnieniami użytkowników i grup użytkowników
    d. Tworzenia i zarządzania profilami użytkowników
    e. Zarządzania strukturą organizacyjną.
    f. Wyżej wymienione mechanizmy muszą posiadać możliwość zastąpienia ich integracją z Active Directory Zamawiającego. Wykonawca zapewni integrację z Active Directory w zakresie automatycznego logowania, blokowania kont i aktualizacji danych o pracownikach. Wymagana jest

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

automatyczna aktualizacja danych na podstawie danych pobieranych z Active Directory (dopuszcza się wykorzystanie ww. mechanizmów w oparciu o platformę MS Office 365).

5. Mechanizm Single Sign-On (SSO) poprzez SAML i/lub OIDC.
6. Wykonawca zapewni możliwość zbiorczej aktualizacji danych w profilach użytkowników na podstawie danych z pliku xls/csv o ustalonej z Zamawiającym strukturze (z możliwością wygenerowania tych plików baz ze struktury organizacyjnej lub pracowników).
7. Pełna obsługa Portalu w języku polskim.
8. Portal musi być zbudowany z wykorzystaniem licencji posiadanych przez Zamawiającego.
9. Możliwość równoczesnej pracy do 1000 osób.
10. Kodowanie znaków zgodnie z - Unicode UTF-8 wersja w aktualnie najnowszej wersji.
11. Strony tworzące Intranet Grupy NCBR muszą być prawidłowo wyświetlane w takich przeglądarkach jak: Mozilla FireFox, Chrome, Microsoft Edge.
12. Strony muszą być responsywne - skalowalne w zależności od wielkości okna przeglądarki, w szczególności poniżej założonej szerokości okna zawartość strony musi być wyświetlana w układzie 1 kolumny.
13. Portal musi zapisywać historię zmian treści z uwzględnieniem co najmniej następujących parametrów: użytkownik, czas zmiany, zmiany treści.
14. Portal musi zapisywać historię logowania z uwzględnieniem co najmniej następujących parametrów: użytkownik, czas logowania, status powodzenia logowania.
15. Portal musi automatycznie blokować konto użytkownika po określonej liczbie nieudanych prób logowania. Liczba nieudanych prób logowania powodująca blokadę konta musi być parametryzowana.
16. Portal 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).
17. Portal musi raportować administratorowi wszelkie błędy w działaniu systemu CMS, w tym także kody błędów HTTP (np. 404).
18. Oprogramowanie musi być utrzymywane na infrastrukturze Zamawiającego (chmura prywatna). Zamawiający nie dopuszcza rozwiązań chmurowych takich jak SaaS/PaaS/IaaS.
    Jeśli oferowane rozwiązanie jest oparte o platformę SharePoint Online oraz nie jest hostowane poza tenantem O365 Zamawiającego jest to rozwiązanie akceptowalne.
19. Oprogramowanie nie może być licencjonowane per user.
20. Oprogramowanie musi być tworzone zgodnie z zaleceniami standardu OWASP-ASVS poziom 2 (Open Web Application Security Project)
21. Oprogramowanie musi być tworzone zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project)
22. W przypadku integracji oprogramowania z Office365 obiekty i pliki składowane w O365 i później transferowane/kopiowane do oferowanego oprogramowania muszą być traktowane jako udostępnione na zewnątrz celem wdrożenia odpowiednich polityk DLP w Office 365.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

23. W przypadku SSO z np. AD/AAD niedopuszczalne jest cacheowanie (zapisywanie) poświadczeń użytkownika w oprogramowaniu.
24. Transferowane pliki z Office365 oraz stacji roboczych Zamawiającego do oferowanego oprogramowania i na odwrót tj. z oferowanego oprogramowania do Office 365 i stacji roboczych muszą zachować wszystkie metadane i klasyfikatory nadane przez wykorzystywane przez Zamawiającego rozwiązania DLP (AIP oraz Safetica DLP).
25. Oprogramowanie musi umożliwiać nadawanie uprawnień obiektom (np. plikom, wiadomościom, artykułom itp.) publikowanym w oprogramowaniu celem ograniczenia dostępu do obiektów osobom/kontom nieuprawnionym.
26. Przechowywane przez Oprogramowanie dane identyfikujące oraz uwierzytelniające w zintegrowanych/powiązanych z Systemem aplikacjach muszą być zabezpieczone przed niepowołanym odczytaniem (np. poprzez szyfrowanie).
27. Oprogramowanie musi spełniać wytyczne przedstawione w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. (https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20120000526).
28. Oprogramowanie musi mieć zdolność korzystania z zewnętrznego systemu autoryzacji (potencjalnie dostarczonego w przyszłości przez Zamawiającego) wraz z funkcjonalnością SSO, na podstawie standardów wymienionych w pozostałych wymaganiach – np. SAML2, OIDC (ADFS / AzureAD).
29. Wykonawca musi udokumentować architekturę w zakresie integracji między systemami (jeśli takie wystąpią), procesy systemowe, diagramy sekwencji, instrukcje stanowiskowe, dokumentację wdrożeniową, dokumentację administracyjną, dokumentację środowisk testowych (jeśli takie wystąpią) oraz pozostałą dokumentację Rozwiązania (w szczególności wymagane przez aplikacje uprawnienia w AAD i interfejsach programistycznych oferowanych przez Microsoft).
30. Oprogramowanie powinno dostarczać mechanizmy związane z ochroną interfejsu WWW przed zakończeniem sesji oraz zewnętrznym dysponowaniem sesją Użytkownika (ataki typu „man in the middle").
31. Oprogramowanie musi w odpowiedni sposób weryfikować błędy tak aby użytkownikowi końcowemu nie była prezentowana informacja o błędzie, zawierająca szczegóły techniczne wystąpienia tego błędu, ujawniające zastosowanie oprogramowania i jego konfigurację. Powinien być generowany standardowy, niezmienny komunikat o błędzie.
32. Oprogramowanie musi w odpowiedni sposób weryfikować zawartość przesyłanych do systemu pól/formularzy aplikacji pod kątem wprowadzanych znaków (zastosowanej walidacji oraz kontroli poprawności składni zapytań), w celu zabezpieczenia przed atakami typu SQL Injection itd. Lokalne walidacje są elementem dodatkowym i nie powinny zastępować właściwego mechanizmu.
33. Oprogramowanie musi zapewniać możliwość określenia uprawnień użytkowników adekwatnie do pełnionych przez nich zadań zgodnie z zasadą minimalnych uprawnień.
34. System musi odrzucać połączenia, które pochodzą od niezautoryzowanych użytkowników oraz niedopuszczonych adresów IP i sieci.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

35. Struktura logów musi być udokumentowana pozwalając na prawidłowe korelowanie zdarzeń z systemem klasy SIEM.
36. Komunikacja z oprogramowaniem musi się odbywać z wykorzystaniem bezpiecznych protokołów tj. min. TLS 1.3 przy użyciu silnych algorytmów szyfrowania minimum AES 256 bits i długości klucza RSA 2048 bits. Zamawiający dopuszcza wersję TLS 1.2 pod warunkiem poddania protokołu utwardzaniu po stronie Wykonawcy (wymagane jest używanie szyfrów AES/GCM oraz ChaCha20-Poly130). Zapis ten dotyczy każdej komunikacji zarówno użytkownika jak i usług teleinformatycznych (poczta, usługi katalogowe itp. Itd.)
37. Dane przesyłane do i z oferowanego Oprogramowania muszą być przesyłane w sposób bezpieczny zapewniając przesyłanym danym integralność oraz poufność (np. poprzez szyfrowanie).
38. Oprogramowanie musi posiadać dokumentację powykonawczą opisującą wszystkie zastosowane mechanizmy bezpieczeństwa.
39. Wykonawca dostarczy Zamawiającemu dokumentację administratora bezpieczeństwa tj. Zestaw dokumentacji opisującej zastosowane rozwiązania dotyczące spełniania wymagań ogólnych (zgodnie z wymaganiami prawa) oraz specyficznych zamawiającego dotyczących bezpiecznej eksploatacji. Dokumentacja, w szczególności, powinna zawierać:
    a. opis zastosowanych mechanizmów ochrony przed naruszeniem zasad dostępu (poufności), integralności, niezaprzeczalności, wiarygodności oraz opis mechanizmów udostępniania, autoryzacji;
    b. opis zastosowanych mechanizmów logowania zdarzeń, śladu audytowego oraz kontroli i monitorowania działań w aplikacji/systemie w tym wszelkich prób naruszenia zasad bezpieczeństwa;
    c. dokumentacja administratora aplikacji i administratora środowiska systemu opisująca szczegółowo funkcjonalności, interfejs oraz zasady zarządzania kontami (użytkownikami) oraz uprawnieniami poszczególnych ról, uprawnień, obiektów, profili, użytkowników itp.;
    d. dokumentacja opisująca sposób realizacji wymagań wynikających z przepisów Rozporządzenie 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) jeśli aplikacja przetwarza dane osobowe;
    e. opis zabezpieczeń interfejsów oraz opis metod zapewnienia poufności i rozliczalności tych kanałów przepływu informacji jeśli aplikacja wykorzystuje jakiekolwiek mechanizmy wymiany informacji z innymi systemami;
    f. dokumentacja z testów bezpieczeństwa aplikacji wykonanych przez Wykonawcę lub wykonanych przez niezależną firmę specjalistyczną.
40. Oprogramowanie musi uniemożliwiać modyfikowanie i usuwanie logów, także przez Administratora systemu.
41. Oprogramowanie musi umożliwiać administratorowi przeglądanie historii logowania użytkowników
42. Oprogramowanie musi posiadać możliwość generowania i przeglądania w oferowanym systemie czynności z działań użytkowników i administratorów oraz logów audytowych.
43. Oprogramowanie musi zapewniać bezpieczny mechanizm przechowywania logów audytowych.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

44. Musi być możliwość przesyłania informacji/logów/zdarzeń z Oprogramowania oraz elementów składowych oprogramowania do zewnętrznego systemu korelacji logów systemu SIEM (Splunk) poprzez REST API i/lub syslog/eventlog
45. Oprogramowanie musi posiadać szczegółowy plan odzyskiwania danych po awarii. Plan ten musi być dostarczony na życzenie Zamawiającemu.
46. Dostęp do Oprogramowania będzie możliwy wyłącznie po dokonaniu uwierzytelnienia.
47. Oprogramowanie musi posiadać mechanizmy zabezpieczeń uniemożliwiające niepowołany dostęp do oferowanego rozwiązania oraz zabezpieczenia przed nieuprawnionym dostęp do danych oraz pozostałych modułów aplikacji oraz aplikacji wykorzystywanych przez rozwiązanie (np. silnik bazodanowy i baza danych).
48. Konfiguracja serwera webowego musi wymuszać ustawienie parametru httpOnly w cookies wysyłanych do użytkownika.
49. Oprogramowanie musi posiadać udostępnione na zewnątrz interfejsy usług sieciowych umożliwiające integracje/komunikację dwustronną z innymi rozwiązaniami takimi jak np. Jira, SIEM, Office365.
50. API powinno wymagać uwierzytelniania poprzez przynajmniej klucz. Zamawiający nie dopuszcza rozwiązania w którym API nie wymaga uwierzytelniania..
51. Oprogramowanie nie może korzystać z rozwiązań zewnętrznych umożliwiających śledzenie aktywności i statystyk dotyczących korzystania oprogramowania przez użytkowników np. przez Google Analytics, Motomo itp.
52. Integracja Oprogramowania z użytkowanym przez Zamawiającego Active Directory umożliwiającą mechanizm SSO może odbyć się tylko za pośrednictwem metod takich jak SAML, WS-Federation, OpenID. Zamawiający posiada w produkcji rozwiązanie AAD oraz ADFS. Zamawiający nie dopuszcza NTLM jako metody SSO.
53. Minimalnym akceptowanym algorytmem asymetrycznym jest RSA 2048.
54. Oprogramowanie powinien wspierać tryb pracy Mandatory Access Control (MAC) oparty na atrybutach bezpieczeństwa i politykach (na podstawie atrybutów i polityki udziela się bądź odmawia dostępu do obiektu) lub RBAC (Role Based Access Control).
55. Oferowane oprogramowanie nie może wymagać uprawnień globalnego administratora celem integracji z MS Office 365.

VIII. Posiadane licencje

Zamawiający posiada subskrypcję pakietu Microsoft Office 365 E5.

Zamawiający posiada środowisko hybrydowe, synchronizacja odbywa się jednokierunkowo z Active Directory on-premise do Microsoft Entra ID.

Portal Intranetowy musi opierać się na usłudze SharePoint Online. Musi istnieć możliwość nadawania uprawnień do stron, plików, folderów w oparciu o grupy typu Security synchronizowanych z lokalnego AD.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

IX. Wymagania dotyczące dostarczanej dokumentacji

Wykonawca dostarczy następującą dokumentację:

1) Dokumentację techniczną:

a. Projekt wykonawczy Portalu oraz jego aktualizację w ramach Etapu III,

b. Instrukcję instalacji i konfiguracji środowiska Intranetu

c. Dokumentację powykonawczą.

2) Konspekt szkoleń zawierający instrukcje obsługi wszystkich wdrożonych funkcjonalności Intranetu oraz materiały szkoleniowe. Dokumentacja wytworzona w ramach realizacji Przedmiotu Zamówienia musi charakteryzować się wysoką jakością wykonania, na którą będą miały wpływ w szczególności następujące czynniki:

- czytelna i zrozumiała struktura poszczególnych dokumentów oraz całej dokumentacji z wyodrębnieniem rozdziałów, podrozdziałów i sekcji wraz ze spisem treści,

- stosowanie standardów, rozumianych jako zachowanie jednolitej i spójnej struktury informacji, formy i sposobu prezentacji treści poszczególnych produktów, ich fragmentów oraz całej dokumentacji,

- kompletność, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia - oznacza to jednoznaczne i wyczerpujące przedstawienie wszystkich zagadnień w odniesieniu do Portalu,

- spójność i niesprzeczność, rozumiane jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumentacji, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach.

Dokumentacja dostarczona w ramach Umowy musi zostać sporządzona w języku polskim. Ostateczne wersje dokumentacji podlegającej odbiorowi muszą zostać przekazane Zamawiającemu w formie papierowej oraz elektronicznej.

X. Gwarancja jakości :

1. Gwarancja Jakości obejmuje wszelkie niezbędne prace związane z utrzymaniem dostępności oraz prawidłowości działania funkcjonalności Intranetu, z wykluczeniem zadań utrzymania i administracji MS SharePoint Zamawiającego.
2. Gwarancja Jakości będzie świadczona w okresie 12 miesięcy od podpisania protokołu odbioru całościowego zamówienia zgodnie z warunkami zawartymi w Umowie.
3. Gwarancja Jakości zobowiązuje Wykonawcę do usuwania na koszt Wykonawcy Awarii Krytycznej i Awarii Niekrytycznej stwierdzonych po realizacji Umowy potwierdzonej podpisanym Protokołem Odbioru Całościowego.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

4. Awarie Krytyczne określa się jako utratę funkcjonalności uniemożliwiającą korzystanie z Intranetu lub jej kluczowych funkcjonalności i wymagającą podjęcia natychmiastowych działań naprawczych. Awaria Krytyczna zgłaszana jest za pomocą „wniosku o pomoc techniczną" wysłanego na wskazany adres e-mail do obsługi wniosków. Po szczegółowej analizie zgłoszenie takie może zostać wyeskalowane do Incydentu.
   Awarie Niekrytyczne określa się jako utratę części funkcjonalności Intranetu niebędących jej funkcjonalnościami kluczowymi lub nieprawidłowe działanie funkcjonalności Intranetu, która nie wymaga natychmiastowego usunięcia i nie uniemożliwia korzystania z Intranetu. Awaria Niekrytyczna zgłaszana jest za pomocą „wniosku o pomoc techniczną" na wskazany adres e-mail do obsługi wniosków.
   Niedostępność platformy Microsoft nie jest winą Wykonawcy.
5. W ramach Gwarancji Jakości, dla potrzeb obsługi Zgłoszeń, Zamawiający zobowiązuje Wykonawcę do dotrzymania następujących parametrów SLA:

Typ Zgłoszenia	Czas reakcji na Zgłoszenie	Czas rozwiązania Zgłoszenia
Awaria Krytyczna	30 minut	1 Dzień Roboczy
Awaria Niekrytyczna	1 Dzień Roboczy	do 5 Dni Roboczych

XI. Prawo opcji – prace rozwojowe

1. Wykonawca zapewni usługę świadczenia prac rozwojowych pozwalających na modyfikację, rozbudowę i usprawnienie Portalu Intranetowego, w liczbie do 50 roboczogodzin przez okres trwania Gwarancji Jakości.
2. Wykonawca będzie świadczył prace rozwojowe, w ramach których jest zobowiązany do:
   a) parametryzacji i konfiguracji funkcji Portalu Intranetowego przez odpowiednie ustawienia i konfigurację w MS SharePoint w trybie określonym w Umowie, w tym konfigurację nowych funkcjonalności;
   b) wspierania modernizacji wewnętrznej architektury intranetu w celu optymalizacji oraz zwiększenia bezpieczeństwa Intranetu Grupy NCBR w zakresie wymaganym dla obsługi Portalu Intranetowego;
   c) przyjmowania i obsługi Zgłoszeń, na zasadach określonych w SOPZ;

3. Parametryzacja Intranetu, o której mowa w ust. 2 pkt a powyżej, dokonywana jest w porozumieniu z Zamawiającym. Zamawiający w trybie przewidzianym w punkcie 4 może zawnioskować o dodanie lub modyfikację stosowanych parametrów lub o konfigurację określonej funkcjonalności. Powyższe Zgłoszenie może zostać uwzględnione, jeśli jego wdrożenie jest technicznie możliwe, a jego implementacja nie wpłynie na poziom bezpieczeństwa całego Intranetu Grupy NCBR.

4. Podstawą do realizacji przez Wykonawcę Prac rozwojowych będzie każdorazowo odrębne zapotrzebowanie zgłoszone przez Zamawiającego.

5. W celu wykonania Prac rozwojowych Zamawiający składa Wykonawcy Zgłoszenie, które będzie zawierało:

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

1) określenie zakresu pracy do wykonania przez Wykonawcę

2) oczekiwany termin realizacji Zgłoszenia

3) kryteria i warunki odbioru Zgłoszenia

6. Sposób instalacji wyników Prac rozwojowych będzie ustalany w trybie roboczym między Stronami w zależności od skali zmian objętych Poprawką, przy czym minimalny czas reakcji na zgłoszenie to 1 dzień roboczy.

7. Podstawowym narzędziem komunikacji, w tym do zlecania i potwierdzania realizacji Prac rozwojowych po produkcyjnym uruchomieniu Portalu Intranetowego oraz zgłaszania uwag lub zastrzeżeń do realizacji Przedmiotu Umowy, jest poczta elektroniczna, tj. adresy wskazane § 10 ust. 1 Umowy.

8. W przypadku nieuzgodnienia ostatecznej treści Zgłoszenia w wyniku negocjacji, Wykonawca jest zobowiązany do wykonania Zgłoszenia zgodnie z wytycznymi Zamawiającego zawartymi w zapytaniu o realizację Zlecenia, o którym mowa w pkt. 5.

9. Odbiór wykonania Prac rozwojowych nastąpi poprzez podpisanie Protokołu odbioru.

10. W przypadku uwag do Zgłoszenia, Wykonawca jest zobowiązany do uzupełnienia lub poprawienia, w terminie wyznaczonym przez Zamawiającego, nie dłuższym jednak niż 3 Dni Robocze.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR