Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. Cel dokumentu

Celem dokumentu jest opisanie szczegółowego przedmiotu zamówienia (SOPZ) oraz kluczowych zapisów umowy dla modelu realizacji end-to-end przez jednego Wykonawcę, obejmującego: analizę/warsztaty, projekt UX/UI, implementację, wdrożenie, migrację, hosting, utrzymanie (RUN), wsparcie (SLA) oraz szkolenia i dokumentację.

Dokument zawiera mierzalne kryteria odbioru, KPI/SLO, metody weryfikacji, wymagania bezpieczeństwa i operacyjne oraz plan wyjścia (exit plan) minimalizujący vendor lock-in.

2. Zakres stosowania i założenia

2.1. Model realizacji

Realizacja odbywa się w modelu „jeden Wykonawca – end-to-end", w którym Wykonawca jest odpowiedzialny zarówno za etap wytworzenia (BUILD), jak i za utrzymanie środowisk (RUN).

Wykonawca dostarczy rozwiązanie w modelu SaaS (Software as a Service). Architektura systemu musi jednak umożliwiać pełną migrację do środowiska IaaS (Infrastructure as a Service) Zamawiającego lub podmiotu trzeciego.

2.2. Założenia bazowe

- System: serwis WWW + panel CMS + środowiska dev/stage/prod.
- Dostępność: WCAG 2.1 AA (minimum; wyższy poziom jeśli będzie wymagany przez ustawodawcę przed odbiorem strony przez Zamawiającego).
- Języki: PL oraz EN.
- Hosting: chmura lub infrastruktura Wykonawcy; konta i domena należą do Zamawiającego.
- Analityka: integracja z narzędziem analitycznym Zamawiającego i systemem zgód cookie.

2.3. Zasady pierwszeństwa dokumentów

W przypadku sprzeczności pierwszeństwo mają kolejno: (1) Umowa, (2) SOPZ, (3) Oferta Wykonawcy, (4) załączniki i materiały pomocnicze – o ile Umowa nie stanowi inaczej.

3. Definicje i skróty

Termin	Definicja
Firma	Narodowe Centrum Badań i Rozwoju
BUILD	Etap wytworzenia: analiza, projekt, implementacja, testy, wdrożenie.
RUN	Etap utrzymania: hosting, monitoring, kopie zapasowe, aktualizacje, wsparcie.
KPI	Wskaźniki sukcesu projektu, weryfikowane w odbiorach lub cyklicznie w RUN.
SLO	Service Level Objective – cel operacyjny (np. dostępność), mierzony w RUN.

SLA	Service Level Agreement – zobowiązanie dot. poziomu usług (SLO + czasy reakcji/naprawy).
Incydent	Zdarzenie powodujące niedostępność lub pogorszenie działania usługi w RUN.
Błąd	Nieprawidłowe działanie w zakresie uzgodnionych wymagań/akceptacji.
Zmiana (CR)	Modyfikacja wymagań lub funkcjonalności poza uzgodnionym zakresem/Definition of Done.
Go-Live	Przejście produkcyjne rozwiązania, spełniające warunki uruchomienia.
API	Application Programming Interface – interfejs programistyczny do komunikacji aplikacji.
ASN	Autonomous System Number – numer systemu autonomicznego; identyfikator operatora w Internecie (używany m.in. przy pomiarach z różnych sieci).
Backlog	Uporządkowana lista wymagań/zadań do realizacji (produktowych i technicznych).
Cache	Mechanizm buforowania odpowiedzi/zasobów w celu przyspieszenia działania serwisu.
CDN	Content Delivery Network – sieć dystrybucji treści (cache na brzegu sieci) w celu poprawy wydajności i odporności.
CI/CD	Continuous Integration / Continuous Delivery (lub Deployment) – automatyzacja budowania, testów i wdrożeń w pipeline.
CLS	Cumulative Layout Shift – metryka stabilności wizualnej (Core Web Vitals).
Core Web Vitals (CWV)	Zestaw metryk UX (LCP, INP, CLS) używany do oceny doświadczenia użytkownika.
Crawl	Automatyczne przeglądanie (skan) serwisu przez crawler w celu wykrycia błędów (np. 404) i porównania URL.
CR	Change Request – wniosek o zmianę poza zakresem/DoD, rozliczany zgodnie z Umową (zob. Zmiana).
CSP	Content-Security-Policy – nagłówek bezpieczeństwa ograniczający źródła zasobów (ochrona m.in. przed XSS).
dev/stage/prod	Środowiska: deweloperskie / testowe (staging) / produkcyjne.
DNS	Domain Name System – system nazw domenowych (mapowanie nazwy na adres IP).
DoD	Definition of Done – uzgodniona definicja

	„zrobione”, kryteria ukończenia elementu backlogu/etapu.
DR	Disaster Recovery – odtwarzanie po awarii; zestaw procedur i narzędzi zapewniających ciągłość działania.
DDoS	Distributed Denial of Service – atak odmowy usługi realizowany z wielu źródeł.
Endpoint	Punkt końcowy (np. URL) usługi lub API, na którym wykonywane są żądania.
HSTS	HTTP Strict-Transport-Security – nagłówek wymuszający użycie HTTPS przez przeglądarkę.
HTTP	Hypertext Transfer Protocol – protokół komunikacji WWW; kody 2xx/3xx/4xx/5xx opisują wynik żądania.
IA	Information Architecture – architektura informacji (struktura, nawigacja, etykiety).
INP	Interaction to Next Paint – metryka responsywności (Core Web Vitals).
LCP	Largest Contentful Paint – metryka szybkości ładowania (Core Web Vitals).
Lighthouse	Narzędzie (Google) do audytu WWW: performance, accessibility, SEO, best practices.
MFA/2FA	Multi-Factor Authentication / Two-Factor Authentication – uwierzytelnianie wieloskładnikowe.
MTTA/MTTR	Mean Time To Acknowledge / Mean Time To Repair – średni czas potwierdzenia / przywrócenia usługi.
p75/p95/p99	Percentyle (75/95/99) rozkładu metryki; np. p95 = wartość, której nie przekracza 95% próbek.
PAM	Privileged Access Management – zarządzanie dostępem uprzywilejowanym (konto admin/produkcyjne).
Pentest	Test penetracyjny – kontrolowana próba przełamania zabezpieczeń w celu znalezienia podatności.
Pipeline	Automatyczny proces w CI/CD (build → test → deploy) uruchamiany np. na commicie.
RPS	Requests Per Second – liczba żądań na sekundę (miara obciążenia).
RPO/RTO	Recovery Point Objective / Recovery Time Objective – dopuszczalna utrata danych / czas odtworzenia.
RUM	Real User Monitoring – pomiary

	wydajności/UX na danych z realnych użytkowników w produkcji.
SBOM	Software Bill of Materials – wykaz komponentów i zależności (wersje/licencje) użytych w oprogramowaniu.
SEO	Search Engine Optimization – optymalizacja widoczności w wyszukiwarkach.
Smoke test	Szybki test podstawowych funkcji po wdrożeniu, potwierdzający „czy dymi”/czy działa krytyczna ścieżka.
Staging	Środowisko przedprodukcyjne do testów integracyjnych i weryfikacji wdrożeń.
TLS	Transport Layer Security – protokół szyfrowania połączeń (HTTPS, certyfikaty).
T&M	Time & Materials – rozliczenie za czas pracy i materiały (model kosztowy).
Uptime monitoring	Monitoring dostępności (ping/HTTP check) wykonywany cyklicznie z wielu lokalizacji.
UX/UI	User Experience / User Interface – projektowanie doświadczenia użytkownika i interfejsu.
Vendor lock-in	Uzależnienie od jednego dostawcy/technologii utrudniające zmianę (wyjście/exit plan).
WAF	Web Application Firewall – zapora aplikacyjna filtrująca i monitorująca ruch HTTP/HTTPS.
WCAG 2.1 AA	Web Content Accessibility Guidelines 2.1, poziom AA – standard dostępności WWW.
WYSIWYG	What You See Is What You Get – edytor treści bez potrzeby znajomości HTML.
SOPZ	Szczegółowy Opis Przedmiotu Zamówienia – dokument opisujący zakres i wymagania zamówienia.
Agile	Zwinne podejście do wytwarzania, oparte na iteracyjnym dostarczaniu wartości i adaptacji do zmian.
Sprint	Iteracja w Scrum – ograniczony czasowo cykl pracy (np. 1–4 tygodnie) zakończony przyrostem.

4. Cele projektu i wskaźniki sukcesu (KPI/SLO)

4.1. Cele biznesowe

- Unowocześnienie serwisu pod względem wizualnym: Interaktywność i grafika zgodna z najnowszymi trendami projektowymi.
- Intuicyjność nawigacji po serwisie: użytkownik szybko odnajduje poszukiwane informacje z naciskiem na Konkursy, Harmonogram konkursów, Kalendarz wydarzeń, zamówienia publiczne.
- Stworzenie przejrzystego i funkcjonalnego modułu do prezentacji Konkursów ogłaszanych przez NCBR z wyszukiwarką.
- Użycie odpowiedniej kolorystyki, czcionek i grafik, spójnych z identyfikacją wizualną NCBR - Zamawiający udostępni aktualną Księgę Znaku NCBR i obowiązujące logotypy.
- Zwiększenie dostępności i użyteczności serwisu dla użytkowników końcowych.
- Poprawa widoczności w wyszukiwarkach (SEO) przy zachowaniu zgodności z wymaganiami prawnymi.
- Bezpieczne i stabilne utrzymanie serwisu (RUN) z mierzalnym SLA.

4.2. KPI jakości, wydajności i UX (weryfikacja w odbiorze końcowym i po Go-Live)

Obszar	Cel/Próg	Metoda pomiaru	Kryterium zaliczenia
Core Web Vitals (RUM lub lab + symulacja mobile)	LCP p75 ≤ 2,5 s; INP p75 ≤ 200 ms; CLS p75 ≤ 0,1 (strona główna i 5 kluczowych szablonów).	Lighthouse CI/WebPageTest + (jeśli dostępne) RUM; profile: Mobile 4G/CPU mid-tier.	Spełnienie progów dla ≥ 90% badanych URL w zestawie testowym.
Lighthouse – Performance	≥ 85 (Mobile) dla strony głównej i 5 kluczowych szablonów.	Lighthouse CI w pipeline; 3 przebiegi, median.	Wynik spełniony dla wszystkich URL w zestawie testowym.
Lighthouse – Accessibility	≥ 90 (Mobile) oraz brak krytycznych błędów dostępności.	Lighthouse + test manualny (klawiatura, czytnik ekranu).	Brak krytycznych niezgodności; pozostałe naprawione lub zaakceptowane planem.
Stabilność	Błędy 5xx ≤ 0,1% w teście obciążeniowym; błędy JS krytyczne = 0 w smoke test.	Test obciążeniowy + logi aplikacyjne + monitoring.	Raport z testów i brak krytycznych defektów.

4.3. KPI dostępności (WCAG) – wymagania zgodności i weryfikacja

Wymagany poziom zgodności: WCAG 2.1 AA (minimum). Weryfikacja obejmuje audyt automatyczny oraz manualny. Wykonawca dostarcza raport audytu wraz z listą niezgodności, planem naprawczym i potwierdzeniem poprawek (retest).

- Minimalny zakres testów manualnych:
    - nawigacja klawiaturą (Tab/Shift+Tab, fokus, skip-linki),
    - kontrast i powiększenie 200%,
    - czytnik ekranu (NVDA/JAWS – przynajmniej jeden),
    - formularze (etykiety, błędy walidacji, komunikaty).

4.4. SLO dostępności usługi w RUN

SLO (miesięcznie): dostępność ≥ 99,9% dla warstwy aplikacyjnej (HTTP 200/301/302 jako dostępne; 5xx jako niedostępne).

Wyłączenia: planowane okna serwisowe do 4 h/miesiąc po wcześniejszym powiadomieniu (min. 48 h) oraz incydenty spowodowane działaniami Zamawiającego lub siłą wyższą.

4.5. Definicja pomiaru dostępności (SLO) i źródło prawdy

- Źródło prawdy: dostępność jest liczona na podstawie raportów z monitoringu uptime wskazanego w Umowie (narzędzie Zamawiającego lub Wykonawcy – do wyboru). W przypadku dwóch narzędzi referencyjnych, źródłem prawdy jest narzędzie Zamawiającego, o ile jego konfiguracja odpowiada uzgodnionym parametrom (interwał, punkty pomiarowe, URL).
- Punkt pomiaru: pomiar realizowany z co najmniej 2 niezależnych lokalizacji (np. różne regiony/ASN) co 1 minutę. Badany jest publiczny adres URL warstwy prezentacji (front) oraz osobno punkt kontrolny API (jeśli dotyczy).
- Kryterium „dostępne/niedostępne”: odpowiedź HTTP 200/301/302 z czasem odpowiedzi ≤ 5 s oznacza „dostępne”. HTTP 5xx, timeout, błędy TLS/DNS oraz brak odpowiedzi oznaczają „niedostępne”.
- Agregacja: dla danego interwału minuta jest liczona jako „niedostępna”, jeżeli ≥ 50% prób w tej minucie zakończy się „niedostępne” w co najmniej jednym punkcie pomiarowym. (Parametry mogą zostać dostosowane w Umowie.)
- Wyłączenia: planowane okna serwisowe (maks. 4 h/mies.), zdarzenia siły wyższej, incydenty wywołane działaniami Zamawiającego oraz niedostępność wynikająca z działań osób trzecich pozostających poza kontrolą Wykonawcy – o ile Wykonawca wykaże należyte działania minimalizujące skutki.

5. Zakres zamówienia (end-to-end)

5.1. Zakres do realizacji

- Warsztaty/discovery, analiza wymagań, backlog i plan realizacji.
- Projekt UX/UI wraz z design system i przekazaniem specyfikacji (handoff).
- Implementacja serwisu i konfiguracja CMS (role, workflow, wersjonowanie treści).
- Przygotowanie środowisk dev/stage/prod oraz CI/CD (min. staging + produkcja).
- Testy: funkcjonalne, regresja, wydajność, dostępność, bezpieczeństwo – zgodnie z planem testów.
- Migracja danych/treści zgodnie z rozdz. 14.
- Wdrożenie, Go-Live, plan rollback.
- Hosting i utrzymanie RUN wraz z monitoringiem, backupem, aktualizacjami i obsługą incydentów.
- Dokumentacja (użytkowa i techniczna), runbook, szkolenia (min. 4 sesje).

5.2. Zakres wyłączenia

- Tworzenie treści (copywriting), opracowanie materiałów redakcyjnych i tłumaczenia – dostarcza Zamawiający.
- Zakup płatnych licencji zewnętrznych i zasobów stock .
- Bieżąca redakcja treści po Go-Live (RUN obejmuje wsparcie techniczne, nie redakcję).

6. Organizacja prac i komunikacja

6.1. Model współpracy

Rekomendowany model: zwinny (Agile) z dwutygodniowymi iteracjami oraz formalnymi odbiorami etapów. Dopuszcza się model kaskadowy, o ile zachowane są artefakty i kryteria odbioru.

6.2. Komunikacja

- Spotkanie statusowe: 1x/tydzień (30–60 min).
- Warsztaty/planowanie: wg potrzeb (min. na start i przed Go-Live).
- Kanały: [Teams], e-mail, system zgłoszeń (ticketing).
- Eskalacja P1: telefon + komunikator; powiadomienie w ≤ 15 min od wykrycia.

7. Etapy realizacji i artefakty

Każdy etap kończy się odbiorem cząstkowym, protokołem oraz spełnieniem kryteriów przejścia. Liczba iteracji poprawek w ramach etapu jest ograniczona, aby zapobiec niekontrolowanemu rozszerzaniu zakresu.

7.1. Etap 1 – Warsztaty / discovery

Artefakty: backlog (wymagania), mapa serwisu/IA, ryzyka i zależności, wstępna architektura, plan projektu.

Iteracje: max 2 rundy doprecyzowania backlogu po warsztatach.

Kryterium przejścia: zaakceptowany backlog i plan (harmonogram, kamienie milowe).

Organizacja warsztatów: liczba osób po stronie Zamawiającego 10–20; forma stacjonarna lub zdalna.

7.2. Etap 2 – Projekt UX/UI

Artefakty: makiety low-fi, prototyp hi-fi, design system (komponenty), specyfikacja dla dev (handoff).

Iteracje: łącznie 4 tury poprawek do wybranej linii graficznej (3 tury w Etapie 2 + 1 tura doprecyzowująca w Etapie 3 w trakcie implementacji).

Kryterium przejścia: akceptacja prototypu + komplet specyfikacji.

Wykonawca przedstawia 3 różne wersje graficzne strony głównej (mobile i desktop). Zamawiający wybiera jedną wersję do wdrożenia.

7.3. Etap 3 – Implementacja i konfiguracja CMS

Artefakty: kod w repozytorium Zamawiającego, konfiguracje, role i uprawnienia, pipeline CI/CD, dokumentacja techniczna. Minimum 2 środowiska (staging/prod) + automatyczne wdrożenia na staging.

Kryterium przejścia: testy funkcjonalne i regresja zaliczone; raport z testów bezpieczeństwa (skan) bez podatności krytycznych.

7.4. Etap 4 – Wdrożenie i uruchomienie (Go-Live)

Artefakty: plan wdrożenia, plan rollback, lista kontrolna Go-Live, raporty z testów (wydajność/a11y/bezpieczeństwo), konfiguracja DNS/TLS.

Kryterium przejścia: spełnienie warunków Go-Live (rozdz. 15.3) oraz protokół uruchomienia.

8. Wymagania funkcjonalne (zgrupowane)

8.1. UX/UI i zgodność z identyfikacją

Unikalny, spójny design odzwierciedlający misję i wizję organizacji, zgodny z identyfikacją wizualną przekazaną przez Zamawiającego, z uwzględnieniem zasad UX/UI i dostępności (WCAG).

8.2. CMS i zarządzanie treścią

- Preferowana platforma CMS: WordPress (dopuszczalne rozwiązania równoważne).
- Obsługa dwóch wersji językowych (PL i EN) w ramach jednego systemu CMS i jednego logowania; wersja EN z treścią dostarczaną przez Zamawiającego.
- Role i uprawnienia z podziałem na administratorów i redaktorów, wraz z workflow akceptacji treści.
- Wersjonowanie treści i możliwość przywracania poprzednich wersji.
- Możliwość włączania/wyłączania wybranych modułów oraz tryb „strona wyłączona” dla wskazanych podstron (komunikat serwisowy).
- Metatagi SEO (title, description) edytowalne per podstrona; automatyczne generowanie, jeśli pola są puste (title = tytuł podstrony, description = pierwsze 60 znaków treści lub title).
- Zamawiający dopuszcza zastosowanie rozwiązania równoważnego do systemu WordPress, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych i technicznych określonych w niniejszym opisie przedmiotu zamówienia, w szczególności w zakresie: zarządzania treścią, rozszerzalności poprzez moduły, zarządzania użytkownikami, integracji poprzez API oraz możliwości instalacji na infrastrukturze Zamawiającego z uwzględnieniem następujących kryteriów równoważności. Rozwiązanie równoważne musi:
  - być systemem zarządzania treścią (CMS) umożliwiającym tworzenie i zarządzanie stronami WWW;
  - być dostępne na licencji open source lub licencji niewymagającej opłat za użytkowników końcowych;
  - umożliwiać instalację na infrastrukturze Zamawiającego (on-premise) lub w środowisku chmurowym;
  - zapewniać dostęp do kodu źródłowego lub możliwość jego modyfikacji poprzez rozszerzenia;
  - zapewniać graficzny edytor treści (WYSIWYG);
  - zapewniać obsługę stron i wpisów (artykułów);
  - zapewniać możliwość tworzenia hierarchii stron;
  - zapewniać zarządzanie kategoriami i tagami;
  - zapewniać planowanie publikacji treści;
  - zapewniać wersjonowanie lub historię zmian treści;
  - zapewniać obsługę multimediów (biblioteka plików);
  - umożliwiać instalowanie rozszerzeń / modułów / pluginów;
  - umożliwiać tworzenie własnych rozszerzeń przez Zamawiającego lub podmioty trzecie;
  - zapewniać dostępność repozytorium dodatków lub otwartego ekosystemu rozszerzeń;
  - umożliwiać tworzenie wielu ról użytkowników;
  - umożliwiać definiowanie uprawnień do edycji, publikacji i administracji;
  - umożliwiać obsługę wielu redaktorów jednocześnie;
  - umożliwiać integrację z mechanizmami uwierzytelniania;
  - umożliwiać dostęp techniczny dla robota Zamawiającego automatyzującego wybrane procesy;

- umożliwiać stosowanie motywów / szablonów graficznych;
- umożliwiać oddzielenie warstwy prezentacji od treści;
- umożliwiać modyfikację szablonów przez programistów;
- oferować REST API umożliwiające integrację z innymi systemami;
- oferować możliwość publikacji treści w modelu headless CMS;
- oferować możliwość integracji z systemami analitycznymi i marketingowymi;
- działać w środowisku serwera WWW;
- korzystać z relacyjnej bazy danych;
- wspierać standardowe technologie webowe (HTML5, CSS, JavaScript);
- zapewniać mechanizmy aktualizacji bezpieczeństwa;
- zapewniać możliwość instalacji aktualizacji systemu i rozszerzeń;
- zapewniać zarządzanie uprawnieniami użytkowników;
- zapewniać wsparcie dla HTTPS;
- być aktywnie rozwijane;
- posiadać publiczną dokumentację techniczną;
- posiadać społeczność użytkowników lub wsparcie producenta.

8.3. Edycja treści (WYSIWYG)

Edytor WYSIWYG ma umożliwiać redakcję treści bez znajomości HTML, w tym m.in.:

- kopie robocze, formatowanie tekstu (pogrubienie, kursywa, podkreślenie), listy, tabele, wstawianie linków, czyszczenie formatowania, cofanie/ponawianie,
- nagłówki H2–H6,
- osadzanie multimediów (np. YouTube),
- możliwość przełączania w tryb HTML edytora,
- możliwość dodania na stronach przycisku: „drukuj”, „zapisz do pliku pdf”
- podgląd w nowym oknie wersji zapisanej.

8.4. Pliki do pobrania i repozytorium mediów

- CMS ma umożliwiać dodawanie plików (domyślnie do 50 MB z możliwością zmiany limitu przez administratora), nadawanie nazw oraz prezentowanie rozmiaru pliku (kB/MB).
- Dopuszczalne formaty plików (minimum): PDF, DOC/DOCX, XLS/XLSX, PPT/PPTX, RTF, ODT, JPG, PNG, GIF, MP3, MP4, AVI, ZIP, RAR. Format SWF/Flash jest niedopuszczalny.

8.5. Elementy nawigacji i szablony

- Mapa serwisu (HTML) dostępna z dowolnego miejsca, z odwzorowaniem hierarchii; elementy BIP oznaczone ikoną.
- Breadcrumbs (okruszki) prezentujące ścieżkę z możliwością przejścia na wyższe poziomy.
- Strona błędu 404 w obu językach oraz strona czasowej niedostępności w obu językach.
- Stopka i nagłówek edytowalne z poziomu CMS.
- Tryb „żałobny” (monochromatyczny) uruchamiany z poziomu CMS.
- Tryb „wysoki kontrast” dostępny dla użytkownika.

8.6. Moduły i obszary tematyczne

Poniższe moduły stanowią minimalny zakres funkcjonalny. Szczegółowe modele danych i kryteria odbioru są doprecyzowane w backlogu po etapie discovery, bez zmiany zakresu biznesowego.

Platforma konkursowa

- Zaawansowana wyszukiwarka konkursów (nazwa, program, finansowanie, status, terminy, słowa kluczowe).
- Dedykowany formularz konkursu: tytuł, logotypy, grafiki, opis, terminy (z automatyczną zmianą statusu), budżet, sekcje tekstowe, multimedia, dokumenty (kategorie/sekcje), metadane do wyszukiwarki.
- Możliwość linkowania do podstron i serwisów zewnętrznych; dedykowane aktualności konkursu, propagacja aktualności do innych miejsc serwisu.
- Polubienia/ulubione bez logowania; pobieranie dokumentów (także ZIP); udostępnianie (social/e-mail/sms),
- Otwarte API pozwalające na przekazywanie użytkownikom zewnętrznym informacji/danych związanych z publikowanymi konkursami przez NCBR oraz listami rankingowymi publikowanymi w serwisie.
    - Dane udostępniane w API zgodne z prezentowanymi na podstronie https://www.gov.pl/web/ncbr/platforma-konkursowa:
    - Udostępniane pola:
        - Nazwa z linkiem do podstrony konkursu,
        - Status
        - Budżet
        - Ogłoszenie konkursu
        - Rozpoczęcie naboru wniosków
        - Zakończenie naboru wniosków
        - Opis
        - Listy Rankingowe

Moduł Aktualności

- Możliwość tworzenia wielu niezależnych zbiorów aktualności; propagacja artykułów do innych modułów jako skróty.
- Artykuł: tytuł, grafika główna, wprowadzenie, treść (WYSIWYG + HTML), multimedia, galerie, data publikacji (edytowalna), załączniki.

Zamówienia Publiczne

- Publikacja postępowań w kategoriach; formularz pól: nazwa, numer, status (aktualne/zakończone/anulowane), daty, jednostka publikująca, opis.
- Zmiana Statusu z aktualne na zakończone następuje po upływie wskazanej daty i/lub przez działanie administratora serwisu.
- Po zmianie statusu na zakończone/anulowane – wyszarzenie tytułu.

- Możliwość linkowania do zewnętrznej Platformy Zakupowej.

Oferty pracy

- Lista ofert z kategoriami: Aktualne/W toku/Zakończone; sortowanie wg daty z możliwością priorytetyzacji.
- Możliwość publikacji list kandydatów dla kategorii: W toku/Zakończone.
- Listy kandydatów nie mogą być dostępne do indeksowania przez wyszukiwarki (boty).
- Kasowanie list po zamknięciu procesu w sposób trwały z zasobów serwisu.
- Wielo-spółkowość: odrębna szata graficzna ogłoszeń i oznaczenie (np. Logo, kolor czcionki, grafika główna) na liście.
- Pola ogłoszenia: stanowisko, dział/jednostka, miejsce, etat, numer ref, daty, wymagania, benefity (ikony), kontakt, link do zewnętrznego systemu CV, forma zatrudnienia, BIP.
- Dla ofert „w toku" i „zakończone": możliwość dodania PDF z listami kandydatów oraz trwałego usuwania plików.

Harmonogram konkursów

- Widok roczny; dla kolejnych lat osobne podstrony.
- Filtrowanie: obszar, rodzaj wnioskującego, źródło finansowania, program, status, daty; sortowanie (start, koniec, nazwa).
- Polubienia/ulubione bez logowania; linkowanie do konkursu w platformie konkursowej.

Biuletyn Informacji Publicznej (BIP)

- Dziennik zmian i rejestr prób nieuprawnionych zmian.
- Oznaczanie treści jako BIP i prezentacja w mapie serwisu z ikoną.
- Pola wymagane: utworzone przez, opublikowane przez, data ostatniej modyfikacji; historia zmian dostępna dla użytkownika (rozwijana).

Pop-up

- Pop-up zamykany przez użytkownika, czasowy (czas definiowany przez administratora) i po przewinięciu strony.
- Administrator serwisu podczas tworzenia/ustawiania pop-upu decyduje o rodzaju pop-up (zamykany przez użytkownika, czasowy, znikający po przewinięciu strony).
- Tytuł, grafika , treść, link, "x" zamykanie okna pop-upu.

Kalendarz

- Widok miesięczny z nawigacją między miesiącami.
- Dzień z wydarzeniem wyróżniony w kalendarzu z podglądem tematów i ilości wydarzeń w danym dniu.
- Formularz wydarzenia:
  - Kiedy: Data i godzina rozpoczęcia oraz zakończenia wydarzenia.
  - Gdzie: Lokalizacja wydarzenia.
  - Opis: Krótki opis wydarzenia.
  - Grafika: Możliwość dodania obrazka lub grafiki związanej z wydarzeniem.

- Dodaj do kalendarza: Opcja dodania wydarzenia do zewnętrznych kalendarzy (np. Outlook, Google Calendar).
- Link: Możliwość dodania linku do strony z dodatkowymi informacjami o wydarzeniu.

- Eksport „Dodaj do kalendarza" :

  Wykonawca wdroży mechanizm pozwalający użytkownikom na szybki eksport terminów wydarzeń (np. daty konkursów, naborów, aktualności) do osobistych kalendarzy zewnętrznych.

  - Obsługiwane platformy: Google Calendar, Microsoft Outlook (wersja desktopowa oraz Web/Office 365) oraz Apple Calendar (iOS/macOS)
  - Brak konieczności instalacji dodatkowego oprogramowania przez użytkownika

9. Wymagania niefunkcjonalne

9.1. Wydajność i skalowanie

Wykonawca przeprowadzi testy obciążeniowe i dostarczy raport. Parametry testów są dopasowane w discovery do profilu ruchu, przy zachowaniu minimum:

- Scenariusz minimalny: 200 RPS przez 10 min + 30 min test stabilności 50 RPS (o ile nie zostanie uzgodniony scenariusz równoważny bardziej adekwatny do profilu ruchu).
- Metryki: p95 czasu odpowiedzi dla kluczowych endpointów ≤ 800 ms (dynamiczne) oraz ≤ 400 ms (cache).
- Błędy: 5xx ≤ 0,1%; 4xx ≤ 1% (z wyłączeniem celowych przypadków).
- Raport: konfiguracja testu, wyniki, wnioski i rekomendacje.

9.2. Dostępność (WCAG) – weryfikacja

Weryfikacja: audyt automatyczny + manualny. Wykonawca usuwa niezgodności przed odbiorem końcowym; dla wyjątków wymagane jest pisemne zaakceptowanie ryzyka przez Zamawiającego oraz plan naprawczy.

9.3. Kompatybilność z przeglądarkami i systemami operacyjnymi

Wykonawca zapewni pełną i poprawną funkcjonalność oraz tożsamość wizualną Serwisu w najnowszych, stabilnych wersjach przeglądarek (wersja bieżąca oraz jedna wstecz – tzw. model n-1) na następujących platformach:

- Desktop (Windows, macOS, Linux): Google Chrome, Microsoft Edge, Mozilla Firefox, Safari (wyłącznie macOS).
- Mobile (Android, iOS): Google Chrome Mobile, Safari Mobile, Samsung Internet.

- Weryfikacja: Serwis musi działać poprawnie również wewnątrz tzw. In-App Browsers (np. przeglądarki wewnątrz aplikacji Facebook, Instagram, LinkedIn).
- Standardy: Kod źródłowy musi być zgodny ze standardami HTML5 oraz CSS3. Wyklucza się stosowanie technologii wycofanych (np. Flash, Silverlight) lub nieobsługiwanych przez w/w przeglądarki.

9.4. Responsywność (RWD) i Mobile-First

Projekt i wdrożenie muszą być realizowane zgodnie z podejściem Mobile-First, zapewniając optymalne doświadczenie użytkownika na ekranach o różnej rozdzielczości.

- Zakres rozdzielczości: Serwis musi skalować się płynnie w zakresie szerokości viewportu od 320px do 1920px (oraz zapewniać poprawne centrowanie/konteneryzację treści na ekranach Ultra-Wide powyżej 1920px).
- Punkty przełamania (Breakpoints): Wykonawca zdefiniuje co najmniej 4 punkty przełamania (np. Mobile, Tablet Portrait, Tablet Landscape/Laptop, Desktop), dostosowane do specyfiki layoutu, a nie tylko do konkretnych modeli urządzeń.
- Interakcje dotykowe: Wszystkie elementy klikalne (buttony, linki, pola formularzy) w widokach mobilnych:
  - muszą posiadać minimalny rozmiar obszaru dotykowego 44x44 px.
  - odstępy między elementami interaktywnymi muszą zapobiegać przypadkowym kliknięciom.
- Błędy krytyczne RWD: Niedopuszczalne jest występowanie poziomego paska przewijania (horizontal scroll) na jakiejkolwiek rozdzielczości oraz nakładanie się na siebie elementów tekstowych i graficznych (tzw. overlap).
- Stabilność wizualna: Zgodnie z parametrem KPI CLS (Cumulative Layout Shift) z pkt 4.2, ładowanie elementów (np. reklam, obrazów, fontów) nie może powodować nieoczekiwanych przesunięć treści powyżej wartości 0,1.

9.5. SEO i analityka

- Sitemapy XML i robots.txt; canonical; hreflang dla wersji językowych.
- Przekierowania 301 po migracji – kompletna mapa URL i walidacja.
- Metadane: title/description, Open Graph/Twitter Cards, dane strukturalne (jeśli dotyczy).
- Integracja z narzędziem analitycznym Zamawiającego oraz systemem tagowania; obsługa zgód cookie.

9.6. API

- Dostęp przez szyfrowany protokół HTTPS.
- Zrealizowane w architekturze REST, z użyciem standardowych metod (GET dla pobierania danych), tylko do odczytu.
- Dane zwracane w formacie JSON (UTF-8), paginacja.
- Wersjonowane w adresie URL (np. /api/v1/contests).

- Wbudowany mechanizm cache i konfigurowalne limitowanie zapytań.
- W skład API wchodzi interaktywna dokumentacja w standardzie OpenAPI 3.0 (np. poprzez Swagger UI).
- Dostępność danych tożsama z dostępnością serwisu WWW (SLA).

9.7. Dopasowanie scenariuszy testów wydajności do profilu ruchu

- W etapie discovery Strony uzgadniają profil ruchu (średni i pikowy), kluczowe ścieżki użytkownika oraz listę endpointów krytycznych.
- Scenariusze testów obejmują co najmniej: (a) strona główna, (b) wyszukiwarka konkursów i listy, (c) szczegóły konkursu/aktualności, (d) pobieranie plików.
- Parametry minimalne z rozdz. 9.1 pozostają wartościami referencyjnymi; mogą zostać podwyższone lub zastąpione scenariuszem równoważnym lepiej odzwierciedlającym ruch, na podstawie danych Zamawiającego.
- Raport z testów zawiera rekomendacje optymalizacji i propozycje konfiguracji cache/CDN/WAF zgodnie z profilem ryzyka i ruchu.

9.8. Wymaganie dla usług hostowanych

- Wymagane jest korzystanie z dostawców usług chmury obliczeniowej certyfikowanych na zgodność z normą ISO 27001;
- Wymagane jest korzystanie z dostawców usług chmury obliczeniowej certyfikowanej na zgodność z normą ISO 27017;
- Wymagane jest korzystanie z dostawców usług chmury obliczeniowej certyfikowanej na zgodność z normą ISO 27018;
- Dostawca chmury obliczeniowej musi zapewniać SLA na wszystkie oferowane usługi na poziomie minimum 99,5%.
- W chmurze obliczeniowej musi być zapewniona możliwość szyfrowania danych kluczem generowanym i zarządzanym przez klienta.
- Dane prawnie chronione, przetwarzane w chmurze obliczeniowej muszą być szyfrowane zawsze „at rest” oraz „in transit”.
- Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwarzanych informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:
    - domyślną zasadę braku dostępu do przetwarzanych informacji klienta;
    - domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych klienta lub w innych uruchamianych usługach chmury obliczeniowej;
    - zasadę „minimum koniecznego” dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez klienta (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem klienta, a cały proces obsługi i wykonania czynności jest logowany.

- udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;
- domyślne uruchamianie nowego środowiska (lub usługi chmury obliczeniowej) separowanego od innych tenantów, z ustawieniami „secure-by-default".
- Zapewniona musi być możliwość zbierania logów związanych z przetwarzaniem informacji w chmurze i zabezpieczenia ich przed nieautoryzowanym dostępem i modyfikacją. Retencja logów ma wynosić minimum 30 dni.
- Chmura obliczeniowa musi posiadać przynajmniej dwa równorzędne ośrodki przetwarzania danych:
    - z możliwością replikacji danych między ośrodkami;
    - z możliwością balansowania ruchu między ośrodkami;
    - z dostępnym bezpośrednim łączem między centrami danych dostawcy chmury.

Uruchomienie i świadczenie usług i składowania danych w chmurze obliczeniowej na terytorium krajów Europejskiego Obszaru Gospodarczego.

10. Wymagania bezpieczeństwa

1. Strona internetowa musi być dostępna za pośrednictwem protokołu https, z wykorzystaniem TLS w wersji 1.2 lub wyższej.
2. Strona internetowa musi wykorzystywać certyfikat wystawiony przez powszechnie rozpoznawany urząd certyfikacji.
3. Zarządzanie stroną internetową obejmuje nadzór nad ważnością certyfikatu oraz podejmowanie działań w celu jego odpowiednio wczesnego odnowienia.
4. Do obsługi strony internetowej muszą być wykorzystywane wyłącznie bezpieczne komponenty, wolne od znanych podatności. Dotyczy to zarówno komponentów front-end (np. skryptów uruchamianych w przeglądarce użytkownika), jak i back-end (np. systemu CMS, oprogramowania serwera WWW, systemowego i bazodanowego).
5. Komponenty wykorzystywane do obsługi strony internetowej muszą być objęte wsparciem producenta, zapewniającym bieżące publikowanie poprawek bezpieczeństwa.
6. Komponenty wykorzystywane do obsługi strony internetowej muszą być objęte procesem zarządzania podatnościami i podlegać regularnym aktualizacjom. Aktualizacje muszą uwzględniać weryfikację poprawności działania i publikacji strony internetowej oraz, w miarę potrzeby, jej dostosowanie do wprowadzonych zmian.
7. Komponenty wykorzystywane do obsługi strony internetowej muszą być eksploatowane zgodnie z warunkami licencyjnymi.
8. Strona internetowa musi posiadać politykę prywatności określającą cele wykorzystania cookies.
9. Strona internetowa musi posiadać mechanizmy umożliwiające wyłączenie cookies podczas korzystania z niej.

10. Strona internetowa musi spełniać wymagania określone w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
11. W przypadku, gdy strona internetowa zawiera odwołania do zewnętrznych serwisów, które znajdują się poza kontrolą Centrum, wymagana jest okresowa weryfikacja poprawności tych odwołań, ze szczególnym uwzględnieniem dostępności serwisów zewnętrznych i ich bezpieczeństwa, a w razie potrzeby, podejmowanie działań korekcyjnych.
12. W przypadku możliwości wprowadzania danych przez użytkownika zewnętrznego, w tym za pomocą formularzy, musi być stosowany mechanizm reCAPTCHA lub inny mechanizm zapewniający ochronę przed masowym wprowadzaniem danych.
13. Zakres danych wprowadzanych przez użytkownika musi być ograniczony do minimum niezbędnego do realizacji celu przetwarzania. Możliwość wprowadzania dodatkowych danych przez użytkownika musi być opcjonalna.
14. Strona internetowa musi publikować klauzule informacyjne w związku z przetwarzaniem danych osobowych użytkownika, zawierające wszystkie wymagane dane zgodnie z art. 13 RODO.
15. Jeżeli przetwarzanie danych wprowadzonych przez użytkownika wymaga jego zgody, strona internetowa musi posiadać mechanizm umożliwiający potwierdzenie zgody przez użytkownika (np. check-box), przy czym:
    a. Domyślny stan mechanizmu musi oznaczać brak zgody;
    b. Zgody nie mogą być łączone, a wyrażenie każdej zgody musi wymagać oddzielnego działania użytkownika.
16. Konta administracyjne CMS muszą umożliwiać zastosowanie mechanizmu dwuetapowej weryfikacji (2FA) podczas logowania
17. Hasła kont logujących się do systemu CMS muszą być przechowywane w sposób bezpieczny, z zastosowaniem funkcji hash-ujących zgodnych z aktualnymi standardami (np. bcrypt, Argon2).
18. System CMS musi wymuszać stosowanie silnych haseł zgodnych z polityką bezpieczeństwa Centrum
19. System CMS musi umożliwiać ochronę logowania przed atakami typu brute force (np. blokada po kilku nieudanych próbach logowania możliwa do zdjęcia po określonym czasie)
20. System CMS i serwer webowy musi być skonfigurowany w taki sposób, aby minimalizować ryzyko ataków typu XSS, CSRF, i SQL Injection, poprzez implementację odpowiednich nagłówków bezpieczeństwa HTTP (np. Content Security Policy, X-Frame-Options, X-Content-Type-Options).
21. Strona powinna być zbudowana jedynie z użyciem wtyczek i motywów pochodzących z zaufanych źródeł, które są regularnie aktualizowane i audytowane pod kątem bezpieczeństwa (min 1 raz w roku).
22. Strona internetowa musi być objęta mechanizmem monitorowania i logowania działań użytkowników administracyjnych oraz zdarzeń systemowych.

23. Strona internetowa musi mieć możliwość udostępniania logów do systemu typu SIEM.
24. Logi muszą być zabezpieczone przed modyfikacją i usunięciem, również przez osoby posiadające uprawnienia administratora w systemie CMS
25. Wymagane jest stosowanie mechanizmu HSTS (HTTP Strict Transport Security), aby wymusić połączenia HTTPS.
26. Wszystkie dane przesyłane pomiędzy użytkownikiem a serwerem powinny być szyfrowane i chronione przed manipulacją.
27. System CMS musi posiadać granularny mechanizm zarządzania uprawnieniami, umożliwiający przypisywanie użytkownikom minimalnych niezbędnych uprawnień zgodnie z zasadą least privilege.
28. Strona internetowa musi być zabezpieczona przed najczęściej występującymi zagrożeniami według (aktualnego na dzień wystawienia ogłoszenia o przetargu) projektu OWASP Top 10
29. Strona musi być zaprojektowana i wykonana zgodnie z (aktualnym na dzień wystawienia ogłoszenia o przetargu) standardem ASVS level 1 lub wyższym
30. Wszelkie zewnętrzne usługi i API wykorzystywane przez stronę internetową muszą obsługiwać bezpieczne protokoły komunikacji (np. OAuth 2.0, HTTPS).
31. Integracje z zewnętrznymi serwisami muszą być objęte monitoringiem i wcześniejszą oceną ryzyka przez Zamawiającego.
32. Strona internetowa musi zostać poddana testom bezpieczeństwa przed jej uruchomieniem (testy penetracyjne i audyt kodu) oraz cyklicznie po wdrożeniu istotnych zmian.
33. Wyniki testów muszą zostać udokumentowane i przekazane zamawiającemu. Wyniki powinny jasno wskazywać, że strona została wykonana zgodnie z wcześniej wspomnianymi praktykami i zasadami.
34. Wykonawca zapewni pełną izolację środowiska hostingowego (np. poprzez LVE lub konteneryzację) uniemożliwiającą dostęp między instancjami.
35. Wykonawca zapewni i skonfiguruje zaporę sieciową Web Application Firewall (WAF) do filtrowania ataków SQLi, XSS oraz exploitów na wtyczki.
36. Wykonawca zapewni stałą ochronę przed atakami typu Denial of Service.
37. Wykonawca przeprowadzi skan podatności CMS, wtyczek i motywów przed uruchomieniem produkcyjnym (Go-Live) oraz cyklicznie raz w miesiącu.
38. Wykonawca zleci wykonanie testu penetracyjnego (zgodnie z OWASP WSTG) przed Go-Live oraz cyklicznie minimum raz w roku.
39. Wykonawca zapewni regularne skanowanie podatności warstwy serwerowej i bazy danych (minimum raz w miesiącu).
40. Podatności krytyczne muszą zostać usunięte w ciągu maksymalnie 14 dni od wykrycia lub wydania poprawki przez producenta.
41. Podatności o wysokim priorytecie muszą zostać usunięte w ciągu maksymalnie 30 dni roboczych.
42. Podatności o średnim priorytecie muszą zostać usunięte w ciągu maksymalnie 60 dni roboczych.

43. Podatności o niskim priorytecie muszą zostać usunięte w ciągu maksymalnie 90 dni roboczych.
44. Wykonawca zobowiązany jest do niezwłocznego informowania Zamawiającego o każdym stwierdzonym incydencie informatycznym lub uzasadnionym podejrzeniu naruszenia bezpieczeństwa informatycznego.
45. Powiadomienie musi nastąpić w czasie nie dłuższym niż 5 godzin od wykrycia incydentu o statusie krytycznym oraz 24 godziny dla pozostałych zdarzeń.
46. Każde zgłoszenie musi zawierać: opis charakteru incydentu, wskazanie zagrożonych zasobów, przewidywane skutki oraz podjęte działania naprawcze.
47. Wykonawca wyznaczy i poda do wiadomości Zamawiającego osobę (lub zespół) odpowiedzialną za koordynację obsługi incydentów.
48. Wykonawca będzie prowadził rejestr wszystkich incydentów oraz prób naruszeń i udostępniał go Zamawiającemu na żądanie.

11. Hosting i utrzymanie (RUN)

11.1. Monitoring i obserwowalność

Wykonawca zapewni ciągły monitoring dostępności Systemu w trybie 24/7/365 z interwałem badania nie dłuższym niż 60 sekund z co najmniej dwóch niezależnych punktów pomiarowych, gwarantując bezzwłoczne wykrywanie przerw w działaniu serwisu oraz błędów krytycznych uniemożliwiających korzystanie z jego funkcji. W ramach świadczonej usługi Wykonawca zobowiązany jest do utrzymywania systemu powiadomień o awariach, który dla incydentów o najwyższym priorytecie (całkowity brak dostępności strony) zapewni powiadomienie Zamawiającego drogą elektroniczną natychmiast po wystąpieniu zdarzenia, a dla pozostałych błędów w czasie do 30 minut w godzinach wsparcia technicznego. Ponadto Wykonawca zapewni rejestrowanie i przechowywanie logów audytowych dotyczących aktywności użytkowników w panelu administracyjnym oraz zmian w treściach strony przez okres minimum 180 dni, zapewniając ich dostępność na żądanie Zamawiającego.

11.2. Kopie zapasowe i odtwarzanie (DR)

Wykonawca jest zobowiązany do wykonywania codziennych kopii zapasowych całego Systemu (bazy danych oraz plików) i ich przechowywania przez okres minimum 30 dni w bezpiecznej, zewnętrznej lokalizacji. Proces ten musi gwarantować, że w przypadku awarii maksymalna utrata danych nie przekroczy 1 godziny (RPO), a pełna sprawność serwisu zostanie przywrócona w czasie nie dłuższym niż 4 godziny (RTO). Raz na kwartał Wykonawca przeprowadzi testowe odtworzenie Systemu z kopii zapasowej i przekaże Zamawiającemu potwierdzenie spójności danych oraz gotowości do przywrócenia usług. Wszystkie kopie zapasowe muszą być przygotowane w sposób umożliwiający ich bezkosztowe przekazanie Zamawiającemu w formatach otwartych (np. SQL dla baz danych), co zapewni pełną swobodę migracji serwisu do środowiska IaaS po zakończeniu współpracy.

12. Gwarancja, SLA i wsparcie

12.1. Rozdzielenie pojęć

Gwarancja dotyczy naprawy błędów wytworzonych w BUILD. Utrzymanie (RUN) dotyczy operacji i dostępności. Rozwój dotyczy zmian (CR) poza zakresem gwarancji.

12.2. Wariant SLA

SLA: wsparcie 8/5 (dni robocze 08:00–16:00) dla P2, P3 i P4, obsługa P1 24/7.

12.3. Klasy incydentów eksploatacyjnych i czasy reakcji

Priorytet	Definicja	Czas reakcji	Czas obejścia/naprawy
P1 – Krytyczny	Incydent powodujący całkowitą niedostępność środowiska produkcyjnego albo brak możliwości korzystania z podstawowej funkcjonalności usługi przez wszystkich lub zdecydowaną większość użytkowników. Incydent uniemożliwia realizację kluczowych procesów biznesowych i nie istnieje skuteczne, akceptowalne operacyjnie obejście.	≤ 5 min	≤ 1 h (obejście) / ≤ 24 h (naprawa)
P2 – Wysoki	Incydent powodujący istotną degradację działania usługi lub niedostępność kluczowej podstron serwisu w szczególności Zakładki z Konkursami NCBR, Strony głównej, Zamówień Publicznych. Problem	≤ 30 min (w godz. wsparcia)	≤ 4 h (obejście) / ≤ 3 dni robocze (naprawa)

	dotyczy istotnej grupy użytkowników.		
P3 – Średni	Incydent nieblokujący działania usługi w całości, lecz powodujący błędne lub ograniczone działanie wybranych funkcji. Problem może dotyczyć części użytkowników lub wybranych scenariuszy użycia, przy czym istnieje możliwe do zastosowania obejście pozwalające na kontynuację pracy z akceptowalnymi utrudnieniami.	≤ 4 h (w godz. wsparcia)	≤ 10 dni roboczych
P4 – Niski	Incydent o niewielkim wpływie na działanie usługi, w szczególności drobna usterka, błąd wizualny, jednostkowa nieprawidłowość lub problem niewpływający istotnie na ciągłość procesów biznesowych. Zgłoszenia o charakterze rozwojowym lub usprawnienia nie stanowią incydentów i są obsługiwane w odrębnym trybie backlogu lub zarządzania zmianą.	≤ 1 dzień roboczy	Uzgodniony termin w backlogu

Po wdrożeniu skutecznego obejścia priorytet incydentu może zostać zweryfikowany i odpowiednio obniżony, jeżeli rzeczywisty wpływ incydentu na działanie usługi i procesy biznesowe został istotnie ograniczony. Ostateczna klasyfikacja incydentu powinna uwzględniać

jego faktyczny wpływ biznesowy, skalę oddziaływania, dostępność obejścia oraz krytyczność funkcji, której incydent dotyczy.

12.4. Raportowanie SLA

- Raport miesięczny: dostępność, liczba incydentów, czasy MTTA/MTTR, wykonane aktualizacje, wyniki testów backup/restore.
- Raport kwartalny: analiza trendów, rekomendacje optymalizacji, przegląd ryzyk i plan działań.

13. Zarządzanie zmianą (Change Request) i prace rozwojowe

Kanał: rejestr CR w systemie ticketowym/backlogu. Każda zmiana ma opis, wpływ, koszt, termin i ryzyka. Rozróżnienie: „błąd" (w ramach gwarancji/SLA) vs „zmiana" (CR płatny).

W ramach realizacji prac rozwojowych Zamawiający przewiduje zlecenia w wymiarze od 30 do maksymalnie 100 roboczogodzin.

W ramach realizacji prac rozwojowych Zamawiający przewiduje w odpowiedzi na zapytanie Zamawiającego Wykonawca w terminie do 3 dni roboczych (lub w innym uzgodnionym przez Strony terminie) przeanalizuje zlecenie i prześle informację zwrotną uwzględniającą informacje techniczne, szacunkową wycenę zleconych prac wraz z możliwym terminem ich realizacji, z zastrzeżeniem że w przypadku konieczności doszczegółowienia przez Zamawiającego informacji przekazanych w zapytaniu, pytanie skierowane przez Wykonawcę do Zamawiającego zatrzymuje bieg terminu.

Zamawiający przeanalizuje i potwierdzi akceptację pracochłonności oraz termin wykonania zlecenia nie później niż 3 dni robocze od otrzymania wyceny przez Wykonawcę.

Termin realizacji prac weekendowych oraz poza godzinami pracy zgłaszany będzie z co najmniej 7-dniowym wyprzedzeniem.

W przypadku zmiany zakresu bądź terminu przez Zamawiającego, wymagane jest potwierdzenie przez Wykonawcę możliwości realizacji wprowadzonych zmian lub rezygnacja ze zlecenia.

Fakt ryzyka przekroczenia szacowanych do realizacji roboczogodzin będzie zgłaszany w momencie wystąpienia takiej sytuacji, w celu podjęcia decyzji o akceptacji dodatkowych godzin przez koordynatora Zamawiającego.

Wykonawca rezerwuje sobie prawo do odrzucenia zlecenia w przypadku, w którym jest ono niemożliwe do zrealizowania z przyczyn technicznych, zgodności z dokumentacją producenta bądź dostępności zasobów w wyznaczonym przez Zamawiającego terminie.

Strony dopuszczają odbiór warunkowy prac realizowanych na podstawie zlecenia.

Strony postanawiają, iż w ramach zleceń – o ile będzie to możliwe ze względu na przedmiot zlecenia – przewidzą odbiory częściowe, w szczególności poszczególnych etapów realizacji zlecenia lub poszczególnych produktów realizacji danego zlecenia.

Po każdym miesięcznym okresie realizacji prac rozwojowych Zamawiający potwierdzi Protokołem Odbioru prawidłową realizację przez Wykonawcę zleconych prac. W tym celu Zamawiający dokonuje weryfikacji przedstawionych w Protokołu Odbioru wykazu prac i je akceptuje, bądź w ciągu 3 dni roboczych od otrzymania Protokołu Odbioru przekazuje Wykonawcy zastrzeżenia.

W przypadku potwierdzenia występowania zgłoszonych przez Zamawiającego błędów w wykonanych pracach, Wykonawca w uzgodnionym przez Strony terminie przystąpi do usuwania błędów w wykonanych pracach.

Wszelkie ustalenia szczegółowe dotyczące poszczególnych zleconych prac rozwojowych mogą być regulowane za porozumieniem Stron w ramach zlecenia, w szczególności sposób rozliczania prac, rozliczenia częściowe.

14. Migracja

14.1. Zakres

- Migracja treści i plików: strony, aktualności, grafika (.jpg, .png , .svg) dokumenty (.pdf, .docx, .xlsx, .zip) z aktualnego serwisu https://www.gov.pl/web/ncbr (oparta na scrapowaniu oryginalnego serwisu).
- Mapowanie URL: pełna lista starych URL → nowe URL; przekierowania 301.
- Szacowany wolumen danych do przeniesienia: ok. 50 GB.

14.2. Kryteria zaliczenia migracji

Obszar	Próg
Przekierowania	≥ 98% URL z listy migracyjnej ustalonej z Zamawiającym przekierowane 301 poprawnie; brak pętli redirect.
Błędy 404	≤ 0,5% żądań dla listy migracyjnej ustalonej z Zamawiającym; wszystkie 404 krytyczne poprawione przed Go-Live.
Kompletność treści	≥ 99% treści z listy migracyjnej ustalonej z Zamawiającym; brak utraty plików.

14.3. Plan powrotu (rollback)

Plan rollback obejmuje: przywrócenie DNS do starej wersji, odtworzenie backupu, utrzymanie przekierowań i komunikatów dla użytkowników.

15. Odbiory, testy i dowody odbiorowe

15.1. Plan testów (minimum)

- Testy funkcjonalne i regresja (na staging).
- Testy wydajnościowe (rozdz. 9.1) + raport.
- Testy dostępności (rozdz. 4.3 i 9.2) + raport audytu i retest.
- Testy bezpieczeństwa + raport.

15.2. Dowody odbiorowe (evidence)

Wykonawca przekazuje następujące artefakty jako dowody spełnienia wymagań (w formie elektronicznej, np. PDF/CSV/linki do pipeline):

- Raport Lighthouse CI/WebPageTest (z konfiguracją profilu i listą URL) z CWV.
- Raport audytu WCAG (automatyczny, np. Lighthouse Accessibility).
- Raport z testów obciążeniowych (parametry, wyniki p95/p99, wnioski).
- Raport ze skanu podatności, audytu kodu oraz raport z pentestu.
- Potwierdzenie testu odtworzenia backupu (czas, osiągnięte RPO/RTO).
- SBOM/rejestr komponentów (wtyczki/biblioteki/wersje/licencje).
- Runbook v1.0 oraz instrukcja wdrożenia/odtworzenia środowiska.

15.3. Warunki Go-Live

- Brak defektów krytycznych (blokujących) oraz brak podatności krytycznych; wysokie naprawione lub zaakceptowane z obejściem i terminem.
- Spełnienie KPI/SLO z rozdz. 4 (potwierdzone raportami).
- Backup wykonany i przetestowany (restore test) na staging.
- Monitoring i alerty skonfigurowane, w tym alerty P1/P2.
- Plan rollback zatwierdzony; osoby kontaktowe i ścieżka eskalacji ustalone.
- Dokumentacja operacyjna (runbook) przekazana w wersji 1.0.

15.4. Mechanika odbiorów, terminy i klasyfikacja wad

- Termin weryfikacji: Zamawiający weryfikuje przekazany etap/artefakt w terminie 10 dni roboczych od dnia jego dostarczenia wraz z kompletem dowodów odbiorowych.
- Zgłaszanie uwag: uwagi są przekazywane w systemie zgłoszeń lub w formie protokołu. Brak uwag w terminie oznacza odbiór warunkowy, chyba że Strony uzgodnią na piśmie przedłużenie terminu.
- Klasy wad: (i) wada krytyczna – uniemożliwia użytkowanie lub narusza bezpieczeństwo/dostępność/zgodność prawną; blokuje odbiór; (ii) wada istotna – istotnie

obniża funkcjonalność, ale istnieje obejście; może skutkować odbiorem warunkowym; (iii) wada nieistotna – kosmetyczna; nie blokuje odbioru.

- Odbiór warunkowy: dopuszczalny, jeżeli pozostają wyłącznie wady nieistotne lub istotne z zaakceptowanym obejściem i terminem naprawy.
- Rozróżnienie „błąd" vs „zmiana/CR": jeżeli funkcja/parametr wynika z SOPZ, zaakceptowanego backlogu lub specyfikacji i nie spełnia kryteriów – traktuje się to jako błąd w ramach gwarancji/SLA. Jeśli zmienia uzgodnione zachowanie lub wykracza poza zakres – jest to CR rozliczany odrębnie.

16. Przekazanie, dokumentacja i szkolenia

16.1. Wymagana dokumentacja

- Dokumentacja użytkowa (CMS): role, workflow, publikacja, wersjonowanie.
- Dokumentacja techniczna: architektura, komponenty, instrukcje wdrożenia, zależności.
- Runbook operacyjny: backup/restore, monitoring, aktualizacje, obsługa incydentów, kontakty, diagram zależności.

16.2. Szkolenia

Minimum: 2 sesje szkoleniowe dla administratorów i 2 sesje szkoleniowe dla redaktorów strony, nagrania i materiały PDF. Zamawiający dopuszcza możliwość szkoleń online i ma prawo nagrać szkolenie na potrzeby wewnętrzne. Dokładny zakres szkoleń do ustalenia.

17. Prawa autorskie, licencje i własność zasobów

17.1. Prawa do kodu i materiałów

Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do wytworzonych utworów (kod, grafiki, konfiguracje) w zakresie wymaganym do korzystania, modyfikacji i utrzymania. Repozytorium kodu prowadzone w narzędziu Zamawiającego.

17.2. Własność kont i dostępów

Konta (domena/DNS/analityka Google Analytics) należą do Zamawiającego. Wykonawca otrzyma role dostępowe na czas realizacji i utrzymania; dostęp jest niezwłocznie odbierany po zakończeniu umowy lub na żądanie Zamawiającego.

17.3. Rejestr komponentów (SBOM)

Wykonawca prowadzi i przekazuje aktualny rejestr komponentów (wtyczki/biblioteki/wersje/licencje) oraz wskazuje komponenty płatne i ich warunki licencyjne.

17.4. Zgodność licencyjna i aktualizacja SBOM

- Wykonawca oświadcza, że przekazywany kod i konfiguracje nie naruszają praw osób trzecich oraz że wykorzystane komponenty open-source są użyte zgodnie z ich licencjami.

- Komponenty o licencjach copyleft (np. GPL) mogą być użyte wyłącznie po uprzednim poinformowaniu Zamawiającego i zaakceptowaniu wpływu na dystrybucję i utrzymanie.
- SBOM/rejestr komponentów jest aktualizowany co najmniej przy każdym wdrożeniu na produkcję oraz w ramach miesięcznych aktualizacji w RUN. Rejestr wskazuje wersje, licencje, krytyczność podatności i status aktualizacji.

18. Plan wyjścia (Exit plan) i ciągłość działania

18.1. Przekazanie systemu

Wykonawca jest zobowiązany do zaprojektowania i utrzymywania usługi w architekturze i w standardach umożliwiających jej pełne przejęcie przez Zamawiającego lub podmiot trzeci, np. w architekturze kontenerowej. Ma to na celu zapewnienie ciągłości działania serwisu oraz niezależności technologicznej Zamawiającego.

Podczas trwania Umowy Wykonawca będzie przekazywał elementy wymienione w pkt. 18.2 co kwartał dla Zamawiającego.

Aby przygotować system do pełnego przejęcia przed zakończeniem umowy, elementy wymienione w pkt. 18.2 zostaną przekazane do testów na 4 miesiące przed jej zakończeniem.

18.2. Zakres przekazania przy zakończeniu umowy

Zakres przekazanych elementów systemu:

- Kod źródłowy (repo), pipeline CI/CD (konfiguracje), dokumentacja i runbook.
- Aktualne dane/pliki konieczne do wdrożenia.
- Backupy: baza danych (dump), pliki/załączniki, konfiguracje – w uzgodnionych formatach.
- Lista kont i dostępów, instrukcja odtworzenia środowiska, SBOM i licencje.
- W przypadku architektury kontenerowej:
    - Kompletna konfiguracja konteneryzacji: pliki definicji obrazów (np. Dockerfile), pliki orkiestracji środowisk (np. Helm charts, Kubernetes manifests lub docker-compose) umożliwiające odtworzenie pełnego stosu technologicznego.
    - Obrazy kontenerów: dostęp do prywatnego rejestru obrazów lub przekazanie obrazów w formie plików (np. format .tar), gotowych do wdrożenia w wersji produkcyjnej.

18.3. Terminy i wsparcie

Wykonawca zapewnia wsparcie migracyjne przez 60 dni od daty zakończenia świadczenia usługi hostingu. Rozliczenie wsparcia: [stawka/h] lub ryczałt [kwota].