

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest **świadczenie usług wsparcia oraz usług rozwoju Systemu Zarządzania Ryzykiem**.

Zamawiający posiada Systemu Zarządzania Ryzykiem – BPM w wersji 5.0 (Link do strony producenta: <https://www.grupablue.pl/system-zarzadzania-ryzykiem/>) wraz z zainstalowanymi modułami (zwanym dalej Systemem).

Wykonywanie poszczególnych zadań polega na realizacji zleceń/zgłoszeń Zamawiającego (zwanym zleceniami lub zgłoszeniami).

I. Usługa wsparcia Systemu i dostawa licencji – wymagania jakościowe i techniczne

1. Usługa wsparcia Systemu będzie polegać na:

- 1.1. diagnozowaniu Systemu,
- 1.2. usuwaniu Błędów,
- 1.3. wgrywaniu poprawek dla eksploatowanych środowisk wykorzystujących System,
- 1.4. upgrade i podnoszenie do najnowszej bezpiecznej stabilnej wersji Systemu wraz z modułami oraz dostawą licencji na czas nieokreślony bez limitu ilości użytkowników dla środowiska produkcyjnego i szkoleniowego,
- 1.5. ocenie możliwości zastosowania poprawek rekomendowanych przez producenta oprogramowania w eksploatowanych środowiskach oraz informowaniu Zamawiającego o możliwości ich wdrożenia,
- 1.6. doradztwie architektonicznym w zakresie zgodności sposobu wykorzystywania Oprogramowania z najlepszymi praktykami rekomendowanymi przez dostawcę oraz zgodności z warunkami Umowy,
- 1.7. doradztwie technicznym i implementacyjnym w zakresie adaptacji nowych lub istotnie zmodyfikowanych wersji Oprogramowania (tj. wersje główne Oprogramowania oraz zestawy poprawek - tzw. Patches) lub migracji środowisk,
- 1.8. informowaniu Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu,
- 1.9. założeniu zgłoszenia serwisowego w serwisie pomocy technicznej producenta, w przypadku wad i błędów Oprogramowania składającego się na System, przekazanie zgłoszenia serwisowego do producenta oprogramowania oraz prowadzenie zgłoszenia w imieniu Zamawiającego,
- 1.10. instruktażu uwzględniającym nowe funkcjonalności po aktualizacji Systemu, aktualizacja dokumentacji technicznej Systemu,
- 1.11. doradztwie technicznym, przekazywaniu na bieżąco informacji o nowych funkcjonalnościach możliwych do zaimplementowania w Systemie,
- 1.12. wsparciu w konfiguracji i optymalizacji Systemu,

- 1.13. aktualizacji/modyfikacji Systemu w przypadku zmian w aktach prawa powszechnie obowiązującego lub wewnętrznych regulacji po wcześniejszym uzgodnieniu ich z Wykonawcą w celu weryfikacji możliwości technicznych dostosowania systemu do planowanej zmiany.
 - 1.14. Wykonawca, w terminie do 7 dni roboczych poinformuje Zamawiającego o wydaniu nowej wersji lub poprawek bezpieczeństwa Systemu, za pośrednictwem komunikacji mailowej lub dedykowanej platformy do obsługi zleceń.
2. Usługa wsparcia:
 - 2.1. musi być prowadzona w języku polskim,
 - 2.2. będzie realizowana na żądanie Zamawiającego zgłoszone w formie elektronicznej lub telefonicznej.
 3. Przyjęcie Zgłoszenia przez Wykonawcę musi być potwierdzone w formie pisemnej lub elektronicznej (poczta elektroniczna).
 4. Zgłoszenia będą dokonywane w dni robocze w godzinach roboczych 8:00-17:00.
 5. Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji Błędów.
 6. Naprawy i prace konfiguracyjne Systemu będą świadczone w siedzibie Zamawiającego w terminach wskazanych w Tabeli w pkt 7 Umowy lub zdalnie po wcześniejszym zatwierdzeniu przez Zamawiającego.
 7. Wykonawca jest zobowiązany do świadczenia poziomu usług oznaczającego zobowiązanie Wykonawcy do dotrzymania poniżej przedstawionych parametrów czasowych w przypadku problemów dotyczących funkcjonowania Systemu:

L.p.	Kategoria zgłoszenia	Czas reakcji na zgłoszenie (od momentu otrzymania zgłoszenia)	Czas rozwiązania zgłoszenia (od momentu reakcji na zgłoszenie)
1.	Błąd Krytyczny	4 godziny robocze	3 dni robocze
2.	Błąd zwykły	24 godziny robocze	14 dni robocze
3.	Pozostałe zgłoszenia	24 godziny robocze	28 dni robocze z możliwością przedłużenia za zgodą Zamawiającego

8. Wykonawca po naprawie Błędu sprawdzi skuteczność i uzyska potwierdzenie od Zamawiającego.
9. Za moment rozwiązania zgłoszenia (naprawy Błędu) uznaje się datę przywrócenia pełnej wydajności i funkcjonalności Systemu lub uzyskania potwierdzenia Zamawiającego.
10. W przypadku, o którym mowa w pkt 1.4 oraz 1.13 Wykonawca, na pisemne zlecenie Zamawiającego (przekazane za pomocą poczty elektronicznej lub dedykowanej platformy do obsługi zleceń),

w terminie do 21 dni roboczych od daty przekazania zlecenia, wykona aktualizację/ modyfikację/ upgrade Systemu.

II. Usługa Rozwoju Systemu

W okresie obowiązywania Umowy Zamawiający może zamówić u Wykonawcy wykonanie zleceń wg bieżących potrzeb Zamawiającego, w ramach dostępnej puli godzin, których łączna liczba nie przekroczy 200 Roboczogodzin. Wykonawcy przysługuje wynagrodzenie jedynie za faktycznie zleconą i zrealizowaną liczbę Roboczogodzin w ramach wykonanych i odebranych przez Zamawiającego Zleceń.

1. Usługa Rozwoju będzie polegać na:

- 1.1. wsparciu w rozwoju Systemu i jego dokumentowanie,
 - 1.2. konsultacje w ramach rozwijania komunikacji Systemu z innymi systemami w środowisku Zamawiającego,
 - 1.3. konsultacje i implementacja nowych metod optymalizacji systemów Zamawiającego w zakresie funkcjonalności oferowanych przez System,
 - 1.4. inne prace wg. potrzeb Zamawiającego (w uzgodnieniu z Wykonawcą) dotyczących rozwoju Systemu,
 - 1.5. dokonywanie zmian i ich wdrażanie w konfiguracji i funkcjonalnościach Systemu,
 - 1.6. przygotowanie instrukcji i innych zleconych dokumentów ułatwiających wykonywanie czynności dla użytkowników Systemu, innych niż wskazane w OPZ,
 - 1.7. przygotowanie skryptów automatyzujących działania użytkowników i administratorów, oraz procedur postępowania i instrukcji, dostarczenia skryptów, plików wykonywalnych, bibliotek itp. wymaganych do wprowadzania zmian w ramach rozwoju Systemu.
2. Wykonawca jest zobowiązany do wykonania Usług z należytą starannością zgodnie ze standardami obowiązującymi w branży informatycznej.
 3. Usługi, o których mowa w pkt 1., realizowane będą przez Wykonawcę na podstawie pisemnych lub elektronicznych zleceń/zgłoszeń składanych przez Zamawiającego poprzez np. system wsparcia udostępniony przez Wykonawcę („zlecenie”).
 4. Rozliczenie wsparcia realizowane będzie realizowane w ujęciu miesięcznym.
 5. Rozliczenie rozwoju realizowane będzie poprzez rozliczanie godzinowe z dokładnością do każdych pełnych 15 minut i zgodnie ze stawką za roboczogodzinę zawartą w ofercie Wykonawcy.
 6. Wykonawca jest zobowiązany wyszczególnić na każdej fakturze z podziałem na usługi wsparcia oraz osobno usługi rozwoju.

7. Przyjęcie zlecenia przez Wykonawcę musi być potwierdzone w formie pisemnej lub elektronicznej w systemie wsparcia.
8. Zgłoszenia będą dokonywane w dni robocze w godzinach roboczych 8:00-17:00.
9. Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji zleceń oraz udostępnienia ich ewidencji na każde żądanie Zamawiającego.
10. Zamawiający po przeprowadzeniu uzgodnień, zgodnie ze zleceniem:
 - 10.1. potwierdzi Wykonawcy udzielenie zlecenia i Strony podpiszą zlecenie lub
 - 10.2. poinformuje Wykonawcę o odstąpieniu od udzielenia zlecenia wraz z podaniem przyczyny.
11. Zamawiający zastrzega, iż rozliczeniu będą podlegały jedynie zlecenia zrealizowane na warunkach wynikających z ich treści. Wszelkie działania podjęte przez Wykonawcę wykraczające poza warunki Zleceń nie będą podlegały rozliczeniu.
12. Prawidłowe zrealizowanie zlecenia, w tym rzeczywista liczba wykorzystanych Roboczogodzin potwierdzona będzie przez Zamawiającego w Protokole Odbioru zlecenia zgodnie z zapisami Umowy.
13. Jeżeli po podpisaniu zlecenia wystąpią okoliczności, które powodują, że konieczna jest zmiana wymagań wskazanych w zleceniu, wówczas Strony zaakceptują uzgodniony Aneks do zlecenia na warunkach zgodnie z zapisami Umowy.

III. Wymagania dodatkowe stawiane wykonawcy w związku z wymaganym doświadczeniem i kompetencjami zespołu wdrożeniowego

14. Wykonawca musi być autoryzowanym i certyfikowanym partnerem producenta proponowanego rozwiązania lub producentem tego rozwiązania.
15. Wykonawca musi przedłożyć co najmniej trzy pozytywne referencje, wystawione dla wykonawcy dostawcy proponowanego rozwiązania wdrożonego u dostawców usług kluczowych w zakresie analogicznym do przedmiotu niniejszego postępowania w okresie ostatnich 2 lat.

Załączniki:

Załącznik nr 1 – Opis funkcjonalności Systemu do zarządzania ryzykiem

Załącznik nr 2 – Warunki rozwoju Systemu

OPIS FUNKCJONALNOŚCI SYSTEMU DO ZARZĄDZANIA RYZYKIEM (RM)

- 1.1. Zgodność z aktualnymi wersjami norm ISO: 31000, 27005, 27001, 22301, 27002, 27799.
- 1.2. Zgodność z RODO - Rozporządzeniem 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.
- 1.3. Zgodność z obowiązującą Ustawą o krajowym systemie cyberbezpieczeństwa wraz z rozporządzeniami szczególnie w kontekście zakresu obowiązków Operatora Usługi Kluczowej.
- 1.4. Zgodność z wymaganiami audytu oceny Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa w zakresie zgodności z Ustawą o krajowym systemie cyberbezpieczeństwa (Ustawa z dnia 05 lipca 2018 Dz.U. 2018 poz. 1560¹), szczególnie (ale nie tylko) w zakresie zarządzania ryzykiem (Obszar 3) – zgodnie z szablonem opublikowanym przez Ministerstwo Cyfryzacji 28 kwietnia 2020 r. – Załącznik nr 1².
- 1.5. Art. 226 Ustawy z dnia 26.04.1974 r. Kodeks pracy (Dz.U. Nr 21, poz. 94 z późn. zm.) - Pracodawca ocenia i dokumentuje ryzyko zawodowe związane z wykonywaną pracą oraz stosuje niezbędne środki profilaktyczne zmniejszające ryzyko, informuje pracowników o ryzyku zawodowym, które wiąże się z wykonywaną pracą, oraz o zasadach ochrony przed zagrożeniami.
- 2.1. System do zarządzania ryzykiem uwzględnia podział ról w procesie zarządzania ryzykiem wraz z możliwością konfiguracji i dostosowania do potrzeb wynikających z danego obszaru. System umożliwia również powiązanie kont użytkowników z domeną Active Directory poprzez zarządzanie uprawnieniami na podstawie RBAC – (Role-Based Access Control).
- 2.2. System do zarządzania ryzykiem umożliwia sprawne zarządzanie dużą liczbą ryzyk (najmniej jeden tysiąc), z podziałem na obszary działania, role, dopasowane do struktury organizacyjnej Centrum-e-zdrowia, procesy i komórki organizacyjne oraz samodzielne stanowiska pracy.
- 2.3. System do zarządzania ryzykiem:
 - 2.3.1. umożliwia implementację i wspomaga metodykę zarządzania ryzykiem w celu zapewnienia zgodności z wymaganiami audytu w zakresie zarządzania ryzykiem Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa w zakresie zgodności z Ustawą o krajowym systemie cyberbezpieczeństwa, szczególnie – zgodnie z szablonem opublikowanym przez Ministerstwo Cyfryzacji 28 kwietnia 2020 r.², w tym również zapewniać symultaniczną obsługę procesów zarządzania ryzykiem adekwatną dla zakresów poszczególnych Usług Kluczowych w organizacji.
 - 2.3.2. umożliwia tworzenie i definiowanie metodyk zarządzania ryzykiem (w oparciu o różne wzory i mechanizmy) dostosowanych do obszarów i poszczególnych kontekstów i atrybutów, w tym m.in. atrybutów bezpieczeństwa informacji, jak poufność, integralność, dostępność, autentyczność, oraz zabezpieczeń, krytyczności. W szczególności system umożliwia dowolne agregowanie podstawowych aktywów

¹ <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560>

² <https://mc.bip.gov.pl/krajowy-system-cyberbezpieczenstwa/operatorzy-uslug-kluczowych/szablon-sprawozdania-z-audytu-zgodnego-z-ustawa-o-krajowym-systemie-cyberbezpieczenstwa.html>

organizacji wprowadzonych do systemu, stosowanie wobec w/w agregacji innych metodyk zarządzania ryzykiem w celu odwzorowania specyficznych procesów biznesowych.

- 2.3.3. umożliwia realizację analizy ryzyka w bezpieczeństwie informacji zgodnie z aktualną wersją norm ISO: 27005 oraz 27001 – w zakresie możliwości mitygacji ryzyk, stosownie do mechanizmów zabezpieczających.
- 2.3.4. umożliwia uwzględnienie zastosowania kontekstu organizacyjnego dla każdego ze zdefiniowanych i konfigurowalnych obszarów (maksymalna wymagana ilość obszarów to 200). Kluczowym jest obszar Departamentu Bezpieczeństwa Teleinformatycznego w tym cyberbezpieczeństwa, bezpieczeństwa informacji.
- 2.3.5. umożliwia prowadzenie rejestru ryzyk, wraz z możliwością śledzenia i przeglądu historii ryzyk – w tym historię każdego ryzyka z osobna, zarówno w procesie przeglądu jak i szacowania, analizy ryzyka,
- 2.3.6. umożliwia komunikację pomiędzy uczestnikami zaangażowanymi w proces zarządzania ryzykiem, polegającą na wysyłaniu powiadomień do osób odpowiedzialnych w procesie zarządzania ryzykiem o pojawiających się zadaniach do realizacji czy wprowadzonych analizach, szacowaniach gotowych do akceptacji,
- 2.3.7. umożliwia wyznaczanie poziomu tolerancji ryzyka oraz umożliwia definiowanie i wybór planów oraz sposobów postępowania z ryzykiem w odniesieniu do wyznaczonej tolerancji, poprzez posiadanie funkcjonalności, w której będzie można definiować takie plany, przypisywać osoby odpowiedzialne, rejestrować zadania, śledzić postępy, wysyłać powiadomienia,
- 2.3.8. umożliwia szacowanie i ocenę ryzyk z analizą skuteczności mechanizmów kontrolnych,
- 2.3.9. umożliwia przeprowadzenie procesu szacowania ryzyka w kontekście zasadności instalacji systemów: przeciwpożarowego, systemu podtrzymania i stabilizacji energii elektrycznej, zabezpieczeń alarmowego i antynapadowego, instalacji systemu zabezpieczeń (drzwi / okna / ściany), podtrzymania warunków temperatury, wilgotności i wentylacji pomieszczeń.
- 2.3.10. ma możliwość tworzenia diagramów procesów BPMN³ o stopniu szczegółowości biznesowej,
- 2.3.11. ma dołączone diagramy BPMN z wdrożonych w nim procesów zarządzania ryzykiem oraz zapewnia ich edycję wraz z rozwojem i dostosowywaniem metodyki do potrzeb.
- 2.3.12. umożliwia prowadzenie kart ryzyk,
- 2.3.13. w ramach konfiguracji Systemu do zarządzania ryzykiem i dostosowywania umożliwia tworzenie i wiązanie formularzy wraz z relacjami,
- 2.3.14. umożliwia wizualizację ryzyk i analiz w postaci konfigurowalnych dashboardów z prezentowaniem na nich danych w formie tabelarycznej, wykresów czy opisów,
- 2.3.15. umożliwia automatyczne powiadomienia, monitory mailowe (m.in. przypomnienia o nadchodzących terminach, nowych ryzykach, incydentach, zdarzeniach, przekroczeniach poziomów ryzyk poza zdefiniowany poziom).

³ Business Process Model and Notation, BPMN (Notacja i Model Procesu biznesowego) – graficzna notacja służąca do opisywania procesów biznesowych. – (źródło: https://pl.wikipedia.org/wiki/Business_Process_Modeling_Notation)

- 2.3.16. umożliwia konfigurowalne, automatyczne wysyłane raporty (oraz na żądanie) – w definiowalnych interwałach czasowych,
- 2.3.17. umożliwia generowanie raportów z analizy ryzyk do formatów minimalnie: .XLSX, .PDF oraz do dashboardów w wersji graficznej.
- 2.3.18. umożliwia import danych do bibliotek, definicji, formularzy minimalnie z plików płaskich .txt oraz posiadać instrukcję i procedurę w języku polskim - jak realizować krok po kroku.
- 2.3.19. umożliwia import danych konfiguracyjnych w formie minimalnie płaskich tabel w plikach tekstowych.
- 2.3.20. umożliwia szacowanie wartości ryzyk, z predefiniowanymi, konfigurowalnymi słownikami i szablonami, metodami i wzorami potrzebnych do notacji.
- 2.3.21. umożliwia okresowe automatyczne generowanie predefiniowanych raportów w tym w formie graficznej, tabelarycznej, opisowej, również np. w formie prezentacji macierzy i map ryzyka.
- 2.3.22. umożliwia ocenę krytyczności procesów, zagrożeń ciągłości działania zgodnie z aktualną wersją ISO 22301
- 2.3.23. umożliwia opracowywanie i przygotowywanie raportów indywidualnych, poprzez m.in. filtrowanie danych ze względu na konfigurowalne kryteria i zdefiniowane kwerendy i zapytania.
- 2.3.24. umożliwia definiowanie, tworzenie i zapisywanie formularzy, skryptów i monitów wg konfigurowalnych parametrów.
- 2.3.25. umożliwia wprowadzanie i monitorowanie zdarzeń operacyjnych, incydentów w związku z bieżącą działalnością, oraz na tej podstawie m.in. umożliwiać wprowadzania planów działania,
- 2.3.26. umożliwia dokonanie szacowania ryzyk powiązanych ze zdarzeniami, incydentami, również w oparciu o zgromadzone dane historyczne,
- 2.3.27. instrukcja obsługi powinna być poza dostarczoną w pliku/plikach PDF oraz zaszyta w system w formie „dymków” lub podpowiedzi.
- 2.3.28. działa w środowisku Windows Server,
- 2.3.29. ma włączoną funkcję szyfrowania TLS 1.2, z udostępnionym przez Zamawiającego certyfikatem.
- 2.3.30. Silnik bazy danych Systemu jest oparty o aktualną i wspieraną wersję przez producenta MS SQL.
- 2.3.31. umożliwia śledzenie, audyt zmian w konfiguracji oprogramowania i bazy danych. Baza danych ma zaimplementowaną i włączoną funkcję audytu bazy danych, polegającą na rejestrowaniu działań wszystkich użytkowników.
- 2.3.32. po stronie klienta jest obsługiwany poprzez znane przeglądarki wiodących producentów i jest aktualizowany, aby w czasie trwania umowy zapewnić ciągłość działania poprzez m.in. wsparcie i obsługę (m.in. Edge, FireFox, Chrome).
- 2.3.33. posiada kreator umożliwiający dodawanie i konfigurowanie, parametrów, formularzy i ankiet w systemie nie wymagający wiedzy programistycznej.
- 2.3.34. umożliwia sprawną pracę dla najmniej 80 osób jednocześnie, z możliwością w przypadku nieobecności danego pracownika zastąpienia go innym.
- 2.3.35. jest wyposażony przez producenta w API, umożliwiające jego przyszłą integrację z

systemami zewnętrznymi i posiadać do niego czytelną dokumentację techniczną, umożliwiającą jego wykorzystanie przez developerów, m.in. do np. zasilania podatnościami, incydentami czy danymi z innych systemów bezpieczeństwa jak SIEM⁴, DLP⁵, EDR⁶, skaner podatności, antywirus, firewall⁷, itp., oraz ticketowych - Jira / Jira Service Desk.

2.3.36. ma możliwość eksportu danych, raportów z analiz do formatu Microsoft Excela oraz formatu PDF.

2.3.37. posiada możliwość rozwijania samodzielnie przez Zamawiającego rozwiązania m.in. przez dodawanie kolejnych obszarów zarządzania ryzykiem.

Załącznik nr 2 do OPZ

⁴ SIEM - to skrót od Security Information and Event Management

⁵ DLP - Data Loss Prevention

⁶ EDR (Endpoint Detection and Response)

⁷ firewall - rodzaj zapory sieciowej

Warunki rozwoju Systemu

W okresie obowiązywania Umowy Zamawiający może zamówić u Wykonawcy wykonanie zleceń wg bieżących potrzeb Zamawiającego, w ramach ogólnej dostępnej puli godzin, których łączna ilość nie przekroczy 200 Roboczogodzin. Zamawiającemu przysługuje prawo wykorzystania, w całości lub części, Roboczogodzin. Wykonawcy przysługuje wynagrodzenie jedynie za faktycznie zleconą i zrealizowaną ilość Roboczogodzin w ramach wykonanych i odebranych przez Zamawiającego Zleceń.

1. Wsparcie będzie realizowane przez okres 12 miesięcy w wymiarze 200 Roboczogodzin od dnia podpisania przez Zamawiającego od podpisania umowy i będzie polegać na:
 - 1.1. wsparciu w rozwoju Systemu i jego dokumentowanie,
 - 1.2. konsultacje w ramach rozwijania komunikacji Systemu z innymi systemami w środowisku Zamawiającego.
 - 1.3. konsultacje i implementacja nowych metod optymalizacji systemów Zamawiającego w zakresie funkcjonalności oferowanych przez System.
 - 1.4. inne prace wg. potrzeb Zamawiającego (w uzgodnieniu z Wykonawcą) dotyczących rozwoju Systemu.
 - 1.5. dokonywanie zmian i ich wdrażanie w konfiguracji i funkcjonalnościach Systemu w zakresie potrzeb Zamawiającego innych niż wymienione w załączniku nr 1 do OPZ - Warunki gwarancji,
 - 1.6. przygotowanie instrukcji i innych zleconych dokumentów ułatwiających wykonywanie czynności dla użytkowników Systemu, innych niż wskazane w OPZ,
 - 1.7. przygotowanie skryptów automatyzujących działania użytkowników i administratorów, oraz procedur postępowania i instrukcji, dostarczenia skryptów, plików wykonywalnych, bibliotek itp. wymaganych do wprowadzania zmian w ramach rozwoju Systemu.
2. Wykonawca jest zobowiązany do wykonania Usług z należytą starannością zgodnie ze standardami obowiązującymi w branży informatycznej.
3. Usługi, o których mowa w pkt 1., realizowane będą przez Wykonawcę na podstawie pisemnych lub elektronicznych zleceń składanych przez Zamawiającego poprzez np. system wsparcia udostępniony przez Wykonawcę.
4. Rozliczenie wsparcia i rozwoju realizowane będzie poprzez rozliczanie godzinowe z dokładnością do każdych pełnych 15 minut i zgodnie ze stawką za roboczogodzinę zawartą w ofercie Wykonawcy.
5. Przyjęcie zgłoszenia przez Wykonawcę musi być potwierdzone w formie pisemnej lub elektronicznej w systemie wsparcia.
6. Zgłoszenia będą dokonywane w dni robocze w godzinach roboczych 8:00-17:00.
7. Wykonawca jest zobowiązany do prowadzenia pełnej i szczegółowej ewidencji Zgłoszeń oraz udostępnienia ich ewidencji na każde żądanie Zamawiającego.
8. Zamawiający po przeprowadzeniu uzgodnień, zgodnie ze Zleceniem:
 - 8.1. potwierdzi Wykonawcy udzielenie Zlecenia i Strony podpiszą Zlecenie lub
 - 8.2. poinformuje Wykonawcę o odstąpieniu od udzielenia Zlecenia wraz z podaniem przyczyny.

9. Zamawiający zastrzega, iż rozliczeniu będą podlegały jedynie Zlecenia zrealizowane na warunkach wynikających z ich treści. Wszelkie działania podjęte przez Wykonawcę wykraczające poza warunki Zleceń nie będą podlegały rozliczeniu.
10. Prawidłowe zrealizowanie Zlecenia, w tym rzeczywista liczba wykorzystanych Roboczogodzin potwierdzona będzie przez Zamawiającego w Protokole Odbioru Zlecenia zgodnie z zapisami Umowy.
11. Jeżeli po podpisaniu Zlecenia wystąpią okoliczności, które powodują, że konieczna jest zmiana wymagań wskazanych w Zleceniu, wówczas Strony zaakceptują uzgodniony Aneks do Zlecenia na warunkach zgodnie z zapisami Umowy.