

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo Rozwoju i Technologii planuje uruchomienie postępowania przetargowego o udzielenie zamówienia publicznego na zakup usługi Call Center wraz z dedykowanym zespołem konsultantów na potrzeby Firmy Bezpiecznej Cyfrowo. Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego.

Opis Przedmiotu Zamówienia na

Świadczenie usługi Call Center wraz z dedykowanym zespołem konsultantów na potrzeby Firmy Bezpiecznej Cyfrowo

SŁOWNIK POJĘĆ I SKRÓTÓW

Termin / skrót	Wyjaśnienie
Dni robocze	Wszystkie dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej
IVR	Z ang. <i>Interactive Voice Response</i> - system w telekomunikacji, umożliwiający interaktywną obsługę osoby dzwoniącej
Konsultant	Osoba zaangażowana bezpośrednio w obsługę kontaktów po stronie Wykonawcy
Live chat (LC)	System umożliwiający Klientowi prowadzenie czatu tekstowego z konsultantem za pośrednictwem właściwego oprogramowania udostępnianego poprzez przeglądarkę internetową
Call Center (CC)	Usługa umożliwiająca obsługę połączeń przychodzących i wychodzących, obsługę LC oraz zgłoszeń zarejestrowanych poprzez formularz kontaktowy
FAQ	Opracowanie najczęściej rozwiązywanych problemów i zadawanych pytań wraz z odpowiedziami i wszelkimi informacjami umożliwiającymi przyszłą obsługę takich przypadków
MRiT	Ministerstwo Rozwoju i Technologii
Skrypt	Zaimplementowany w Systemie sposób obsługi Kontaktu. Skrypty mogą być wariantowe – wówczas ich przebieg zależy od zdarzeń i decyzji Konsultanta.
Sprawa	Problem lub zagadnienie, którego rozwiązania oczekuje Klient
Umowa	Umowa na świadczenie usługi Call Center oraz dedykowanego zespołu Konsultantów.
Utwór	Każdy wytwór umysłu, inwencja, ulepszenie, plan, projekt, dzieło, dokumentacja, film, opracowanie, wzory raportów, aktualizacje lub inne, utrwalone w jakiegokolwiek postaci, w szczególności w postaci dokumentu, tekstu, obrazu, wideo, audio lub innych materiałów, wykonanych przez Wykonawcę bądź jego podwykonawców, powstałe w wyniku wykonania umowy, w formie dokumentacji pisemnej, elektronicznej lub innej, stanowiące utwory w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych
Klient	Osoba korzystająca z usług zespołu Konsultantów.

1. WPROWADZENIE

Niniejszy dokument przedstawia szczegółowy opis przedmiotu zamówienia na usługę Call Center wraz z dedykowanym zespołem Konsultantów świadczących wsparcie dla zalogowanych użytkowników korzystających Biznes.gov.pl (serwisu dla przedsiębiorców, właścicieli firm oraz obsługujących ich profesjonalistów – księgowych, prawników, doradców podatkowych itp.). Postępowanie dotyczy obsługi usług z obszaru cyberbezpieczeństwa:

1. Usługa analityczna dojrzałości cyfrowej i cyberbezpieczeństwa firm
 2. Usługa pre-weryfikacji zgodności z zaleceniami NIS2
 3. Usługa pre-kwalifikacji dot. wymagań dla produktów z elementami cyfrowymi
- przez okres 4 miesięcy od dnia zawarcia umowy. Dokument powstał w oparciu o analizę realizowanych w MRiT procesów, obserwację funkcjonujących centrów kontaktu oraz wiedzę pozyskaną w wyniku doświadczeń płynących z działającej od 2011 usługi typu MCP (Multikanałowe Centrum Pomocy) w MRiT.

2. KONTEKST ZAMÓWIENIA

Program Firma Bezpieczna Cyfrowo to nowatorski program mający na celu wsparcie polskich przedsiębiorców w budowaniu kompetencji cyfrowych oraz podniesieniu poziomu cyberbezpieczeństwa w sektorze MŚP (małych i średnich przedsiębiorstw). Inicjatywa ta odpowiada na rosnące zagrożenia cyberatakami, wzmacniając stabilność obrotu gospodarczego oraz promując nowy standard ochrony danych w firmach.

Rozwój kompetencji cyfrowych wśród polskich przedsiębiorców, ze szczególnym naciskiem na cyberbezpieczeństwo.

Zwiększenie cyberbezpieczeństwa w sektorze MŚP oraz stabilności obrotu gospodarczego w Polsce.

Wprowadzenie nowego standardu cyberbezpieczeństwa w firmach, zapewniającego ochronę danych własnych oraz partnerów biznesowych.

Program składa się z dwóch głównych komponentów: edukacyjnego i certyfikacji. Każdy przedsiębiorca może bezpłatnie wziąć udział w etapie edukacyjnym, który obejmuje:

Diagnoza – ocena stanu cyberbezpieczeństwa firmy oraz umiejętności cyfrowych za pomocą specjalistycznej ankiety.

Edukacja – spersonalizowany raport, który wskazuje mocne strony firmy oraz obszary do poprawy, wraz z konkretnymi zaleceniami.

Doskonalenie – przedsiębiorcy realizują zalecenia z raportu, wprowadzając odpowiednie zabezpieczenia i udoskonalać swoje procedury.

Usługi polegają na wypełnieniu interaktywnego kwestionariusza, podzielonego na obszary tematyczne. Przedsiębiorca, korzystając z elektronicznej usługi dostępnej online, odpowiada na zadane pytania.

Po zakończeniu, na podstawie udzielonych odpowiedzi, automatycznie generowany jest spersonalizowany raport. Zawiera on zestaw rekomendacji/wskazówki dla przedsiębiorcy.

Wynik samooceny ma charakter wyłącznie informacyjny i nie wpływa na ewentualną decyzję certyfikacyjną.

Konsultanci odpowiadają na pytania i prowadzą doradztwo wykorzystując różne kanały komunikacyjne: telefon (w dni robocze od 8 do 17), Live Chat (w dni robocze od 8 do 17), lub formularz kontaktowy (24h na dobę). Usługi Call Center są świadczone w języku polskim i angielskim.

3. PRZEDMIOT ZAMÓWIENIA

Zamówienie obejmuje świadczenie usługi Call Center wraz z zapewnieniem dedykowanego zespołu konsultantów. Zakres prac dotyczy przyjmowanie zgłoszeń i udzielanie odpowiedzi przez Konsultantów Wykonawcy na pytania Klientów dotyczące kwestii związanych z użytkowaniem usług w ramach programu Firma Bezpieczna Cyfrowo oraz proaktywny kontakt i pomoc Klientom.

4. OPISY USŁUG – MINIMALNE ZAKRESY WYMAGAŃ DLA POSZCZEGÓLNYCH USŁUG

1. CZTEROMIESIĘCZNY PLAN REALIZACJI PRZEDMIOTU ZAMÓWIENIA

W ramach realizacji zamówienia Wykonawca zobowiązany jest do przygotowania w formie opisowej oraz graficznej planu realizacji przedmiotu zamówienia w okresie najbliższych czterech miesięcy uwzględniający rozwój świadczonych usług.

Wykonawca zobowiązany jest do przedstawienia planu działania obejmującego minimum:

1. Dostarczenia usługi spełniającej minimalne wymagania opisane w rozdziale 4.2 OPZ
2. Organizację zespołu składającego się minimum z 10 Konsultantów spełniającym warunki minimalne wskazane w rozdziale 4.4 OPZ.
3. Przygotowanie FAQ wskazanego w rozdziale 4.6 OPZ

2. UDOSTĘPNIENIE USŁUGI CALL CENTER

Udostępnienie usługi Call Center w oparciu o technologię chmurową (np. oprogramowanie działające w przeglądarce). Wymagania:

- przyłączenie usługi Call Center do sieci operatora lub operatorów współpracujących,
- udostępnienie minimum 10 stanowisk konsultantów (w tym min. 6 konsultantów pracujących jednocześnie) oraz dwóch stanowisk dla managerów,
- IVR z możliwością nagrywania własnych komunikatów,
- zarządzanie połączeniami przychodzącymi poprzez budowę schematów drzewa IVR (dni i godziny pracy Infolinii, konfiguracja kilku różnych opcji przed połączeniem z konsultantem),
- zarządzanie kolejką połączeń przychodzących z informacją o długości i liczbie oczekujących połączeń w kolejce,
- system udostępniający dane statystyczne, w szczególności:
 - liczbę połączeń odebranych i nieodebranych w ujęciu dziennym/miesięcznym,
 - czas oczekiwania w kolejce w ujęciu dziennym,
 - liczbę połączeń zrzucanych przez agenta,
- system do automatycznego nagrywania rozmów z możliwością ich eksportu do plików wav lub mp3,
- odbieranie i nawiązywanie połączeń głosowych,

- Live Chat - system umożliwiający Klientowi prowadzenie czatu tekstowego z konsultantem za pośrednictwem właściwego oprogramowania udostępnianego poprzez przeglądarkę internetową,
- formularz kontaktowy dostępny w trybie 24h na dobę.

3. USŁUGA WSPARCIA W ZAKRESIE WYPEŁNIANIA ANKIETY SAMOOCENY POZIOMU BEZPIECZEŃSTWA ORAZ REALIZACJI ZALECEŃ Z RAPORTU

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

- Uruchomienia, udostępnienia i świadczenia usługi wsparcia w zakresie wypełniania ankiety samooceny poziomu bezpieczeństwa oraz realizacji zaleceń z raportu (wprowadzania odpowiednich zabezpieczeń i pomagania udoskonalać procedury Przedsiębiorców). Ma ona polegać na wsparciu przedsiębiorców chcących zrealizować e-usługi z obszaru cyberbezpieczeństwa w serwisie Biznes.gov.pl oraz pomoc dla przedsiębiorców chcących wdrażać środki techniczne i organizacyjne wpływające na poprawę cyberbezpieczeństwa w firmie.
- Uruchomienia, udostępnienia i świadczenia usługi wsparcia w zakresie usługi pre-weryfikacji zgodności z zaleceniami NIS2 - e-usługa pozwoli ocenić, czy działalność firmy podlega regulacjom NIS2 i jak się do nich przygotować. Usługa pre-weryfikacji zgodności z NIS2 to kompleksowa ocena stanu cyberbezpieczeństwa firmy, mająca na celu identyfikację luk w porównaniu do wymagań unijnej dyrektywy, stworzenie mapy drogowej wdrożenia, a także pomoc w przygotowaniu do raportowania incydentów.
- Uruchomienia, udostępnienia i świadczenia usługi wsparcia w zakresie usługi pre-kwalifikacji dot. wymagań dla produktów z elementami cyfrowymi – e-usługa pozwoli zrozumieć wymagania zapewniające wyższy poziom cyberbezpieczeństwa i odporności produktów cyfrowych wynikające z Cyber Resilience Act i wdrożyć je w praktyce.

4. ZESPÓŁ KONSULTANTÓW

Na cele obsługi procesów Zamawiającego Wykonawca zbuduje zespół składający się z Konsultantów dedykowanych wyłącznie do wykonywania usługi. Wykonawca w godzinach pracy zapewni pracę ciągłą Call Center w każdej godzinie pracy infolinii (dni robocze 8-17). Wykonawca zapewni optymalny rozkład mocy przerobowych Konsultantów, uwzględniający statystyczne obciążenie dziennie, tygodniowe i miesięczne. Liczba dostępnych Konsultantów będzie dopasowywana do prognozowanego ruchu w danym okresie.

Wykonawca będzie przeprowadzał szkolenia Konsultantów, co najmniej raz w miesiącu, w celu uzupełnienia wiedzy Konsultantów, na podstawie materiałów wskazanych przez Zamawiającego (zaadaptowanych przez Wykonawcę) lub na podstawie materiałów własnych przygotowanych przez kierującego zespołem Konsultantów. Jednocześnie Zamawiający zobowiązuje się organizować szkolenia dla Konsultantów z zakresu wykraczającego poza kompetencje wykonawcy (w tym np. zmiany w prawie i zmiany w działaniu systemu).

Wykonawca będzie na bieżąco monitorował jakość pracy Konsultantów. Każdy Konsultant powinien mieć sprawdzane co najmniej dwie rozmowy dziennie, pod względem jakości przeprowadzonej rozmowy oraz prawidłowości udzielonej informacji.

Wykonawca odpowiada za działania i zaniechania Konsultantów Wykonawcy jak za działania i zaniechania własne. Wykonawca zapewnia, że przy wykonywaniu usługi będzie się posługiwał wyłącznie Konsultantami Wykonawcy, którzy dają należyłą rękojmię wykonywania przedmiotu umowy.

Zatrudnieni do wykonywania usługi Konsultanci muszą spełniać następujące wymagania ogólne:

- Wykształcenie wyższe o profilu technicznym i/lub doświadczenie (min. 6 miesięcy) pracy w dziale service desk / zarządzania incydentami / cyberbezpieczeństwa lub pokrewnym.
- Umiejętność analizy i interpretacji danych z różnych źródeł.
- Zdolność identyfikacji trendów, wzorców i obszarów problematycznych.
- Wysoka organizacja pracy i metodyczność.
- Umiejętność analitycznego myślenia i wyciągania wniosków na podstawie danych.
- Wysoki poziom samodzielności, odpowiedzialności i dobrej organizacji pracy.
- Proaktywność w działaniu i szukaniu rozwiązań.
- Znajomość języka angielskiego na poziomie B2 (wymagane dla min. 50% zespołu Konsultantów).

Poniższa tabela prezentuje oczekiwane moduły wiedzy i umiejętności, które muszą posiadać zatrudnieni do wykonywania usługi Konsultanci.

Kompetencja oczekiwana w momencie rozpoczęcia świadczenia usługi

Lp.	Kompetencja / wymaganie
1.	Dobra znajomość usługi analizy dojrzałości cyfrowej i cyberbezpieczeństwa firm.
2.	Dobra znajomość usługi pre-weryfikacji zgodności z zaleceniami NIS2.
3.	Dobra znajomość usługi pre-kwalifikacji dot. wymagań dla produktów z elementami cyfrowymi.
4.	Znajomość, umiejętność interpretacji oraz zrozumienia dokumentu „PC-FBC Program Certyfikacji Firma Bezpieczna Cyfrowo”.
5.	Znajomość, umiejętność interpretacji oraz zrozumienia dokumentu „Cyber Essentials: Requirements for IT infrastructure”.
6.	Znajomość przepisów dyrektyw NIS 2 oraz CRA
7.	Wiedza z zakresu budowania odporności organizacji na cyberzagrożenia (cyberresilience).
8.	Wiedza z zakresu identyfikacji, oceny, dokumentowania i akceptacji ryzyka cybernetycznego.
9.	Wiedza z zakresu reagowania na incydenty bezpieczeństwa, w tym wykrywania, raportowania i analizy.
10.	Wiedza i umiejętności z zakresu zarządzania tożsamością i dostępem do kont i zasobów sieciowych, w tym modeli IAM, autoryzacji i polityk haseł.
11.	Wiedza i umiejętności z zakresu administracji systemami operacyjnymi, aplikacjami oraz interfejsami użytkownika, zarządzania aktualizacjami, łatkami i modernizacją systemów IT.
12.	Wiedza i umiejętności z zakresu zarządzania ochroną przed złośliwym oprogramowaniem (malware).
13.	Wiedza i umiejętności z zakresu narzędzi i technik cyberobrony, w tym monitorowania i wykrywania, identyfikowania i reagowania na zagrożenia oraz incydenty bezpieczeństwa.
14.	Umiejętność oceny wiarygodności dostawców i produktów pod kątem bezpieczeństwa.

15.	Umiejętność efektywnego planowania i organizowania zadań.
16.	Umiejętność rozumienia priorytetów biznesowych klientów.
17.	Umiejętność analizowania informacji z wielu źródeł i podejmowania decyzji w warunkach niepewności.
18.	Umiejętność skutecznej komunikacji pisemnej i werbalnej na różnych poziomach technicznych.
19.	Umiejętność stosowania myślenia krytycznego oraz rozwiązywania problemów technicznych.

Tabela 1

Zamawiający zastrzega sobie prawo do weryfikacji kompetencji zespołu przed rozpoczęciem świadczenia usługi. Zamawiający zastrzega sobie prawo do wyboru osób spełniających przedstawione wymagania.

Kompetencja oczekiwana po pierwszym miesiącu (30 dni kalendarzowych) świadczenia usługi

Lp.	Kompetencja / wymaganie
1.	Wiedza z zakresu standardów, modeli i ram bezpieczeństwa (np. CIA, RMF, CIAAN).
2.	Wiedza z zakresu strategii bezpieczeństwa organizacji oraz polityk prywatności i zgodności.
3.	Wiedza z zakresu architektury systemów informatycznych i projektowania bezpiecznych środowisk IT
4.	Wiedza z zakresu usług cyfrowych i identyfikacji sieci
5.	Wiedza z zakresu projektowania bezpiecznych sieci, ich topologii, konfiguracji i komponentów.
6.	Wiedza z zakresu zabezpieczeń brzegowych (Firewall)
7.	Wiedza z zakresu bezpiecznej konfiguracji systemów, aplikacji i komponentów sieciowych.
8.	Wiedza z zakresu zarządzania aktualizacjami
9.	Wiedza z zakresu ochrony przed złośliwym oprogramowaniem, algorytmów szyfrowania oraz ich zastosowań w ochronie danych
10.	Wiedza z zakresu protokołów sieciowych, routingu, modeli komunikacji (np. OSI, VPN) oraz kontroli dostępu użytkowników
11.	Wiedza z zakresu monitorowania aktywności użytkowników oraz analizy zachowań w systemach.
12.	Wiedza z zakresu tworzenia kopii zapasowych, odzyskiwania danych oraz zapewnienia dostępności systemów.
13.	Wiedza z zakresu analizy zagrożeń, wektorów ataków, charakterystyki systemów atakujących oraz oceny ryzyk środowiskowych i operacyjnych w kontekście bezpieczeństwa systemów.

14.	Wiedza z zakresu typowych podatności aplikacji oraz metod ich zabezpieczania i remediacji.
15.	Wiedza z zakresu oceny podatności systemów oraz wykorzystania źródeł danych o podatnościach.
16.	Wiedza z zakresu narzędzi do analizy ruchu sieciowego, monitorowania i wykrywania nieprawidłowości.
17.	Wiedza z zakresu zabezpieczeń fizycznych i cyfrowych oraz metod ich wykrywania i eliminacji.
18.	Wiedza z zakresu kontroli bezpieczeństwa, ograniczeń systemowych oraz wymagań aplikacyjnych i sieciowych.
19.	Umiejętność zarządzania systemami operacyjnymi, serwerami i stacjami roboczymi.
20.	Umiejętność monitorowania przepływu danych w sieci oraz aktywności systemowej.
21.	Umiejętność przeprowadzania analizy ryzyka, zagrożeń, luk oraz anomalii w sieci.
22.	Umiejętność normalizacji danych oraz analizy logów i ruchu sieciowego.
23.	Umiejętność oceny i wdrażania środków zaradczych oraz produktów bezpieczeństwa.
24.	Umiejętność oceny skuteczności zabezpieczeń oraz zgodności z wymaganiami.
25.	Umiejętność utrzymywania rejestrów i przekazywania informacji zarządczych.

Tabela 2

Po pierwszym miesiącu świadczenia usługi Konsultanci Wykonawcy muszą posiadać wiedzę opisaną w powyższej tabeli (Tabela 2). Wiedza Konsultantów może zostać zweryfikowana poprzez przeprowadzenie testu kompetencyjnego przygotowanego przez Zamawiającego. Zamawiający zastrzega sobie prawo do wyboru osób spełniających przedstawione wymagania.

Wykonawca zobowiązuje się zapewnić zespół prezentujący kompetencje określone powyżej do końca czasu świadczenia usługi (co oznacza jego bieżące uzupełnienia w razie takiej potrzeby bez przerw w dostępie wskazanej liczby Konsultantów o określonych kompetencjach).

W przypadku zmian w zespole Wykonawcy każda nowa osoba musi spełniać wymogi ogólne oraz szczegółowe określone w tabelach 1 i 2 powyżej.

Materiały szkoleniowe zostaną udostępnione Wykonawcy w momencie rozpoczęcia usługi. Przykładowe ogólnodostępne źródła wiedzy z wymaganych obszarów:

- ISO/IEC 27001 Technika Informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania.
- ISO/IEC 27002 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji.
- ISO/IEC 27005 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji.
- ISO 31000 Zarządzanie ryzykiem – Wytyczne.
- Cyber Essentials: Requirements for IT infrastructure, v3.1, April 2023.
- Cyber Essentials Readiness Tool <https://getreadyforcyberessentials.iasme.co.uk/>.
- Materiały i treści z obszaru cyberbezpieczeństwa dostępne na stronach rządowych

4. ZESPÓŁ REALIZUJĄCY PROJEKT PO STRONIE WYKONAWCY

Wykonawca zobowiązany jest do stworzenia po swojej stronie Zespołu, którego struktura musi minimalnie wypełniać funkcje, opisane w poniższym punkcie.

Funkcje wskazane poniżej mogą być łączone w ten sposób, że 1 osoba może pełnić maksymalnie 2 funkcje. W szczególności dopuszczalne jest łączenie funkcji kierownika ds. Zespołu Konsultantów, który jednocześnie może pełnić rolę Konsultanta.

Do zadań Kierownika Projektu należy minimalnie:

- a) nadzór nad prawidłową realizacją projektu oraz bieżącym utrzymaniem produktów projektu,
- b) nadzór nad Koordynatorami oraz Kierownikiem Zespołu Konsultantów,
- c) kontakty oraz prezentacja raportów przed Zamawiającym.

Do zadań Koordynatora ds. technicznych należy minimalnie:

- a) realizacja zadań związanych z prawidłowym funkcjonowaniem i ciągłym rozwojem systemu,
- b) administrowanie systemem Wykonawcy, w tym zarządzanie uprawnieniami Klientów, słownikami i konfiguracja powiadomień,
- c) konfiguracja komunikatów automatycznych w formie IVR, zgodnie z ustaleniami z Zamawiającym.

Do zadań Kierownika Zespołu Konsultantów należy:

- a) Zarządzanie Konsultantami realizującym zadania CC,
- b) Dbłość o ciągłość działania i bezawaryjność funkcjonowania CC,
- c) Działanie na rzecz tworzenia ulepszeń i prawidłowości funkcjonowania CC,
- d) Przygotowywanie raportów zgodnych z Umową lub OPZ lub na zlecenie Zamawiającego związanych z funkcjonowaniem CC,
- e) Przygotowanie i prezentacja raportów z pracy Call Center przed Zamawiającym, w trybie cotygodniowym lub innym, ustalonym z Zamawiającym, w formie prezentacji zdalnej lub osobistej,
- f) przekazywanie Zamawiającemu raportów o alertach ws. potencjalnych problemów technicznych,

Do zadań Konsultantów należy:

- a) Obsługa zgłoszeń i wiadomości przychodzących
- b) Obsługa połączeń wychodzących
- c) Obsługa Live Chat
- d) Obsługa zgłoszeń z formularza kontaktowego
- e) Tworzenie wkładu do nowych zagadnień do FAQ

- f) Tworzenie sugestii aktualizacji zagadnień już istniejących w FAQ

5. RAPORTY Z WYKONANIA UMOWY

Wykonawca będzie przekazywał Zamawiającemu do 5 dnia kolejnego miesiąca raporty w zakresie wykonania umowy.

Szczegółowy format raportów zostanie określony po podpisaniu Umowy.

Minimalny zakres danych oczekiwany w raporcie:

- liczba połączeń odebranych i nieodebranych w ujęciu dziennym/miesięcznym
- czas oczekiwania w kolejce w ujęciu dziennym
- liczba połączeń zrzucanych przez agenta
- aktywności na Live Chat
- obsługa zgłoszeń z formularza kontaktowego
- dostępność konsultantów

6. PRZYGOTOWANIE I PRZEKAZANIE ZAMAWIAJĄCEMU FAQ

Wykonawca przygotuje i przekaze Zamawiającemu opracowanie (FAQ) najczęściej rozwiązywanych problemów i zadawanych pytań wraz z odpowiedziami i wszelkimi informacjami umożliwiającymi przyszłą obsługę takich przypadków. Forma FAQ zostanie doprecyzowana na początku realizacji przedmiotu zamówienia.

Załączniki:

Załącznik nr 1 – Formularz Ofertowy