Państwowy Instytut Geologiczny
Państwowy Instytut Badawczy
państwowa służba geologiczna
państwowa służba hydrogeologiczna

SPECYFIKACJA

WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie

PODSTAWOWYM Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI

na podstawie art. 275 pkt 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 z późn. zm.), o wartości szacunkowej zamówienia poniżej 215 000 EURO, nie mniejszej jednak niż 130 000 złotych.

oznaczenie sprawy: **EZP.26.178.2022**

PRZEDMIOT ZAMÓWIENIA:

Usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB

ZATWIERDZAM:
Pełnomocnik dyrektora PIG-PIB
ds. Zamówień Publicznych
Katarzyna Karczewska

Warszawa, dnia 17.10.2022 r.

pgi.gov.pl

ul. Rakowiecka 4, 00-975 Warszawa
tel. (+48) 22 45 92 000, biuro@pgi.gov.pl

Sąd Rejonowy dla m. st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS, Nr 0000122099
NIP 525-000-80-40

1. ZAMAWIAJĄCY

Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy

00-975 Warszawa, ul. Rakowiecka 4

NIP: 525-000-80-40, REGON: 000332133

wpisany do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000122099.

Adres strony internetowej prowadzonego postępowania: https://platformazakupowa.pl/pn/pgi, zwana dalej również „Platformą".

2. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

Zmiany i wyjaśnienia SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej: https://platformazakupowa.pl/pn/pgi.

3. TRYB UDZIELENIA ZAMÓWIENIA

3.1 Postępowanie o udzielenie przedmiotowego zamówienia publicznego prowadzone jest na podstawie przepisów ustawy z dnia 11 września 2019 Prawo zamówień publicznych (Dz. U. 2022 poz. 1710 z późn zm.) - zwanej dalej "ustawą Pzp" – oraz przepisów wykonawczych wydanych na jej podstawie, w szczególności rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy – zwanego dalej „rozporządzeniem MR"- w trybie podstawowym na podstawie art. 275 pkt 2 ustawy Pzp oraz niniejszej Specyfikacji Warunków Zamówienia, zwaną dalej „SWZ".

3.2 Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji w celu ulepszenia treści ofert, które podlegać będą ocenie w ramach kryterium oceny ofert.

3.3 W przypadku skorzystania przez Zamawiającego z uprawnienia wynikającego z art. 275 pkt 2 ustawy Pzp, Zamawiający przewiduje możliwość ograniczenia liczby Wykonawców, których zaprosi do negocjacji do liczby zapewniającej konkurencję – nie mniej jednak niż 3 i nie więcej niż 5. Jeśli liczba złożonych ofert będzie mniejsza niż 3, Zamawiający zaprosi do negocjacji wszystkich Wykonawców, których oferty nie podlegały odrzuceniu.

3.4 Zamawiający, w celu ograniczenia liczby Wykonawców zaproszonych do negocjacji ofert, zastosuje kryterium oceny ofert opisane w pkt 17 SWZ.

3.5 Zamawiający poinformuje równocześnie wszystkich Wykonawców, którzy w odpowiedzi na ogłoszenia o zamówieniu złożą ofertę o Wykonawcach:

3.5.1 których oferty nie zostały odrzucone, oraz punktacji przyznanej ofertom w każdym kryterium oceny ofert i łącznej punktacji,

3.5.2 których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne,

3.5.3 którzy nie zostali zakwalifikowani do negocjacji oraz punktacji przyznanej ich oferentom w każdym kryterium oceny ofert i łącznej punktacji, w przypadku, o którym mowa w art. 288 ust. 1 ustawy Pzp.

3.6 Zamawiający, w zaproszeniu do negocjacji, wskaże miejsce, termin i sposób prowadzenia negocjacji oraz kryteria oceny ofert, w ramach których będą prowadzone negocjacje w celu ulepszenia treści ofert.

3.7 Prowadzone negocjacje będą miały charakter poufny.

3.8 Zamawiający poinformuje równocześnie wszystkich Wykonawców, których oferty złożono w odpowiedzi na ogłoszenie o zamówieniu nie zostaną odrzucone i którzy brali udział w negocjacjach, o zakończeniu negocjacji oraz zaprosi ich do składania ofert dodatkowych.

3.9 Zamawiający wyznaczy termin na złożenie ofert dodatkowych z uwzględnieniem czasu potrzebnego na przygotowanie tych ofert, z tym, że termin ten nie będzie krótszy niż 5 dni od dnia przekazania zaproszenia, do składania ofert dodatkowych.

3.10 Wykonawca będzie mógł złożyć ofertę dodatkową, która zawierać będzie nowe propozycje w zakresie treści oferty podlegającej ocenie w ramach kryteriów oceny ofert wskazanych przez Zamawiającego w zaproszeniu do negocjacji.

3.11 Oferta dodatkowa nie będzie mogła być mniej korzystna w żadnym z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.

3.12 Oferta przestaje wiązać Wykonawców z zakresie, w jakim złoży on ofertę dodatkową zawierającą korzystniejsze propozycje w ramach każdego z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji.

3.13 Oferta dodatkowa, która będzie mniej korzystna w którymkolwiek z kryterium oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu, podlegać będzie odrzuceniu.

3.14 Ofertę Wykonawcy niezaproszonego do negocjacji uznaje się za odrzuconą.

3.15 Jeżeli Zamawiający uzna, po otwarciu ofert, że nie będzie prowadził negocjacji, dokona wyboru najkorzystniejszej oferty spośród niepodlegających odrzuceniu ofert złożonych w odpowiedzi na ogłoszenie o zamówieniu.

3.16 Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych o jakich mowa w art. 3 ustawy Pzp.

3.17 Zgodnie z art. 310 pkt 1 ustawy Pzp Zamawiający przewiduje możliwość unieważnienia przedmiotowego postępowania, jeżeli środki, które Zamawiający zamierzał przeznaczyć na sfinansowanie w całości lub części zamówienia, nie zostały mu przyznane.

3.18 Zamawiający nie przewiduje aukcji elektronicznej.

3.19 Zamawiający nie przewiduje złożenia oferty w postaci katalogów elektronicznych.

3.20 Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.

3.21 Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 ustawy Pzp.

4. OPIS PRZEDMIOTU ZAMÓWIENIA

4.1 Przedmiotem zamówienia jest **usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB.**

4.2 Szczegółowy zakres oraz sposób realizacji przedmiotu zamówienia został określony w:

– załączniku nr 1 do SWZ – Opis przedmiotu zamówienia

– załączniku nr 2 do SWZ – Projektowane postanowienia umowy.

4.3 Oznaczenie przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

Kod i nazwa CPV: 48000000-8 Pakiety oprogramowania i systemy informatyczne.

Kod i nazwa CPV: 71356300-1 Usługi wsparcia technicznego.

4.4 Zamawiający nie dopuszcza składania ofert częściowych. Zamawiający nie dokonuje podziału ponieważ podział przedmiotu zamówienia na części grozi nadmiernymi trudnościami technicznymi oraz generuje poważne ryzyko niewłaściwego wykonania zamówienia.

4.5 Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

4.6 Zamawiający na podstawie art. 441 ustawy Pzp przewiduje zastosowanie prawa opcji.

4.6.1 zamówienie opcjonalne – od dnia 01.01.2024 r. do dnia 31.12.2024 r. Zamawiający poinformuje Wykonawcę o zamiarze skorzystania z prawa opcji nie później niż do dnia 15.12.2023 r.

4.6.2 **Prawo opcji realizowane będzie na takich samych warunkach jak zamówienie gwarantowane.**

4.7 Zamawiający będzie mógł skorzystać z prawa opcji w sytuacjach i na zasadach opisanych w § 2. Termin realizacji Umowy i warunki dostawy ust. 1. **Załącznika nr 2 do SWZ** – Projektowane postanowienia umowy.

4.8 Cena świadczenia usług świadczonych w ramach prawa opcji będzie identyczna jak zamówienia podstawowego, określonego w Ofercie Wykonawcy złożonej przez Wykonawcę na wzorze formularza oferty stanowiącym **Załącznik nr 3 do SWZ**.

4.9 Zamawiający nie ma obowiązku korzystać z prawa opcji. Wykonawcy nie przysługuje prawo roszczeń z tytułu niewykorzystania prawa opcji lub jego pełnej wartości.

4.10 Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 7 ustawy Pzp.

4.11 Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 ustawy Pzp.

4.12 Zamawiający nie określa dodatkowych wymagań związanych z zatrudnianiem osób, o których mowa w art. 96 ust. 2 pkt 2 ustawy Pzp.

5. TERMIN WYKONANIA ZAMÓWIENIA

5.1 Termin realizacja zamówienia: 12 miesięcy od daty zawarcia umowy.

5.2 Termin realizacji zamówienia opcjonalnego – od dnia 01.01.2024 r. do dnia 31.12.2024 r. Zamawiający poinformuje Wykonawcę o zamiarze skorzystania z prawa opcji nie później niż do dnia 15.12.2023 r. Prawo opcji realizowane będzie na takich samych warunkach jak zamówienie gwarantowane.

6. PODWYKONAWSTWO

6.1 Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).

6.2 Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia

6.3 Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

6.4 W przypadku niewskazania części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i firm podwykonawców, przyjmuje się, iż przedmiot zamówienia zostanie w całości wykonany samodzielnie przez Wykonawcę.

6.5 Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.

7. PODSTAWY WYKLUCZENIA ORAZ WARUNKI UDZAIŁU W POSTĘPOWANIU

7.1 Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych w:

7.1.1 art. 108 ust. 1 ustawy Pzp;

7.1.2 art. 109 ust. 1 pkt 4 ustawy Pzp;

7.1.3 art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835).

7.2 Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.

7.3 W postępowaniu mogą wziąć udział Wykonawcy, którzy spełniają następujące warunki udziału w postepowaniu:

7.3.1 **zdolności do występowania w obrocie gospodarczym:**

Zamawiający nie stawia warunku w powyższym zakresie;

7.3.2 **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:**

Zamawiający nie stawia warunku w powyższym zakresie;

7.3.3 **sytuacji ekonomicznej lub finansowej:**

Zamawiający nie stawia warunku w powyższym zakresie;

7.3.4 **zdolności technicznej lub zawodowej:**

Wykonawca spełni warunek jeżeli wykaże, że;

7.3.4.1 w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał co najmniej jedną dostawę licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem o wartości nie mniejszej niż 300 000,00 zł brutto.

7.3.4.2 przy realizacji zamówienia będzie dysponował osobami o odpowiednich kwalifikacjach zawodowych i uprawnieniach niezbędnych do prawidłowej realizacji zamówienia;

7.3.4.2.1 co najmniej jedną osobą posiadającą ważny certyfikat administratora DLP

7.3.4.2.2 co najmniej dwie osoby posiadające ważny certyfikat administratora e-mail security

7.3.4.2.3 co najmniej jedną osobą posiadającą ważny certyfikat administratora web security

Każda z osób wskazanych w pkt. 7.3.4.2. SIWZ może pełnić w zespole nie więcej niż dwie różne funkcje.

7.4 Zamawiający, w stosunku do Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w odniesieniu do warunku dotyczącego zdolności technicznej lub zawodowej – dopuszcza łączne spełnianie warunku przez Wykonawców.

7.5 Zamawiający może na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.

8. POLEGANIE NA ZASOBACH INNYCH PODMIOTÓW

8.1 Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.

8.2 W odniesieniu do warunków dotyczących doświadczenia, Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają świadczenie do realizacji którego te zdolności są wymagane.

8.3 Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Wzór zobowiązania stanowi **załącznik nr 5 do SWZ.**

8.4 Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.

8.5 Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.

8.6 **UWAGA**: Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

8.7 Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w pkt 9.2.1. SWZ, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby, zgodnie z katalogiem dokumentów określonych w pkt 9 SWZ.

9. OŚWIADCZENIA I DOKUMENTY, JAKIE ZOBOWIĄZANI SĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA (PODMIOTOWE ŚRODKI DOWODOWE)

9.1 Na ofertę składa się:

9.1.1 **formularz „Oferta”** stanowiący **załącznik nr 3 do SWZ**.

9.2 Oświadczenia lub dokumenty składane **razem z ofertą**:

9.2.1 oświadczenie, o niepodleganiu wykluczeniu oraz spełnieniu warunków udziału w postępowaniu – zgodnie z **Załącznikiem nr 4 do SWZ**;

9.2.2 zobowiązanie innego podmiotu lub inny podmiotowy środek dowodowy, o których mowa w pkt 8.4 SWZ (jeżeli dotyczy) – **Załącznik nr 5 do SWZ;**

9.2.3 oświadczenie Wykonawców występujących wspólnie, z którego treści wynika, które usługi wykonają poszczególni Wykonawcy, o którym mowa w pkt 11.4 SWZ (jeżeli dotyczy) – zgodnie z **Załącznikiem nr 6 do SWZ**;

9.2.4 oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu dla podmiotów udostępniających zasoby – zgodnie z **załącznikiem nr 7 do SWZ** (jeżeli dotyczy);

9.2.5 dokumenty, z których wynika prawo do podpisania oferty, odpowiednie pełnomocnictwa (jeżeli dotyczy);

9.2.6 uzasadnienie dotyczące zastrzeżenia dokumentów jako tajemnica przedsiębiorstwa (jeżeli dotyczy).

9.3 Informacje zawarte w oświadczeniu, o którym mowa w pkt 9.2.1 SWZ stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

9.4 Zamawiający wezwie Wykonawców, których oferty zostały najwyżej ocenione, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, jeżeli wymagał ich złożenia w ogłoszeniu o zamówieniu lub dokumentach zamówienia, aktualnych na dzień złożenia podmiotowych środków dowodowych.

9.5 Podmiotowe środki dowodowe wymagane od Wykonawcy na potwierdzenie nie podlegania wykluczeniu obejmują:

9.5.1 oświadczenie Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej Zamawiający odstąpi od wezwania do złożenia oświadczenia jeżeli w postępowaniu zostanie złożona 1 oferta;

9.5.2 Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w pkt 9.2.1. SWZ, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby, zgodnie z katalogami dokumentów określonymi w pkt 9.6.1. SWZ.

9.5.3 odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzone nie wcześniej niż 3 miesiące przed ich złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;

9.5.4 jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast dokumentów o których mowa w pkt 9.5.3. SWZ składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury. Dokumenty powinny być wystawione nie wcześniej niż 3 miesiące przed ich złożeniem;

9.5.5 jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 9.5.4 SWZ, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Dokument powinien być wystawiony nie wcześniej niż 3 miesiące przed ich złożeniem.

9.6 Podmiotowe środki dowodowe wymagane od Wykonawcy na potwierdzenie spełnienia warunków udziału w postępowaniu obejmują:

9.6.1 wykaz usług wykonanych w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich przedmiotu, daty wykonania i podmiotów, na rzecz których usługi zostały wykonane oraz załączeniem dowodów określających, czy te usługi zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy**.**

9.6.2 Wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego, wraz z informacjami na temat ich kwalifikacji zawodowych niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informację o podstawie do dysponowania tymi osobami.

9.7 Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:

9.7.1 może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał w oświadczeniu, o którym mowa w pkt 9.2.1. SWZ dane umożliwiające dostęp do tych środków;

9.7.2 jest w ich posiadaniu, pod warunkiem, że Wykonawca potwierdzi ich prawidłowość i aktualność (podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w pkt. 9.2.1 SWZ).

9.8 Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

9.9 W zakresie nieuregulowanym ustawą Pzp lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy rozporządzenia MR oraz rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.

10. INFORMACJA O PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH

10.1 Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.

11. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA)

11.1 Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.

11.2 W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w pkt 9.2.1. SWZ, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

11.3 W odniesieniu do warunków określonych w pkt 7.3 SWZ, wymagania te mogą być spełnione wspólnie przez Wykonawców składających ofertę wspólną (nie musi ich spełniać osobno każdy z Wykonawców składających ofertę wspólną). Na ich potwierdzenie należy złożyć dokumenty określone w pkt 9.6 SWZ.

11.4 Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które usługi wykonają poszczególni Wykonawcy.

11.5 Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

11.6 Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji Wykonawcy są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które usługi wykonają poszczególni Wykonawcy.

12. SPOSÓB KOMUNIKACJI

12.1 Komunikacja w postępowaniu o udzielenie zamówienia, z uwzględnieniem wyjątków określonych w ustawie Pzp, odbywa się przy użyciu środków komunikacji elektronicznej. Przez środki komunikacji elektronicznej rozumie się środki komunikacji elektronicznej zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).

12.2 Komunikacja między Zamawiającym a Wykonawcami, w szczególności składanie oświadczeń, wniosków, zawiadomień oraz przekazywanie informacji odbywa się za pośrednictwem Platformy, o której mowa w pkt 1 SWZ i formularza „Wyślij wiadomość do zamawiającego" dostępnego na stronie Platformy dotyczącej danego postępowania. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem Platformy poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.

12.3 Zamawiający informuje, że instrukcje korzystania z Platformy znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.

12.4 Wykonawca, przystępując do przedmiotowego postępowania o udzielenie zamówienia:

12.4.1 akceptuje warunki korzystania z Platformy określone w Regulaminie dostępnym w zakładce „Regulamin" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/1-regulamin oraz uznaje go za wiążący;

12.4.2 zapoznał i stosuje się do Instrukcji składania ofert dostępnej w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.

12.5 Zamawiający będzie przekazywał Wykonawcom informacje w postaci elektronicznej za pośrednictwem Platformy. Informacje dotyczące przedmiotowego postępowania Zamawiający będzie zamieszczał na platformie w sekcji "Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w postaci elektronicznej za pośrednictwem Platformy do konkretnego Wykonawcy. Wykonawca w trakcie toczącego się postępowania powinien sprawdzać komunikaty i wiadomości przesłane przez Zamawiającego bezpośrednio na Platformie, gdyż system powiadomień Platformy może ulec awarii lub powiadomienie może trafić do folderu SPAM.

12.6 Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

12.7 Zamawiający określa niezbędne wymagania sprzętowo – aplikacyjne umożliwiające pracę na Platformie, tj.:

12.7.1 stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s;

12.7.2 komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje;

12.7.3 zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10.0.;

12.7.4 włączona obsługa JavaScript;

12.7.5 zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf;

12.7.6 Platforma działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8;

12.7.7 oznaczenie czasu odbioru danych przez Platformę stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

12.8 Ofertę, a także oświadczenie o jakim mowa w pkt 9.2.1. SWZ składa się w oryginale, pod rygorem nieważności, w formie elektronicznej podpisanej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej

opatrzonej podpisem zaufanym lub podpisem osobistym. Podmiotowe środki dowodowe, pełnomocnictwa, zobowiązanie podmiotu udostępniającego zasoby sporządza się w formie lub postaci elektronicznej.

12.9 Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane przez Wykonawcę muszą być zgodne z obowiązującym Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

12.10 Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. 2020 r., poz. 2452) oraz rozporządzenia MR.

13. OPIS SPOSOBU PRZYGOTOWANIA OFERT ORAZ WYMAGANIA FORMALNE DOTYCZĄCE SKŁADANYCH OŚWIADCZEŃ I DOKUMENTÓW

13.1 Wykonawca może złożyć tylko jedną ofertę.

13.2 Treść oferty musi odpowiadać treści SWZ.

13.3 Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy. W celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania, Zamawiający żąda od Wykonawcy odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.

13.4 Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy zamieszczonych w załącznikach do SWZ, powinny być sporządzone zgodnie z tymi wzorami.

13.5 Oferta wraz z załącznikami musi być sformułowana w języku polskim, w sposób czytelny, logiczny, z zachowaniem postaci elektronicznej (Zamawiający rekomenduje następujące formaty danych .doc, .docx, .pdf) i podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

13.6 Ofertę wraz z wymaganymi dokumentami należy umieścić na Platformie pod adresem: https://platformazakupowa.pl/pn/pgi. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania". Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.

13.7 Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno.

13.8 W przypadku konieczności skompresowania w ofercie kilku dokumentów, użytkownik powinien te dokumenty zapisać jako .zip, .7Z, .tar, .gz (Zamawiający rekomenduje zapisać dokumenty jako .zip). Oferta skompresowana do innego formatu danych niż .zip, .7Z, .tar, .gz zostanie odrzucona na podstawie art. 226 ust. 1 pkt. 6 ustawy Pzp.

13.9 Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku "Złóż ofertę" i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.

13.10 Dokumenty lub oświadczenia sporządzone w języku obcym Wykonawca musi złożyć wraz z tłumaczeniem na język polski. Podczas oceny ofert Zamawiający będzie się opierał na tekście przetłumaczonym na język polski.

13.11 Jeśli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233), Wykonawca powinien nie później niż w terminie składania ofert, zastrzec, że nie mogą one być udostępnione oraz wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na Platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.

13.12 Stosownie do powyższego, jeśli Wykonawca nie dopełni ww. obowiązków wynikających z ustawy, Zamawiający będzie miał podstawę do uznania, że zastrzeżenie tajemnicy przedsiębiorstwa jest bezskuteczne i w związku z tym potraktuje daną informację, jako niepodlegającą ochronie i niestanowiącą tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji.

13.13 Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Platformy.

13.14 Wszystkie koszty związane z uczestnictwem w postępowaniu, w szczególności z przygotowaniem i złożeniem oferty ponosi Wykonawca składający ofertę. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

14. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca będzie związany ofertą przez okres 30 dni, tj. do dnia **24.11.2022 r**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

15. SPOSÓB I TERMIN SKŁADANIA I OTWARCIA OFERT

15.1 Wykonawca składa ofertę za pośrednictwem Platformy pod adresem: https://platformazakupowa.pl/pn/pgi.

15.2 Termin składania ofert upływa w dniu **26.10.2022 r**. o godz. 10:00.

15.3 Otwarcie ofert nastąpi w dniu **26.10.2022 r**. o godz.10:05.

15.4 Najpóźniej przed otwarciem ofert, Zamawiający udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

15.5 Niezwłocznie po otwarciu ofert, udostępnia się na stronie internetowej prowadzonego postępowania w sekcji „Komunikaty" informacje o:

15.5.1 nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;

15.5.2 cenach zawartych w ofertach.

16. OPIS SPOSOBU OBLICZANIA CENY OFERTY

16.1 Wykonawca podaje cenę za realizację przedmiotu zamówienia zgodnie ze wzorem formularza „Oferta" – załącznik nr 3 do SWZ.

16.2 Cena w formularzu „Oferta" musi uwzględniać wszystkie wymagania niniejszej SWZ oraz obejmować wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.

16.3 Wszystkie ceny netto określone przez Wykonawcę w formularzu „Oferta" zostaną ustalone na okres ważności umowy i nie będą podlegały zmianom.

16.4 W przypadku wystąpienia omyłek rachunkowych, za prawidłowe Zamawiający przyjmie ceny jednostkowe netto i dokona przeliczenia oferty zgodnie ze sposobem wskazanym w formularzu „Oferta".

16.5 Wszystkie ceny będą określone w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku, a wszystkie płatności będą realizowane w złotych polskich, zgodnie z obowiązującymi przepisami.

16.6 Zamawiający nie przewiduje rozliczeń w walucie obcej.

16.7 Jeżeli została złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2022 r. poz. 931), dla celów zastosowania kryterium ceny, Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W ofercie, o której mowa w pkt 16.1. SWZ, Wykonawca ma obowiązek:

16.7.1 poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;

16.7.2 wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;

16.7.3 wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;

16.7.4 wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

16.8 Wzór formularza „Oferta" został opracowany przy założeniu, iż wybór oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego w zakresie podatku VAT. W przypadku, gdy Wykonawca zobowiązany jest złożyć oświadczenie o powstaniu u Zamawiającego obowiązku podatkowego, to winien odpowiednio zmodyfikować treść formularza.

16.9 W przypadku gdy ofertę składa osoba fizyczna nieprowadząca działalności gospodarczej cena oferty powinna zawierać zaliczkę na podatek dochodowy oraz wszelkie należne składki, które to Zamawiający, zgodnie z obowiązującymi przepisami, będzie zobowiązany naliczyć i odprowadzić. Tym samym, Wykonawca będący osobą fizyczną nieprowadzącą działalności gospodarczej wyrazi zgodę na pomniejszenie swoich należności (ceny oferty) o zaliczki i składki, które Zamawiający będzie zobowiązany naliczyć i odprowadzić w związku z realizacją umowy. Należność wypłacona bezpośrednio Wykonawcy nie będzie wówczas równa cenie oferty. Wobec powyższego w celu zapewnienia porównywalności ofert cena oferty złożonej przez osobę fizyczną nieprowadzącą działalności gospodarczej powinna zawierać zaliczkę na podatek dochodowy oraz wszelkie należne składki, które to Zamawiający, zgodnie z obowiązującymi przepisami, byłby zobowiązany naliczyć i odprowadzić.

16.10 Zamawiający zwróci się o udzielenie wyjaśnień (w tym złożenie dowodów) jeżeli cena oferty lub jej istotne części składowe wydadzą się rażąco niskie w stosunku do przedmiotu zamówienia i będą budziły wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów.

17. OPIS KRYTERIÓW OCENY OFERT WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

17.1 Ocenie zostaną poddane oferty nie podlegające odrzuceniu.

17.2 Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował określonym następującymi kryteriami i ich znaczeniem:

Nazwa kryterium	Waga podana w punktach
Cena brutto	**100**

17.3 Oferty oceniane będą w następujący sposób:

W kryterium **„cena brutto" (C)**:

$$C = \frac{\text{najniższa cena}}{\text{cena oferty badanej}} \times 100 \text{ pkt}$$

17.4 Liczba punktów przyznana poszczególnym ofertom zostanie obliczona z dokładnością do dwóch miejsc po przecinku.

17.5 W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty, w tym zaoferowanej ceny.

18. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium

19. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

20. INFORMACJA O FORMALNOŚCIACH JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

20.1 Zamawiający zawiera umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.

20.2 Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt 20.1 SWZ, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę.

20.3 W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.

20.4 Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.

20.5 Przed podpisaniem umowy Wykonawca powinien dostarczyć: pełnomocnictwo do podpisania umowy, jeżeli nie wynika ono z załączonych do oferty dokumentów.

21. INFORMACJE O TREŚCI ZAWIERANEJ UMOWY ORAZ MOŻLIWOŚCI JEJ ZMIANY

21.1 Wybrany Wykonawca jest zobowiązany do zawarcia umowy w sprawie zamówienia publicznego na warunkach określonych w Projektowych postanowieniach umowy, stanowiących **Załącznik nr 2 do SWZ.**

21.2 Zakres świadczenia Wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.

21.3 Na podstawie art. 455 ust. 1 i 2 ustawy Pzp, Zamawiający przewiduje możliwość zmian zawartej umowy w stosunku do treści wybranej oferty w zakresie wskazanym w Projektowych postanowieniach umowy, stanowiących **Załącznik nr 2 do SWZ.**

21.4 Zmiana umowy wymaga dla swej ważności, pod rygorem nieważności, zachowania formy pisemnej.

22. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej na zasadach przewidzianych w dziale IX ustawy Pzp (art. 505–590).

23. DANE OSOBOWE

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", Zamawiający informuje, że:

- administratorem Pani/Pana danych osobowych jest Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy, ul. Rakowiecka 4, 00-975 Warszawa, tel. (+48) 22 45 92 000, fax. tel. (+48) 22 45 92 001, email biuro@pgi.gov.pl;
- administrator wyznaczył inspektora ochrony danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania danych osobowych pod adresem poczty elektronicznej: iod@pgi.gov.pl lub pisemnie na adres siedziby PIG-PIB;
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywających na Zamawiającym;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art.18 oraz art. 74 ustawy Pzp;
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem określonym w przepisach ustawy PZP, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
- posiada Pani/Pan:
  a. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

b. na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników);

c. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia;

d. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

- nie przysługuje Pani/Panu:

a. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

b. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

c. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;

- Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od Wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z włączeń, o których mowa w art. 14 ust. 5 RODO.

24. ZAŁĄCZNIKI:

24.1 Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia;

24.2 Załącznik nr 2 do SWZ – Projektowane postanowienia umowy;

24.3 Załącznik nr 3 do SWZ – Formularz „Oferta”;

24.4 Załącznik nr 4 do SWZ – Oświadczenie o niepodleganiu wykluczeniu oraz spełnieniu warunków udziału w postępowaniu;

24.5 Załącznik nr 5 do SWZ – Zobowiązanie podmiotu udostępniającego zasoby;

24.6 Załącznik nr 6 do SWZ – Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia;

24.7 Załącznik nr 7 do SWZ – Oświadczenie podmiotu udostępniającego zasoby, o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu

Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest usługa wsparcia i subskrypcji dla posiadanych przez Zamawiającego system filtrowania i bezpieczeństwa ruchu WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla Państwowego Instytutu Geologicznego – Państwowego Instytutu Badawczego.

   1) System filtrowania i bezpieczeństwa ruchu WWW (FORCEPOINT TRITON) wraz z modułem WEB DLP lub równoważny dla około 950 użytkowników sieci LAN Zamawiającego.

   2) System ochrony danych DLP (FORCEPOINT TRITON) wraz z: (TRITON AP-DATA DISCOVER, TRITON AP-ENDPOINT DLP, TRITON AP-WEB, TRITON AP-EMAIL) lub równoważny dla około 950 użytkowników sieci LAN Zamawiającego.

   3) System ochrony poczty (FORCEPOINT TRITON) wraz z: (Antispam, Antivirus, Email DLP-Module) lub równoważny dla około 950 użytkowników sieci LAN zintegrowany z Active Directory.

   Usługa wsparcia powinna zawierać również update wyżej wymienionych systemów do najnowszej dostępnej wersji (przynajmniej raz w ciągu trwania umowy) oraz codzienną aktualizację polityk i filtrów w module ochrony poczty.

2. Rozszerzenie systemu o usługę utrzymania oraz wdrożenia modułu DLP Cloud Application lub równoważny.

3. Zamawiający posiada następujące produkty:
   - TRITON AP-WEB (wraz z: Web DLP Module)
   - TRITON DLP (wraz z TRITON AP-DATA DISCOVER, TRITON AP-ENDPOINT DLP, TRITON AP-WEB, TRITON AP-EMAIL)
   - TRITON AP-EMAIL (wraz z: Antispam, Antivirus, Email DLP-Module)

4. Wymagania serwisowe:
   - w przypadku problemów wynikających z braku wiedzy Zamawiającego, możliwość skorzystania z bezpłatnego wsparcia telefonicznego 24 godziny na dobę 7 dni w tygodniu,
   - w przypadku awarii działania elementu usługi, usunięcie jej w czasie maksymalnie 62 godzin od daty potwierdzenia przyjęcia zgłoszenia,
   - w przypadku ustania działania całego systemu, usunięcie awarii w czasie 24 godziny od daty potwierdzenia przyjęcia zgłoszenia,
   - czas reakcji na zgłoszenie 1 dzień, tj. najpóźniej do godz. 16.00 dnia następnego po dniu zgłoszenia

5. Na potrzeby realizacji przedmiotu zamówienia Wykonawca zostanie dopuszczony do serwerów Zamawiającego poprzez zdalny dostęp.

6. Termin realizacji zamówienia:
   - zamówienie gwarantowane – od dnia 01.01.2023 r. do dnia 31.12.2023 r.,
   - zamówienie opcjonalne – od dnia 01.01.2024 r. do dnia 31.12.2024 r. Zamawiający poinformuje Wykonawcę o zamiarze skorzystania z prawa opcji nie później niż do dnia 15.12.2023 r. Prawo opcji realizowane będzie na takich samych warunkach jak zamówienie gwarantowane.

Specyfikacja wymagań na system równoważny systemowi Forcepoint Web, Email i DLP Security.

System musi zapewnić dostęp do konfiguracji poprzez jedną konsolę.

Specyfikacja wymagań w zakresie kontroli dostępu do stron sieci web i ruchu sieciowego

1. Rozwiązanie powinno umożliwiać monitorowanie i kontrolę połączeń do sieci www z wykorzystaniem protokołów HTTP i HTTPS.
2. Rozwiązanie powinno filtrować ruch http/https porównując odwołania ze specjalizowaną bazą danych (dostarczaną przez producenta) podzieloną na kategorie (np. Sport, Adult Material, Entertainment, Shopping, Travel, etc). Rozwiązanie powinno posiadać co najmniej 90 kategorii dla ruchu web.
3. Rozwiązanie powinno umożliwiać tworzenie własnych kategorii i dodawanie do nich zarówno tych URL, których nie ma w bazie dostarczanej przez producenta jak i tych, które się tam znajdują, ale w innej kategorii.
4. Baza adresów URL musi być nieprzerwanie aktualizowana przez producenta m.in. poprzez stosowanie:
    - specjalnych robotów internetowych przeszukujących i analizujących zasoby sieci,
    - mechanizmów sztucznej inteligencji dokonujących klasyfikacji zawartości stron,
    - specjalny zespół ludzi weryfikujących poprawność klasyfikacji.
5. Baza producenta musi być aktualizowana możliwie często, a rozwiązanie musi mieć możliwość automatycznego ich pobierania od producenta. Ponadto dla stron na które wchodzili pracownicy firmy, a które nie były skategoryzowane w bazie, powinna istnieć możliwość ich automatycznego wysyłania do producenta w celu kategoryzacji.
6. Rozwiązanie powinno także analizować pozostały ruch sieciowy i rozpoznawać jego rodzaj. Administrator systemu powinien mieć możliwość zabronić lub zezwolić na wykorzystanie przez użytkowników określonych protokołów – np. powinna istnieć możliwość zablokowania protokołów IRC, P2P, IM w tym Gadu-Gadu. Protokoły sieciowe powinny być podzielone na kategorie (np. Instant Messaging, P2P File Transfer, etc). Rozwiązanie powinno posiadać co najmniej 100 protokołów podzielonych na co najmniej 12 kategorii.
7. Analiza i rozpoznawanie powinno dotyczyć również protokołów tunelowanych w połączeniach HTTP i HTTPS.
8. Rozwiązanie powinno umożliwiać tworzenie własnych definicji protokołów.
9. Rozwiązanie powinno zawierać zintegrowany serwer proxy z funkcją cache.
10. Rozwiązanie powinno umożliwiać wdrożenie serwera proxy w dwóch trybach:
    a) jawne proxy (explicit proxy), gdy przeglądarki na komputerach w sieci muszą zostać skonfigurowane ręcznie lub z wykorzystaniem mechanizmów PAC (Proxy Auto Configuration) oraz WPAD (Web Proxy Auto Discovery),
    b) przezroczyste proxy (transparent proxy), gdy ruch z komputerów jest przekierowywany na serwer proxy w sieci. W tym drugim przypadku przekierowanie ruchu na serwer proxy powinno być możliwe z wykorzystaniem przełącznika sieciowego i informacji dostępnych w warstwie 4 modelu ISO/OSI, trasowania opartego o polityki (PBR - policy based routing) lub protokołu WCCP v2.
11. Wymagane jest, aby dostarczony serwer proxy mógł zostać skonfigurowany dla poprawnego działania we współpracy z innymi serwerami proxy w konfiguracji hierarchicznych łańcuchów proxy (proxy chaining), zarówno jako serwer podrzędny (downstream) oraz nadrzędny (upstream).
12. Na serwerze proxy powinno być możliwe uwierzytelnienie użytkowników z wykorzystaniem mechanizmów Kerberos, LDAP oraz NTLM.
13. W przypadku, gdy dostarczone proxy zostanie wdrożone, jako nadrzędne musi ono potrafić skorzystać z informacji dotyczących uwierzytelnionego użytkownika, jeżeli tylko są one dostarczane przez proxy podrzędne.
14. Rozwiązanie powinno umożliwiać zbudowanie klastra wysokiej dostępności serwerów cache.
15. Powinno być możliwe również zapewnienie wysokiej dostępności serwerów cache przy wykorzystaniu mechanizmu wirtualnego IP.
16. Zawarty w rozwiązaniu serwer proxy musi umożliwiać kategoryzację odwiedzanych przez użytkowników stron internetowych na podstawie ich bieżącej zawartości. Powinno być możliwe ograniczenie analizy zawartości stron internetowych w czasie rzeczywistych do tych, których nie ma w bazie URL dostarczanej przez producenta oraz

kilku kategorii wskazanych przez producenta. Ta funkcjonalność powinna w szczególności dotyczyć dynamicznych stron Web 2.0.

17. Rozwiązanie powinno umożliwiać zarządzanie możliwością wykonywania w ramach popularnych portali społecznościowych wybranych funkcji takich jak np. użycie funkcji chat, publikowanie komentarzy, zdjęć, materiałów video.

18. Serwer proxy musi umożliwiać usuwanie aktywnej zawartości jak ActiveX, JavaScript, oraz VBScript z zawartości serwowanej użytkownikom.

19. Serwer proxy musi umożliwiać blokowanie złośliwej zawartości jak szkodliwe oprogramowanie i wirusy z wykorzystaniem zarówno tradycyjnego skanowania antywirusowego jak i zaawansowanych technik wykrywania zagrożeń jak heurystyka.

20. Polityki dotyczące skanowania bezpieczeństwa zawartości powinny umożliwiać tworzenie wyjątków dla poszczególnych stron internetowych w zakresie kategoryzacji zawartości, skanowania zagrożeń bezpieczeństwa oraz usuwania aktywnej zawartości.

21. Rozwiązanie musi blokować dostęp do stron związanych z takimi zagrożeniami jak spyware, phishing, keylogging, oraz złośliwy kod mobilny. Rozwiązanie powinno także blokować ruch wychodzący do internetu generowany przez oprogramowanie typu spyware obecne na zainfekowanych komputerach w sieci.

22. Administrator systemu musi mieć możliwość zabronić, lub zezwolić na dostęp pracowników firmy do stron z określonych kategorii korzystając z takich wyznaczników jak użytkownik, grupa użytkowników, adres IP stacji, zakres adresów IP, dzień tygodnia, pora dnia, lub czas przebywania w danych ośrodkach web.

23. Rozwiązanie powinno umożliwić użytkownikowi uzyskanie dostępu do strony z zablokowanej kategorii na podstawie znajomości hasła. Powinna istnieć możliwość definiowania indywidualnych haseł użytkowników jak również dla ich grup.

24. Rozwiązanie oprócz blokowania dostępu do stron wybranych kategorii powinno umożliwiać wyświetlenie na ekranie użytkownika informacji, iż strona, którą chce wyświetlić jest zabroniona przez politykę firmy z możliwością wejścia na tą stronę po świadomym wyrażeniu chęci przez użytkownika.

25. Rozwiązanie musi umożliwiać pełne dostosowanie stron z komunikatami dla użytkowników do własnych potrzeb, wliczając zmiany komunikatów oraz grafiki, np. umieszczenie własnego logo.

26. Administrator systemu powinien mieć możliwość tworzenia polityki dostępu do zasobów internetu także w oparciu o zajętość pasma sieciowego. Np. powinna istnieć możliwość zabronienia dostępu do określonych kategorii, gdy zajętość pasma sieciowego wyniesie 50%, itp.

27. Dodatkowo tworzenie polityki dostępu do stron internetowych powinno uwzględniać również:
    a) Słowa kluczowe zawarte w adresie URL
    b) Typy plików

28. Rozwiązanie musi posiadać możliwość przezroczystej identyfikacji użytkowników wychodzących do internetu, oraz pozwalać na integrację z następującymi usługami katalogowymi: Active Directory (Native/Mixed Mode), Sun Java System Directory Server, Novell Directory via LDAP umożliwiając egzekwowanie polityk przypisanych do indywidualnych użytkowników lub ich grup.

29. W przypadku braku informacji identyfikujących użytkownika powinna istnieć możliwość wymuszenia uwierzytelnienia użytkownika przez Rozwiązanie.

30. Rozwiązanie musi być wyposażone w moduł raportujący, umożliwiający:
    - Generowanie raportów z podziałem na pojedynczych użytkowników ich grupy, kategorie i protokoły. Raporty te powinny być dostępne przez przeglądarkę.
    - Generowanie w/w raportów ale z ukryciem danych pozwalających zidentyfikować użytkownika (na raporcie zamiast adresu IP, nazwy, loginu itp., powinny być identyfikatory nieznaczące – np. liczby).
    - Bieżący wgląd w aktywność użytkowników.

31. Przeglądanie aktywności użytkowników powinno móc wykorzystywać takie kryteria jak:
    a) Adres URL
    b) Kategoria adresu URL
    c) Źródłowy adres IP
    d) Docelowy adres IP

e) Port
f) Protokół
g) Domena
h) Grupa użytkowników
i) Użytkownik
j) Akcja
k) Dzień

32. Aktywność użytkowników powinna być przedstawiana z wykorzystaniem miar takich jak:
    a) Ilość żądań (Hit) lub wizyt (wyświetleń stron)
    b) Ilość danych wysłanych np. w KB
    c) Ilość danych pobranych np. w KB
    d) Ilość danych (wysłanych + pobranych) np. w KB
    e) Czas przeglądania

33. Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie powinny być dostępne przez zintegrowaną webową konsolę administracyjną z możliwością delegacji uprawnień do administrowania poszczególnymi składnikami i opcjami systemu.

34. Rozwiązanie powinno umożliwiać delegowanie uprawnień do zarządzania i raportowania zarówno dla użytkowników domenowych jak i użytkowników tworzonych w bazie oprogramowania filtrującego.

35. W przypadku delegacji uprawnień powinno być możliwe zablokowanie przez administratora nadrzędnego możliwości odblokowania wybranych kategorii przez administratora podrzędnego.

36. Główny administrator oprogramowania filtrującego powinien mieć możliwość wglądu w szczegółowy audyt aktywności pozostałych administratorów zawierający następujące informacje:
    a) Data akcji,
    b) Nazwa administratora, który przeprowadził akcję
    c) Element, na którym podejmowana jest akcja,
    d) Akcja (np. zalogowanie, wylogowanie, oraz dodanie, zmiana i usunięcie obiektu),
    e) W przypadku zmiany obiektu jego poprzednia i obecna wartość.

37. Dostęp do webowej konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu https.

38. Konsola powinna umożliwiać zintegrowane zarządzanie rozwiązaniami tego samego producenta do ochrony poczty elektronicznej oraz ochrony przed wyciekiem danych (DLP).

39. Konsola zarządzająca powinna zawierać ekran przedstawiający wykres sumarycznej aktywności z ostatnich 24 godzin oraz podstawowe statystki jak najpopularniejsze kategorie, najczęściej blokowani użytkownicy, oraz inne. Powinna istnieć możliwość dostosowania tego widoku do własnych potrzeb. Ekran ten musi również zawierać ostrzeżenia dotyczące poprawności pracy poszczególnych komponentów oprogramowania.

40. Zawarte w rozwiązaniu proxy powinno umożliwiać inspekcję szyfrowanych połączeń HTTPS.

41. Podczas nawiązywania połączenia z komputera użytkownika do serwera docelowego serwer proxy musi móc przeprowadzić kontrolę najważniejszych aspektów związanych z certyfikatem jakim legitymuje się serwer docelowy, włączając w to:
    a) zgodność adresu zawartego w certyfikacie (podmiot certyfikatu) i żądanego przez użytkownika,
    b) datę ważności certyfikatu,
    c) kontrolę pełnego łańcucha certyfikacji,
    d) unieważnienie certyfikatu z wykorzystaniem CRL oraz OCSP.

42. Rozwiązanie powinno utrzymywać i umożliwiać administratorom zarządzanie listą zaufanych głównych urzędów certyfikacji (Trusted Root CA) wykorzystywaną przy weryfikowaniu certyfikatów serwerów docelowych.

43. Możliwa powinna być konfiguracja, w której użytkownicy są ostrzegani przed nieprawidłowościami, ale mogą kontynuować. Informacje o takich zdarzeniach powinny być widoczne w konsoli zarządzającej w postaci incydentów umożliwiających zdefiniowanie administratorowi akcji dla takich połączeń w przyszłości. Akcje powinny zawierać co najmniej:
    a) blokowanie, ale z możliwością kontynuowania, jeżeli taka opcja jest globalnie włączona dla użytkowników
    b) blokowanie bez możliwości kontynuowania dla tej strony, nawet jeżeli taka opcja jest globalnie włączona dla użytkowników
    c) wyłączenie inspekcji https dla tej strony, czyli tunelowanie połączenia przez proxy

44. Musi być możliwe dostosowanie stron wyświetlanych użytkownikom w przypadku wykrytych przez proxy nieprawidłowości oraz błędów.

45. Serwer proxy musi umożliwiać zarządzanie połączeniami do serwerów docelowych wymagających certyfikatu klienta w celu uwierzytelnienia połączenia.

46. Rozwiązanie powinno umożliwiać wyłączenie skanowania połączeń HTTPS dla określonych kategorii stron internetowych zapewniając zachowanie prywatności przez użytkowników korzystających np. z serwisów bankowości internetowej.

47. Konsola zarządzająca dla serwera proxy musi udostępniać dostęp do aktualnych oraz historycznych danych dotyczących działania serwera proxy jak:
    a) Ilość operacji na sekundę
    b) Przepustowość w Mbit na sekundę
    c) Współczynnik trafień dla serwera cache
    d) Wykorzystanie przestrzeni cache na dysku
    e) Wykorzystanie przestrzeni cache w pamięci RAM
    f) Wykorzystanie cache DNS
    g) Błędy http
    h) Obciążenie procesora

48. Rozwiązanie powinno być dostępne w postaci oprogramowania instalowanego na odpowiednio dobranych serwerach oraz jako rozwiązanie sprzętowe na dedykowanej platformie wykorzystującej mechanizmy wirtualizacji dostarczanej przez tego samego producenta w formie urządzenia do montażu w rack.

49. Rozwiązanie musi oferować dodatkowe możliwości rozbudowy swojej funkcjonalności np poprzez integrację z systemem DLP. W wyniku takiej integracji analiza wychodzącego ruchu HTTP i HTTPS pod kątem polityk DLP powinna być realizowana przez silnik serwera proxy bez konieczności wykorzystania protokołu ICAP w celu przekazania próbek do analizy przez serwer DLP.

Specyfikacja wymagań w zakresie kontroli dostępu do ochrony przed wyciekiem informacji (DLP)

1. System musi umożliwiać ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.

2. System musi realizować swoje funkcje zarówno na poziomie sieci (Network DLP) oraz stacji końcowej jak komputer, czy laptop (Endpoint DLP).

3. Zarządzanie, obsługa incydentów, oraz raportowanie musi być spójne dla ochrony na poziomie sieci i stacji końcowych i odbywać się z pojedynczej webowej konsoli zarządzającej.

4. Dostęp do konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu https.

5. Ochrona informacji powinna odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.

6. System musi umożliwiać monitorowanie i ochronę wielu kanałów komunikacyjnych, w szczególności:
    a) http oraz https
    b) email
    c) komunikatory internetowe

7. System musi umożliwiać definiowanie własnych kanałów transmisji, które mają być monitorowane.

8. System w zakresie stacji końcowej musi umożliwiać monitorowanie takich czynności jak kopiowanie informacji na zewnętrzne nośniki danych, nagrywanie płyt, lokalne drukowanie, wklejanie informacji w okna aplikacji.

9. System musi umożliwiać tworzenie polityk uwzględniających takie akcje jak:
    a) wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym powiadamiane powinny być następujące osoby:
        i. nadawca, czyli osoba, która wysyłała informacje,
        ii. zwierzchnik nadawcy,
        iii. właściciel informacji zdefiniowany w polityce,
        iv. właściciel polityki.
    b) blokowanie transmisji naruszających zdefiniowaną politykę,
    c) kwarantannę informacji,
    d) szyfrowanie informacji,

e) umożliwienie użytkownikowi kontynuowania operacji po zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na stacji końcowej.

10. System musi umożliwiać łączenie polityk w grupy.

11. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
    a) Kto wysyła informacje,
    b) Gdzie informacje są wysyłane,
    c) W jaki sposób informacje są wysyłane (patrz punkt 6),
    d) Co jest wysyłane, czyli właściwa identyfikacja treści (patrz punkt 12).

12. System musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
    a) słowa kluczowe,
    b) wyrażenia regularne,
    c) tworzenie odcisku palca – fingerprint,
    d) Algorytmy Machine Learning

13. Algorytm tworzenia odcisku palca musi tworzyć wiele odcisków palca dla pojedynczego pliku, tak aby chronić informacje zawarte w pliku a nie wyłącznie dokument w całości.

14. System musi również umożliwić tworzenie odcisków palca z zasobów zawartych w bazach danych. Tworzenie takich odcisków powinno odbywać się bez uprzedniego kopiowania informacji do pliku (np. za pomocą ODBC).

15. System musi zawierać predefiniowane reguły ochrony informacji, dotyczące np. numerów krat kredytowych, IBAN, oraz takich identyfikatorów jak PESEL, REGON, NIP, nr Dowodu Osobistego.

16. System musi umożliwiać integrację z usługami katalogowymi umożliwiająca m.in.:
    a) przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,
    b) przypisanie użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,
    c) wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o zwierzchniku użytkownika.

17. Producent systemu DLP musi w swoim portfolio produktów oferować system Web Security oraz filtrowania URL, który w integracji z systemem DLP będzie udostępniał dodatkowe informacje widoczne w szczegółach incydentu, np. kategoria strony internetowej do której miejsce miał transfer informacji.

18. System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego (funkcjonalność Discovery). Funkcjonalność ta powinna być również oferowana dla folderów Exchange, serwera SharePoint oraz baz danych.

19. Konsola zarządzająca powinna zawierać ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.

20. Konsola zarządzająca powinna umożliwiać zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora.

21. System musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów.

22. System w ramach odnotowanych incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana.

23. Producent systemu musi w swoim portfolio produktów oferować serwer proxy i cache umożliwiający inspekcję SSL i przekazywanie informacji wysyłanych tym kanałem do systemu DLP w celu sprawdzenia zgodności z polityką ochrony informacji. Integracja powinna wykorzystywać znany protokół komunikacji jak np. ICAP.

24. Producent systemu DLP oprócz rozwiązań bezpieczeństwa danych, musi również dostarczać rozwiązań bezpieczeństwa poczty elektronicznej oraz bezpieczeństwa web. Dzięki temu jest on w stanie w swoich laboratoriach m.in. analizować na jakie strony prowadzą odnośniki umieszone w wiadomościach email (spam), dokonywać ich kategoryzacji oraz badać na ile ich odwiedzanie jest niebezpieczne.

25. System musi umożliwiać rozpoznawanie tekstu zawartego w plikach graficznych i jego analize pod względem wrażliwości informacji (OCR). Ta funkcjonalność powinna być oferowana zarówno dla skanowania dokumentów jak i dla dokumentów graficznych wysyłanych poprzez styk z Internetem (smtp, http, https)

26. Oprogramowanie klienckie (Endpoint) powinno być oferowane w polskiej wersji językowej.

Specyfikacja wymagań w zakresie ochrony DLP dla aplikacji chmurowych

1. System umożliwia ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.
2. System ochrony aplikacji chmurowych integruje się z istniejącym systemem klasy DLP Zamawiającego.
3. System realizuje swoje funkcje za pośrednictwem API, które komunikuje się z aplikacją oferowanymi jako SaaS, w szczególności MS 365 oraz Google for Business.
4. Zarządzanie, obsługa incydentów oraz raportowanie jest spójne dla ochrony na poziomie sieci, stacji końcowych oraz aplikacji chmurowych i odbywa się z pojedynczej webowej konsoli zarządzającej.
5. Dostęp do konsoli zarządzającej odbywa się w bezpiecznym połączeniu https.
6. Ochrona informacji odbywa się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.
7. System umożliwia stosowanie polityk granularnie dla różnych aplikacji SaaS.
8. System umożliwia tworzenie polityk uwzględniających takie akcje jak:
   a) wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym powiadamiane powinny być następujące osoby:
      - ✓ nadawca, czyli osoba, która wysyłała informacje
      - ✓ zwierzchnik nadawcy,
      - ✓ właściciel informacji zdefiniowany w polityce,
      - ✓ właściciel polityki,
   b) blokowanie transmisji wychodzących (upload) naruszających zdefiniowaną politykę,
   c) blokowanie transmisji przychodzących (download) naruszających zdefiniowaną politykę,
   d) kwarantannę informacji,
   e) kwarantannę informacji wraz z notyfikacją użytkownika,
   f) utworzenie bezpiecznej kopii informacji,
   g) usuwanie uprawnień udostępniania dostępu do informacji dla osób zewnętrznych (unshare external),
   h) usuwanie uprawnień udostępniania dostępu do informacji dla wszystkich odbiorców (unshare all),
9. System umożliwia łączenie polityk w grupy.
10. System umożliwia budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
    a) kto wysyła informacje,
    b) gdzie informacje są wysyłane,
    c) w jaki sposób informacje są wysyłane,
    d) co jest wysyłane, czyli właściwa identyfikacja treści,
11. System wykorzystuje szeroką gamę mechanizmów identyfikowania treści, m.in.:
    a) słowa kluczowe,
    b) wyrażenia regularne,
    c) tworzenie odcisku palca – fingerprinting,
    d) algorytmy Machine Learning,
    e) weryfikacja klasyfikacji treści w przypadku, gdy stosowane jest rozwiązanie typu „Data Classification”,
    f) typ pliku – mechanizm odporny na zmianę rozszerzenia,
    g) nazwa pliku,
    h) rozmiar pliku.
12. Algorytm tworzenia odcisku palca działa tak, aby chronić informacje zawarte w pliku (również jego fragmenty), a nie wyłącznie dokument w całości.
13. System umożliwia tworzenie odcisków palca z zasobów zawartych w bazach danych.
14. System zawiera predefiniowane reguły ochrony informacji, dotyczące np. numerów krat kredytowych, IBAN oraz takich identyfikatorów jak PESEL, REGON, NIP, nr Dowodu Osobistego.
15. System umożliwia aktywowanie ochrony DLP na kanale chmurowym przy wykorzystaniu istniejących polityk w systemie Zamawiającego.

16. System umożliwia zautomatyzowane wykrywanie informacji objętych politykami ochrony umieszczonych w aplikacjach chmurowych zarządzanych przez Zamawiającego (funkcjonalność Cloud Discovery).

17. Konsola zarządzająca umożliwia zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora.

18. System umożliwia ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów.

19. System w ramach odnotowanych incydentów udostępnia informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana. Wgląd w tak szczegółowe informacje jest kontrolowany zgodnie z uprawnieniami administratora.

20. System posiada możliwość rozbudowy o ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS, w szczególności MS O365 oraz Google for Business.

21. Ochrona informacji w chmurze opiera się o te same mechanizmy stosowane w rozwiązaniu lokalnym włączając Fingerprinting oraz Machine Learning.

22. System posiada funkcjonalność klasyfikowania informacji (w tym plików oraz wiadomości pocztowych email), lub w pełni integrować się z takim rozwiązaniem.

Specyfikacja wymagań w zakresie ochrony poczty elektronicznej

1. System ochrony musi realizować funkcje ochrony antyspamowej dla ruchu SMTP.

2. System musi umożliwiać filtrowanie poczty zarówno przychodzącej, wychodzącej jak i komunikacji wewnętrznej, dla tego powinno być możliwe definiowanie osobnego zestawu polityk dla każdego z kierunku przesyłania wiadomości.

3. System zarządzania politykami musi umożliwiać jednokrotne definiowanie elementów takich jak filtry i akcje a następne ich wielokrotne wykorzystywanie w występujących w politykach regułach.

4. Możliwe do podjęcia w ramach polityk akcje powinny obejmować co najmniej:
   a) dostarczenie wiadomości z wykonaniem dodatkowych akcji:
      - zmodyfikowanie tematu wiadomości
      - usunięcie i/lub dodanie nagłówka X-header
      - wysłanie kopii wiadomości pod wskazany adres lub adresy email
   b) zablokowanie wiadomości
   c) zapisanie wiadomości do wskazanej kolejki
   d) wysłanie powiadomienia, gdzie:
      - jego nadawcą może być oryginalny nadawca, administrator lub wskazany adres
      - jego odbiorcą może być oryginalny nadawca, oryginalny adresat, administrator, wskazany adresat lub adresaci (wszyscy z wymienionych lub dowolnie wybrani)
      - temat i zawartość powiadomienia mogą być w pełni dostosowane do potrzeb
      - do powiadomienia może być dołączona oryginalna wiadomość przed lub po filtrowaniu.

5. Każda z polityk powinna składać się z reguł które powinny być przetwarzane w kolejności „z góry na dół”, do końca listy reguł, lub do reguły, która wprowadzi akcję końcową np. zablokuj wiadomość, lub umieść w kwarantannie.

6. System musi umożliwiać wykorzystanie co najmniej dwóch systemów badania reputacji nadawców dla poczty przychodzącej. Jednym z nich musi być dowolny, publiczny serwis Real-Time Blacklist (RBL) drugi zaimplementowany w rozwiązaniu powinien traktować jako spamerów tych z nadawców dla których odsetek spamu w wiadomościach przekroczył jeden ze zdefiniowanych poziomów: 97%, 99%, albo 100%.

7. System musi wykorzystywać funkcję reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie szeregu weryfikacji, oraz odrzucenie połączenia w przypadku:
   a) braku rekordu PTR
   b) niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS,
   c) niezgodności rekordu PTR z rekordem A

8. System musi umożliwiać weryfikacja, czy nadawca jest autoryzowany do wysyłania wiadomości z określonym polem nadawcy w oparciu o SPF (Sender Policy Framework). System musi umożliwiać co najmniej:

a) odrzucenie wiadomości jeżeli rekord SPF nie istnieje
b) odrzucenie wiadomości jeżeli rekord SPF nie pasuje do domeny nadawcy

9. W ramach ochrony przed atakami Directory Harvest system musi umożliwiać monitorowanie i ograniczanie ilości połączeń z jednego adresu IP w określonym przedziale czasu. Powinna istnieć możliwość zdefiniowania okresu czasu od 1 sekundy do 1 godziny oraz osobnego ograniczenia maksymalnej ilości połączeń i wiadomości.

10. Dodatkowo powinna istnieć możliwość tymczasowego zablokowania na zdefiniowany czas przyjmowania wiadomości z adresów IP dla których odnotowano wiadomości zawierające określoną liczbę niewłaściwych adresatów z chronionej domeny.

11. System musi zawierać moduł DLP klasy Enterprise umożliwiający identyfikację chronionych informacji z użyciem mechanizmów:
    a) słowa kluczowe
    b) słowniki
    c) wyrażenia regularne
    d) właściwości przesyłanych plików takie jak prawdziwy typ pliku, jego nazwa lub rozmiar
    e) cyfrowe identyfikatory (fingerprint) tworzone dla danych nieuporządkowanych takich jak pliki na serwerach plików
    f) cyfrowe identyfikatory (fingerprint) tworzone dla danych uporządkowanych np przechowywanych w bazach danych.

12. System musi umożliwiać zarządzanie kolejkami (folderami) dla blokowanych wiadomości w zakresie zarządzania predefiniowanymi oraz tworzenia nowych. Wiadomości kierowane do określonych kolejek powinny móc być przechowywane w ramach urządzenia appliance lub poza nim na zasobie dostępnym przez NFS lub Samba.

13. System musi umożliwiać wdrożenie w konfiguracji wysoce dostępnego klastra active-active. Maksymalna ilość urządzeń w klastrze nie powinna być mniejsza niż 8.

14. Rozwiązanie musi być wyposażone w moduł raportujący, umożliwiający:
    a) Generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem.
    b) Harmonogram musi umożliwiać generowanie raportów codziennie, co tydzień lub co miesiąc. W przypadku opcji co tydzień powinno być możliwe dowolne wskazanie wybranych dni tygodnia. W przypadku opcji co miesiąc powinno być możliwe dowolne wskazanie wybranych dni miesiąca np. 2, 15, 17-31.
    c) Harmonogram musi umożliwiać generowanie raportów, dla wszystkich dat, zdefiniowanego okresu lub relatywnie czyli za okres np. ostatniego dnia, tygodnia, miesiąca w zakresie od 1 do 5 dla każdego z nich.
    d) Powinno być możliwe dostarczanie raportów w postaci plików pdf, xls, oraz html.
    e) Powinno być możliwe dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.

15. Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie powinny być dostępne przez zintegrowaną webową konsolę administracyjną z możliwością delegacji uprawnień do administrowania poszczególnymi składnikami i opcjami systemu.

16. Rozwiązanie powinno umożliwiać delegowanie uprawnień do zarządzania i raportowania zarówno dla użytkowników domenowych jak i użytkowników tworzonych w bazie oprogramowania filtrującego.

17. Główny administrator oprogramowania filtrującego musi mieć możliwość wglądu w szczegółowy audyt aktywności pozostałych administratorów zawierający następujące informacje:
    a) Data akcji,
    b) Nazwa administratora, który przeprowadził akcję
    c) Element, na którym podejmowana jest akcja,
    d) Akcja (np. zalogowanie, wylogowanie, oraz dodanie, zmiana i usunięcie obiektu),
    e) W przypadku zmiany obiektu jego poprzednia i obecna wartość.

18. Dostęp do webowej konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu https.

19. Konsola powinna umożliwiać zintegrowane zarządzanie rozwiązaniami tego samego producenta do ochrony wykorzystania przez użytkowników stron internetowych oraz ochrony przed wyciekiem danych (DLP).

20. Konsola zarządzająca powinna zawierać ekran przedstawiający wykres sumarycznej aktywności z ostatnich 24 godzin oraz podstawowe statystki. Powinna istnieć możliwość dostosowania tego widoku do własnych potrzeb. Ekran ten musi również zawierać ostrzeżenia dotyczące poprawności pracy poszczególnych komponentów oprogramowania.

21. System musi udostępniać mechanizm pozwalający na przeglądanie przez chronionych użytkowników wiadomości umieszczonych w kwarantannie, umożliwiając im również zwolnienie wybranych wiadomości z kwarantanny.

22. Dodatkowo decyzją administratora użytkownicy powinni mieć możliwość zarządzać swoimi własnymi listami zabronionych i dopuszczonych nadawców,
23. System musi umożliwiać rozszerzenie o integrację z usługą dostarczoną przez tego producenta i działającą w chmurze, której zadaniem jest pre-filtering wiadomości w celu wykrycia wirusów oraz spamu w wiadomościach.
24. System musi umożliwiać integrację z rozwiązaniem bezpieczeństwa web tego samego producenta w celu analizy zawartych w wiadomościach adresów URL.
25. System musi umożliwiać szyfrowanie TLS oraz posiadać możliwość integracji z rozwiązaniem do szyfrowania wiadomości (tzw Encryption Gateway) firm trzecich.
26. Producent oprogramowania filtrującego oprócz rozwiązań bezpieczeństwa poczty elektronicznej, musi również dostarczać rozwiązań bezpieczeństwa web oraz ochrony przed wyciekiem poufnych informacji (DLP). Dzięki temu jest on w stanie w swoich laboratoriach m.in. analizować na jakie strony prowadzą odnośniki umieszone w wiadomościach email (spam), dokonywać ich kategoryzacji oraz badać na ile ich odwiedzanie jest niebezpieczne.

W przypadku zaproponowania rozwiązań równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.

Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

Projektowane postanowienia umowy
Umowa nr CRZP/26/01115/2022
(zamówienie publiczne nr EZP.26.178.2022)

zawarta pomiędzy:
Państwowym Instytutem Geologicznym – Państwowym Instytutem Badawczym z siedzibą w Warszawie (adres: 00-975 Warszawa, ul. Rakowiecka 4), wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000122099, NIP 525-000-80-40, Regon 000332133, reprezentowanym przez/w imieniu którego działają:
*(w przypadku przedsiębiorcy wpisanego do KRS)**
……..…, z siedzibą w …… przy ulicy ……, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy …… w …….. , …… Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: ……., NIP ……, Regon ……, *kapitał zakładowy*
reprezentowaną przez:
……..……..……
zwaną w dalszej części umowy „**Wykonawcą**”,
*(w przypadku przedsiębiorcy wpisanego do centralnej ewidencji i informacji o działalności gospodarczej)**
panem/panią …… zam. …….., ul. ……, legitymującym/ą się dowodem osobistym seria … numer ……, działającym/ą na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod firmą **……..** adres: ……, ul. ……, NIP:……., *reprezentowanym/ą przez: …… (na mocy ……..)*
zwanym/zwaną w dalszej części umowy „**Wykonawcą**”
*(w przypadku spółki cywilnej)**
panem/panią …….. zam. …….., ul. ……, legitymującym/ą się dowodem osobistym seria … numer ……, działającym/ą na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod firmą **……..** adres ……, ul. ……, NIP: ……., *reprezentowanym/ą przez: …… (na mocy ……..)*
panem/panią …….. zam. …….., ul. ……, legitymującym/ą się dowodem osobistym seria … numer ……, działającym/ą na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod firmą **……..** adres ……, ul. ……, NIP:……., *reprezentowanym/ą przez: …… (na mocy ……..)* wspólnikami spółki cywilnej …….., adres ……, NIP ……..
zwanymi w dalszej części umowy łącznie „**Wykonawcą**”
zwanymi także łącznie **Stronami.**

w rezultacie dokonanego przez Zamawiającego wyboru oferty w przetargu w trybie podstawowym pn.: **Usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB** (oznaczenie sprawy ……..), zgodnie z *ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j.:* Dz. U. z 2022 roku, poz. 1710 z późn. zm.*) – dalej „ustawa Pzp”* – została zawarta umowa (dalej „Umowa”) o następującej treści:

§ 1. Przedmiot Umowy

1. Na warunkach określonych w Umowie oraz dokumentach w niej przywołanych, oraz za cenę w niej określoną, Zamawiający odpowiednio zamawia i kupuje, a Wykonawca sprzedaje i zobowiązuje się do dostarczenia licencji systemu filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP oraz ochrony DLP dla aplikacji chmurowych zwanych dalej „Oprogramowaniem”, określonych co do rodzaju i ilości w Załączniku nr 2 do Umowy (Ofercie Wykonawcy z dnia ……r.), o minimalnych parametrach technicznych szczegółowo opisanych w Opisie Przedmiotu Zamówienia, stanowiącym Załącznik nr 1 do Umowy.

2. Ponadto, Wykonawca zobowiązuje się - przez okres i na zasadach określonych w Opisie przedmiotu zamówienia – do świadczenia wsparcia technicznego (maintenance) dla dostarczonego Oprogramowania, obejmującego w szczególności konsultacje, pomoc i porady dotyczące problemów technicznych, w tym usuwanie błędów działania systemu oraz dostęp do najnowszej wersji oprogramowania, aktualizacji polityk i filtrów we wszystkich modułach (WEB \ DLP \ E-MAIL).

3. Zamawiający dopuszcza, aby Oprogramowanie, wchodzące w skład Przedmiotu Umowy, było dostarczone w wersji językowej polskiej lub angielskiej.

4. Dostarczone Oprogramowanie winno być w wersji kompatybilnej z systemami operacyjnymi MS Windows w wersji 10. Wykonawca dostarczy Zamawiającemu Oprogramowanie z kluczami licencyjnymi w formie elektronicznej, z kodami dostępu niezbędnymi do pobrania ze strony producenta Oprogramowania plików instalacyjnych wraz z dokumentacją.

5. Wykonawca oświadcza, że dostarczone przez niego Oprogramowanie nie narusza jakichkolwiek praw osób trzecich, zwłaszcza w zakresie przepisów o wynalazczości, znakach towarowych, prawach autorskich i prawach pokrewnych oraz nieuczciwej konkurencji oraz że posiada prawo do udzielania licencji/sublicencji lub odsprzedaży Oprogramowania.

6. Wykonawca podejmie wszelkie niezbędne działania, w celu zabezpieczenia Zamawiającego przed jakimikolwiek nieuprawnionymi działaniami osób trzecich zmierzających do dochodzenia swoich praw do Oprogramowania w zakresie własności intelektualnej, o ile działania tych osób trzecich i ewentualne naruszenia praw do Oprogramowania w zakresie własności intelektualnej mają związek z obowiązkami Wykonawcy wynikającymi z niniejszej Umowy. W przypadku wystąpienia osób trzecich z roszczeniami mającymi na celu dochodzenie ich praw w tym zakresie wobec Zamawiającego, Wykonawca zobowiązuje się zwolnić Zamawiającego z jakiejkolwiek odpowiedzialności z tego tytułu w szczególności zaś zobowiązuje się pokryć wszelkie koszty związane z prowadzonymi przez Zamawiającego postępowaniami oraz wypłacone przez Zamawiającego odszkodowania z tego tytułu.

7. W odniesieniu do kolejnych wersji Oprogramowania udoskonalonych w drodze tzw. upgrade'ów i update'ów, Zamawiającemu przysługują takie same uprawnienia, jak w stosunku do wersji pierwotnej Oprogramowania.

8. Wykonawca zapewnia i oświadcza, że posiada wiedzę, doświadczenie, urządzenia i narzędzia informatyczne niezbędne do prawidłowego wykonania Umowy, a ponadto zobowiązuje się wykonać przedmiot Umowy z należytą starannością, profesjonalnie, przy zachowaniu zasad współczesnej wiedzy i najlepszych praktyk, właściwych dla rodzaju usługi będącej przedmiotem Umowy, zgodnie ze standardami obowiązującymi w branży informatycznej, obowiązujących w tym zakresie przepisów oraz zgodnie z zachowaniem najwyższych standardów jakości.

§ 2. Termin realizacji Umowy i warunki dostawy

1. Wykonawca zobowiązuje się dostarczyć Oprogramowanie, o którym mowa w § 1 ust. 1 Umowy wraz z dokumentami potwierdzającymi prawo Zamawiającego do asysty technicznej (Certyfikat Asysty Technicznej) w terminie do 31 grudnia 2022 r. W terminie wskazanym *w zdaniu poprzedzającym Wykonawca zobowiązany jest również do instalacji, konfiguracji i integracji Oprogramowania stosownie do wymagań Opisu Przedmiotu Zamówienia* (dotyczy licencji Oprogramowania równoważnego).*
   Oprogramowanie dostarczone będzie drogą elektroniczną poprzez umożliwienie Zamawiającemu pobrania Oprogramowania ze wskazanego przez Wykonawcę zasobu internetowego oraz dostarczenie dokumentów potwierdzających udzielenie licencji, informacji niezbędnych do instalacji/uruchomienia Oprogramowania oraz kluczy licencyjnych/aktywacyjnych, które uruchomią procedurę dostępu oraz pozwolą na korzystanie z Oprogramowania.
   2. Wykonawca zobowiązuje się do świadczenia wsparcia technicznego o którym mowa w § 1 ust. 2 Umowy w terminach:
   1) zamówienie gwarantowane – od dnia 01.01.2023 r. do dnia 31.12.2023 r.,
   2) zamówienie opcjonalne – od dnia 01.01.2024 r. do dnia 31.12.2024 r.
   3) Zamawiający poinformuje Wykonawcę o zamiarze skorzystania z prawa opcji o którym mowa w ust 2 pkt 2 powyżej nie później niż do dnia 15.12.2023 r. Prawo opcji realizowane będzie na takich samych warunkach jak zamówienie gwarantowane

§ 3. Wynagrodzenie i warunki płatności

1. Łączne wynagrodzenie za realizację przedmiotu zamówienia ustala się na kwotę netto ……. zł (słownie: …… złotych ……./100) tj. brutto …….. zł (słownie: …… złotych ……/100), w tym:
1) zamówienie podstawowe: netto ……. zł (słownie: …… złotych ……./100) tj. brutto …….. zł (słownie: …… złotych ……/100),
2) zamówienie opcjonalne: netto ……. zł (słownie: …… złotych ……./100) tj. brutto …….. zł (słownie: …… złotych ……/100),

zgodnie z Ofertą Wykonawcy z dnia …….., stanowiącą Załącznik nr 2 do niniejszej Umowy.
2. Wynagrodzenie ustalone na podstawie postanowień ust. 1 powyżej wyczerpuje wszelkie roszczenia Wykonawcy wobec Zamawiającego związane z realizacją Umowy i koszty, jakie poniesie Wykonawca z tytułu

należytego jej wykonania i Wykonawcy nie przysługuje od Zamawiającego zwrot jakichkolwiek kosztów poniesionych przez Wykonawcę w związku z realizacją Umowy.

3. Wynagrodzenie wskazane ust. 1 pkt 1 powyżej płatne będzie w dwóch ratach, na podstawie poprawnie wystawionych przez Wykonawcę faktur. Faktury będą doręczone Zamawiającemu, z tym, że:
   a) I rata w wysokości 25 % wynagrodzenia płatna na podstawie faktury wystawionej po podpisaniu przez Strony Protokołu odbioru bez zastrzeżeń;
   b) II rata w wysokości 75 % wynagrodzenia, płatna będzie na podstawie faktury wystawionej na początku trzeciego kwartału 2023 r.
4. Wynagrodzenie wskazane w ust. 1 pkt 2 płatne będzie w całości, na podstawie faktury wystawionej na początku pierwszego kwartału 2024 r. w przypadku skorzystania przez Zamawiającego z prawa opcji.
5. Zapłata za Przedmiot Umowy nastąpi przelewem na numer rachunku bankowego Wykonawcy wskazany na fakturze (albo, w przypadku konieczności zastosowania mechanizmu podzielonej płatności – na rachunki bankowe Wykonawcy, w tym rachunek VAT Wykonawcy, wskazane na fakturze), w terminie do 30 dni od doręczenia Zamawiającemu prawidłowej pod względem merytorycznym i formalnym faktury.
6. Za nieterminowe uregulowanie należności Wykonawcy przysługują odsetki ustawowe.
7. W przypadku, gdy usługa nie będzie wykonywana przez cały miesiąc, wynagrodzenie Wykonawcy ulega proporcjonalnemu obniżeniu do liczby dni w, których usługa była świadczona danym miesiącu.
8. Za datę dokonania płatności Strony uznają datę obciążenia rachunku bankowego Zamawiającego.
9. Wykonawca jest zobowiązany do wpisania na fakturze numeru niniejszej Umowy.
10. Wykonawca zobowiązany jest do przekazania prawidłowo wystawionej faktury, elektronicznie na adres: faktury@pgi.gov.pl przy użyciu komunikatu zwrotnego/autorespondera lub papierowo na adres: Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy, ul. Rakowiecka 4, 00 - 975 Warszawa.
11. Wykonawca bez pisemnej zgody Zamawiającego nie może przenieść na osoby trzecie w drodze przelewu lub działania o podobnym charakterze całości bądź części należności wynikających z niniejszej Umowy.
12. Zamawiający dopuszcza, na wniosek Wykonawcy, realizację płatności przed upływem terminu wynikającego z Umowy, jeżeli łącznie zostaną spełnione następujące warunki:
    1) Wykonawca wyrazi zgodę w formie elektronicznej (e-mail) lub pisemnej na pomniejszenie wynagrodzenia z danej faktury o wysokość skonta i doręczy Zamawiającemu odpowiednią fakturę korygującą;
    2) skonto jest to zmniejszenie sumy należności przez Wykonawcę, jeżeli Zamawiający decyduje się na dokonanie zapłaty przed umówionym terminem;
    3) wysokość skonta jest zależna od wartości brutto faktury i wynosi:
       a) wartość brutto faktury do 17 000,00 zł – skonto w wysokości 500,00 zł,
       b) wartość brutto faktury powyżej 17 000,00 zł do 50 000,00 zł – skonto w wysokości 3% wartości faktury brutto, nie mniej niż 800,00 zł,
       c) wartość brutto faktury powyżej 50 000,00 zł do 100 000,00 zł – skonto w wysokości 2% wartości faktury brutto, nie mniej niż 1 500,00 zł,
       d) wartość brutto faktury powyżej 100 000,00 zł – skonto w wysokości 1% wartości faktury brutto, nie mniej niż 2 000,00 zł;
    4) Wykonawca na dzień złożenia wniosku nie ma naliczonych kar umownych ani nie jest nimi zagrożony;
    5) płatność nastąpi nie wcześniej niż po upływie 10 dni licząc od daty otrzymania faktury.
13. Zamawiający zastrzega, iż realizacja płatności przed upływem terminu wynikającego z Umowy, stanowi wyłącznie uprawnienie Zamawiającego, a Wykonawca nie ma roszczenia o realizację płatności przed ustalonym terminem zapłaty wynikającym z Umowy.
14. Wykonawca oświadcza, że w przypadku, gdy transakcje będące przedmiotem Umowy, są objęte solidarną odpowiedzialnością za zobowiązania podatkowe, o których mowa w przepisach o podatku od towarów i usług, wykona prawidłowo zobowiązania podatkowe, w szczególności prawidłowo określi stawki podatku od towarów i usług oraz wpłaci na rachunek urzędu skarbowego kwotę podatku od towarów i usług przypadającą na te transakcje. W przypadku uznania przez administrację podatkową, że z tytułu przedmiotu transakcji Wykonawca / Zamawiający nie wykonał prawidłowo zobowiązań podatkowych, Wykonawca zobowiązuje się do poniesienia obciążeń nałożonych na Zamawiającego przez administrację podatkową.
15. Zamawiający oświadcza, że jest czynnym podatnikiem podatku VAT i posiada numer identyfikacyjny NIP 525 000 80 40.
16. Wykonawca oświadcza, że jest / nie jest zarejestrowanym czynnym/zwolnionym podatnikiem podatku VAT i posiada numer identyfikacyjny NIP ..... oraz zobowiązuje się do poinformowania Zmawiającego o każdej zmianie statusu podmiotu VAT najpóźniej z doręczeniem faktury. W przypadku nie wypełnienia obowiązku informacyjnego Wykonawca zobowiązuje się do poniesienia obciążeń nałożonych na Zamawiającego przez administrację podatkową, z tego powodu.
17. Wykonawca zarejestrowany na potrzeby podatku od towarów i usług jako podatnik VAT czynny oświadcza, że w fakturach wystawionych w związku z wykonywaniem przedmiotu niniejszej Umowy, każdorazowo będzie

wskazany rachunek banku, który jest ujawniony w wykazie podmiotów, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług („wykaz podatników VAT").

18. W przypadku wskazania przez Wykonawcę zarejestrowanego na potrzeby podatku od towarów i usług jako podatnik VAT czynny w fakturze rachunku bankowego nieujętego w wykazie podmiotów VAT, Zamawiający uprawniony będzie do dokonania zapłaty na dowolny rachunek bankowy Wykonawcy ujawniony w wykazie podatników VAT na dzień zlecenia przelewu. W razie braku jakiegokolwiek rachunku Wykonawcy ujawnionego w powyższym wykazie, bieg terminu płatności rozpoczyna się od dnia wskazania przez Wykonawcę (na adres dla doręczania faktur), dla potrzeb płatności, rachunku bankowego ujawnionego w wykazie płatników VAT.
19. Wykonawca zarejestrowany na potrzeby podatku od towarów i usług jako podatnik VAT czynny oświadcza, że zapłata przez Zamawiającego na rachunek ujawniony w wykazie podatników VAT stanowić będzie zapłatę wynagrodzenia.
20. Za termin zapłaty Strony uznają datę obciążenia rachunku Zamawiającego.
21. W przypadku opóźnienia Zamawiającego w zapłacie wynagrodzenia Wykonawca upoważniony jest do naliczenia odsetek ustawowych.
22. Bez zgody Zamawiającego Wykonawca nie może przenieść na osoby trzecie wierzytelności wynikających z Umowy.
23. Zamawiający niniejszym oświadcza, iż w rozumieniu art. 4c ustawy z dnia 8.03.2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j. Dz. U z 2022 roku, poz. 893) posiada status dużego przedsiębiorcy.
24. *Wykonawca oświadcza, że jest osobą fizyczną wykonującą działalność gospodarczą, zatrudniającą pracowników, zawierającą umowy zlecenie lub umowy o świadczenie usług, i tym samym nie zachodzi konieczność przedkładania przez niego, na potrzeby Umowy, informacji, o której mowa w art 8b ust. 2 ustawy o minimalnym wynagrodzeniu za pracę. W przypadku zmiany w wyżej wymienionych warunkach wykonywania działalności, Wykonawca zobowiązuje się do niezwłocznego pisemnego poinformowania o tym fakcie Zamawiającego, oraz do przedłożenia w formie pisemnej, elektronicznej lub dokumentowej informacji o liczbie godzin wykonania zlecenia lub świadczenia usług, w terminie poprzedzającym termin wypłaty wynagrodzenia, nie później niż w terminie przedłożenia Zamawiającemu faktury lub innego dokumentu księgowego. (jeśli dotyczy)*

§ 4. Odbiór przedmiotu Umowy

1. Z czynności odbioru przedmiotu Umowy Strony sporządzą Protokół odbioru z udziałem przedstawicieli obu Stron, w terminie nie dłuższym niż 2 dni od daty wydania (udostępnienia) Zamawiającemu przedmiotu odbioru. Wzór protokołu odbioru stanowi **Załącznik nr 3** do Umowy.
2. Protokół odbioru będzie zawierał wszelkie ustalenia dokonane w toku odbioru, w tym ujawnione wady, braki, jak też termin wyznaczony Wykonawcy na usunięcie stwierdzonych w trakcie odbioru ewentualnych zastrzeżeń (nie dłuższy niż 3 dni), o ile w ramach odbioru Strony nie uzgodnią wszelkich zaistniałych rozbieżności, przy czym podpisanie bez zastrzeżeń protokołu odbioru potwierdza fakt należytego wykonania Umowy i jest podstawą do wystawienia przez Wykonawcę faktury VAT. Warunkiem podpisania protokołu odbioru bez zastrzeżeń jest dostarczenie przedmiotu Umowy, w tym certyfikatu asysty technicznej, zgodnie z wymogami określonymi Umową i jej załącznikami a *w przypadku licencji Oprogramowania równoważnego realizacja obowiązku, o którym mowa w § 2 ust. 1 Umowy, zdanie drugie.*
3. Do podpisywania Protokołu odbioru wyznacza się:
   1. ze strony Zamawiającego: p. **……..**;
   2. ze strony Wykonawcy: p. **…….**;
4. Bez podpisów ww. osób upoważnionych do dokonania czynności odbioru, czynność odbioru jest bezskuteczna i nie stanowi podstawy do wystawienia przez Wykonawcę faktury.
5. Zmiana przedstawicieli Stron wskazanych w ust. 3 lub ich danych teleadresowych następuje poprzez zawiadomienie dokonywane na piśmie lub na adres poczty elektronicznej drugiej Strony, pod rygorem uznania korespondencji wysłanej na dotychczasowy adres za skutecznie doręczoną. Zmiana danych nie wymaga sporządzenia aneksu do Umowy.
6. Strony zobowiązują się do wzajemnego przekazywania sobie niezwłocznie wszelkich informacji mogących mieć wpływ na realizację Umowy. Wykonawca niezwłocznie udzieli odpowiedzi w formie pisemnej na zgłaszane przez Zamawiającego uwagi dotyczące realizacji Przedmiotu Umowy, w terminie nie dłuższym niż 2 dni robocze od dnia zgłoszenia uwag.

§ 5. Warunki wsparcia technicznego

1. Wsparcie techniczne realizowane będzie bez limitu na ilość zgłoszeń, przez wykwalifikowane osoby, posiadające wiedzę niezbędną do realizacji takiej usługi.
2. W ramach wsparcia technicznego Wykonawca zobowiązuje się w szczególności do konsultacji, pomocy i udzielenia porad dotyczących problemów technicznych, w tym usuwania błędów działania systemu oraz zapewnia dostęp do najnowszej wersji Oprogramowania, aktualizacji polityk i filtrów w module ochrony poczty.

3. Wsparcie techniczne będzie świadczone na rzecz Zamawiającego na podstawie zgłoszenia Zamawiającego, dokonanego: w formie elektronicznej na adres e-mail: …… lub telefonicznej (całodobowo): ……
4. Czas reakcji na zgłoszenie usterki to 1 dzień, tj. najpóźniej do godz. 16.00 dnia następnego po dniu zgłoszenia. Konsultacje telefoniczne będą świadczone całodobowo przez wszystkie dni tygodnia.
5. Naprawy serwisowe wykonywane będą we wszystkie dni tygodnia w godzinach uprzednio ustalonych z Zamawiającym, przy czym:
    1. w przypadku awarii działania elementu usługi, usunięcie jej nastąpi w czasie nie dłuższym niż 62 godziny od daty potwierdzenia przyjęcia zgłoszenia,
    2. w przypadku ustania działania całego systemu, usunięcie awarii nastąpi w czasie nie dłuższym niż 24 godziny od daty potwierdzenia przyjęcia zgłoszenia,
6. Wykonawca dołoży wszelkich starań i uruchomi możliwe środki, aby maksymalnie skrócić czas oczekiwania na wsparcie techniczne oraz realizacji tak, by uzyskać wymierny efekt jakościowy.
7. Dla każdej nowej wersji Oprogramowania Wykonawca dostarczy Zamawiającemu „Instrukcję użytkownika” oraz
8. „Instrukcję instalacji”.
9. Wykonawca udziela Zamawiającemu gwarancji na świadczoną usługę na zasadach określonych umową licencyjną producenta Oprogramowania systemowego, która będzie dołączona do Umowy.
10. Wszelkie zmiany konfiguracyjne w Oprogramowaniu Wykonawca zobowiązany jest dokumentować, a dokumentację pełnej konfiguracji przekazywać Zamawiającemu w wersji elektronicznej.
11. Zamawiający dopuszcza możliwość udzielenia zgody na ustanowienie dla Wykonawcy zdalnego dostępu do serwera Zamawiającego, na potrzeby realizacji przedmiotu Umowy, na podstawie pisemnego wniosku złożonego przez Wykonawcę, sporządzonego wg wzoru określonego w **Załączniku nr 4 do** Umowy.
12. Szczegółowy zakres wsparcia technicznego oraz terminy i zasady realizacji określa OPZ.
13. Wsparcie techniczne będzie świadczone w języku polskim.

§ 6. Kary umowne

1. W razie wystąpienia zwłoki w wykonaniu Umowy, ponad termin określony w § 2 ust. 1, Wykonawca zobowiązuje się do zapłaty Zamawiającemu kary umownej w wysokości 0,5 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 pkt 1 powyżej, za każdy dzień zwłoki.
2. W razie wystąpienia zwłoki w wykonaniu obowiązków wynikających z gwarancji lub wsparcia technicznego określonych w § 6 ust. 4 i 5 ponad terminy ustalone w tych postanowieniach Umowy, Wykonawca zapłaci Zamawiającemu kary umowne w wysokości 0,5 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 pkt 1 powyżej, za każdy dzień zwłoki.
3. W przypadku odstąpienia od Umowy – przez Zamawiającego lub Wykonawcę - z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 pkt 1 powyżej.
4. Kary umowne mogą być dochodzone z każdego tytułu odrębnie i podlegają sumowaniu, przy czym łączna wysokość kar umownych nie może przekroczyć 20% łącznego wynagrodzenia umownego brutto, określonego w § 3 ust. 1 pkt 1 Umowy.
5. Ponadto, niezależnie od kar umownych, w przypadku niewykonania lub nienależytego wykonania przez Wykonawcę jakichkolwiek zobowiązań wynikających z Umowy Zamawiający uprawniony będzie do zlecenia zastępczego wykonania lub usunięcia wad na koszt i ryzyko Wykonawcy.
6. Jeżeli kary umowne nie pokryją poniesionej szkody, Zamawiający może dochodzić na zasadach ogólnych odszkodowania uzupełniającego przewyższającego kary umowne.
7. W razie wystąpienia opóźnienia w płatności za przedmiot umowy Zamawiający zapłaci Wykonawcy odsetki ustawowe za każdy dzień opóźnienia.
8. Wykonawca wyraża niniejszym nieodwołalną zgodę na potrącanie kar umownych z wszelkich przysługujących mu należności, choćby były jeszcze niewymagalne, w tym z przysługującego mu wynagrodzenia, o ile na dzień potrącenia bezwzględnie obowiązujące przepisy nie stanowią inaczej. Zamawiający zawiadomi pisemnie Wykonawcę o wysokości i podstawie naliczania kar umownych.

§ 7 Siła wyższa

1. Przez siłę wyższą rozumie się zdarzenie zewnętrzne, mające charakter nadzwyczajny i niezależny od woli Stron, którego skutkom nie można było zapobiec, pomimo podjęcia po temu starań, niezależnie czy zdarzenia te wystąpiły przed zawarciem czy w trakcie obowiązywania niniejszej Umowy.
2. W szczególności za siłę wyższą uznać należy: działania wojenne, niepokoje społeczne, trzęsienia ziemi, klęski żywiołowe, epidemie i pandemie, pożary, powodzie, akty władzy, akt terroru, przerwę w dostawie prądu i blokadę granic, akty władz publicznych – o ile mają wpływ na prawidłowe realizowanie postanowień Umowy i nie są wynikiem okoliczności zawinionej przez Stronę.

3. W razie wystąpienia siły wyższej, Strona powołująca się na siłę wyższą, jest zobowiązana powiadomić o tym fakcie drugą Stronę niezwłocznie, lecz nie później niż w terminie 7 dni od dnia w którym powzięła wiedzę możliwości wystąpienia siły wyższej. Jeżeli na dzień powiadomienia, o którym mowa w zdaniu pierwszym, siła wyższa uniemożliwia należyte wykonanie zobowiązań wynikających z umowy lub Strona powołująca się na siłę wyższą jest w stanie przewidzieć, wykonanie których zobowiązań będzie niemożliwie do spełnienia zgodnie z umową, winna to wykazać w tym powiadomieniu.
4. Terminu, o którym mowa ust. 3, nie stosuje się, jeśli w wyniku wystąpienia siły wyższej Strona zobowiązana do powiadomienia nie ma technicznych i faktycznych możliwości jej dokonania. W takim przypadku termin na powiadomienie biegnie od dnia przywrócenia możliwości dokonania notyfikacji.
5. W terminie 7 dni od ustania siły wyższej Strona dotknięta siłą wyższą powiadomi pisemnie drugą Stronę i wykaże w jakim stopniu jej wystąpienie uniemożliwiło należyte wykonanie zobowiązań wynikających z umowy.
6. Po otrzymaniu powiadomienia, o którym mowa w ust. 3 i 5, każda ze Stron umowy, może żądać przedstawienia dodatkowych oświadczeń lub dokumentów potwierdzających wpływ siły wyższej na należyte wykonanie zobowiązań wynikających z umowy.

§ 8. Zmiany w Umowie

1. Zamawiający przewiduje możliwość wprowadzenia zmian postanowień zawartej Umowy w stosunku do treści przedłożonej w niniejszym postępowaniu oferty, w następującym zakresie i przypadkach:
   1) zmiany przepisów prawa (jej zaistnienia lub wejścia w życie) lub wydania przez odpowiednie organy nowych wytycznych lub interpretacji dotyczących stosowania przepisów prawa, opublikowanych w Dzienniku Urzędowym Unii Europejskiej, Dzienniku Ustaw, Monitorze Polskim, Dzienniku Urzędowym odpowiedniego ministra lub innych oficjalnych publikatorach, w zakresie w jakim zmiana przepisów prawa lub wydane wytyczne lub interpretacje wymagają zmiany sposobu realizacji Umowy, w tym mogą wymagać zmiany zakresu świadczeń Wykonawcy określonych w Umowie;
   2) wystąpienia przyczyn niezależnych od Wykonawcy, związanych z równolegle prowadzonymi przez Zamawiającego projektami, zadaniami, postępowaniami mającymi wpływ na realizację Umowy lub w związku ze zmianami okoliczności wynikającymi ze specyfiki działalności Zamawiającego;
   3) zaistnienia co najmniej jednej z możliwości: a) usprawnienia wykonywania przedmiotu Umowy, b) zmniejszenia kosztów realizacji przedmiotu Umowy lub c) zwiększenia bezpieczeństwa wykonywania przedmiotu Umowy, która to zmiana Umowy może nastąpić w zakresie terminów lub kolejności wykonywania poszczególnych czynności w ramach Umowy, oraz wyłącznie jeżeli nie zakłóci prawidłowej realizacji Umowy;
   4) powstania możliwości zastosowania nowszych rozwiązań organizacyjnych, technologicznych lub technicznych, niż istniejących w chwili zawarcia Umowy, jeżeli te rozwiązania będą odpowiadały celom i wymaganiom Zamawiającego określonym w Umowie lub zapewnią prawidłowe wykonywanie Umowy, a okażą się korzystniejsze z punktu widzenia kosztów wykonywania Umowy, wydajności Sprzętu lub Oprogramowania lub usprawnienia zastosowanych rozwiązań;
   5) ujawnienia się powszechnie występujących wad Oprogramowania Zamawiający dopuszcza zmianę w zakresie przedmiotu Umowy polegającą na zastąpieniu Oprogramowania produktem zastępczym, spełniającym wszelkie wymagania przewidziane w Umowie dla Oprogramowania, to samo dotyczy dostarczanego Sprzętu, pod warunkiem że spełnia on minimalne wymagania określone przez Zamawiającego w postępowaniu o udzielenie zamówienia publicznego na podstawie którego zawarto Umowę;
   6) gdy niezbędna jest zmiana terminu realizacji Umowy lub poszczególnych przyjętych w Umowie terminów, w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które Strony nie miały wpływu, odpowiednio o czas trwania tych okoliczności lub zdarzeń
   7) gdy niezbędna jest zmiana terminu realizacji Umowy z uwagi na wstrzymanie lub zawieszenie realizacji Umowy przez Zamawiającego, wynikające z przyczyn leżących wyłącznie po stronie infrastruktury technicznej Zamawiającego;
   8) w zakresie sposobu realizacji Umowy lub terminu realizacji Umowy w przypadku uzasadnionych przyczyn technicznych lub funkcjonalnych powodujących konieczność zmiany sposobu wykonania Umowy lub terminu realizacji Umowy, np. wycofanie z produkcji lub zaprzestanie/wstrzymanie produkcji, wprowadzenie nowej technologii zgodnej z Umową;
   9) gdy wystąpi konieczność zmiany terminu odbioru przedmiotu Umowy lub terminów realizacji Umowy z uwagi na okoliczności leżące po stronie Zamawiającego tj. związanych z równolegle prowadzonymi przez Zamawiającego projektami lub zadaniami lub postępowaniami mającymi wpływ na realizację Umowy lub w związku ze zmianami okoliczności wynikającymi ze specyfiki działalności Zamawiającego;
   10) poprawy jakości lub innych parametrów charakterystycznych dla danego elementu objętego przedmiotem Umowy lub zmiany technologii na równoważną lub lepszą, podniesienia wydajności urządzeń oraz klasy bezpieczeństwa – w sytuacji wycofania z rynku przez producenta lub zakończenia produkcji zaoferowanego przez Wykonawcę przedmiotu Umowy, pojawienia się na rynku urządzeń nowszej generacji pozwalających na

zaoszczędzenie kosztów realizacji przedmiotu Umowy lub kosztów eksploatacji przedmiotu Umowy, pod warunkiem, że zmiany te nie spowodują zwiększenia ceny ofertowej;

11) zmiany terminu realizacji Umowy (lub jej części) lub zasad rozliczenia ze względu na przyczyny będące konsekwencją zaistnienia zdarzeń spowodowanych przez „siłę wyższą" (tj. zdarzenia nagłe powstałe niezależnie od Stron Umowy, które są poza kontrolą Stron Umowy, na których czas trwania Strony nie mają jakiegokolwiek wpływu, a których zaistnienie uniemożliwia wypełnienie któregokolwiek z zobowiązań wynikających z Umowy) lub innych zdarzeń lub obiektywnych przeszkód o zbliżonym charakterze (tj. niezależnych do woli Stron Umowy), których rozmiaru i intensywności nie można - pomimo zachowania należytej staranności - przewidzieć w dniu zawarcia Umowy, o ile ich wystąpienie będzie miało rzeczywisty wpływ na realizację Umowy);
12) zaistnienie zdarzeń siły wyższej lub nieznanych Stronom i niezależnych od ich woli lub starania okoliczności, których nie można było wcześniej przewidzieć;
13) wydłużenia okresu gwarancji Sprzętu;
14) w przypadku wniesienia odwołania na działania lub zaniechania Zamawiającego, o czas trwania postępowania odwoławczego, jeżeli wskutek tego postępowania nie będzie możliwa realizacja zamówienia w terminie wynikającym z Umowy;
15) zmiany wysokości naliczonej kary umownej, w sytuacji, gdy zobowiązanie Wykonawcy zostało w znacznej części wykonane a Zamawiający nie poniósł z tej przyczyny szkody.

2. Zamawiający dopuszcza dokonanie odpowiednich zmian wysokości wynagrodzenia w przypadku zmiany:
   1) stawki podatku od towarów i usług oraz podatku akcyzowego,
   2) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,
   3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenie lub ubezpieczenie zdrowotne,
   4) zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U z 2018 poz. 2215 oraz z 2019 r. poz. 1074 i 1572),

   - jeżeli zmiany te będą miały wpływ ma koszty wykonania zamówienia przez Wykonawcę
3. Zmiany, o których mowa w ust. 2 mogą nastąpić po 12 miesiącach od daty zawarcia Umowy.
4. Wykonawca może zwrócić się do Zamawiającego z pisemnym wnioskiem o przeprowadzenie negocjacji w sprawie odpowiedniej zmiany wynagrodzenia po dniu opublikowania przepisów obejmujących zmiany, o których mowa w ust. 2 i zgodnie z zasadami określonymi w tych zmienianych przepisach. Wniosek powinien zawierać propozycję zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumenty niezbędne do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 2 mają lub będą miały wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Wykonawcy określonych w Umowie, a w szczególności:
   1) przyjęte przez Wykonawcę zasady kalkulacji wysokości kosztów wykonania Umowy oraz założenia, co do wysokości dotychczasowych oraz przyszłych kosztów wykonania Umowy, wraz z dokumentami potwierdzającymi prawidłowość przyjętych założeń;
   2) wykazanie wpływu zmian, na wysokość kosztów wykonania Umowy przez Wykonawcę;
   3) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Wykonawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Wykonawcę.
5. W przypadku złożenia przez Wykonawcę powyższego wniosku, Strony będą prowadziły negocjacje z uwzględnieniem poniższych postanowień.
6. W terminie 1 miesiąca od otrzymania wniosku, o którym mowa w ust. 4, Zamawiający może zwrócić się do Wykonawcy o jego uzupełnienie, poprzez przekazanie dodatkowych wyjaśnień, informacji lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałami).
7. Zamawiający zajmie pisemne stanowisko wobec wniosku Wykonawcy, w terminie 1 miesiąca od dnia otrzymania kompletnego (po uzupełnieniach wniosku). Za dzień przekazania stanowiska uznaje się dzień jego wysłania na adres właściwy dla doręczeń pism dla Wykonawcy.
8. W przypadku uwzględnienia wniosku Wykonawcy przez Zamawiającego, Strony podejmą działania w celu uzgodnienia treści aneksu do Umowy oraz jego podpisania.
9. Poza zmianami opisanymi w ust.1, zmiana Umowy może nastąpić w przypadkach określonych w art. 455 ust. 1 i 2 ustawy Pzp, zgodnie z warunkami określonymi w postanowieniach przepisów art. 454-455 ustawy Pzp.
10. Każda zmiana Umowy może nastąpić jedynie za zgodą obu Stron wyrażoną na piśmie w formie aneksu pod rygorem nieważności, z zastrzeżeniem postanowień § 5 ust. 5 oraz ust. 1 pkt 15 powyżej (w zakresie którego zmiana przebiega w drodze porozumienia).

§ 9. Odstąpienie od umowy i jej rozwiązanie

1. Zamawiający, jest uprawniony do odstąpienia od Umowy (w całości lub części), ze skutkiem na dzień złożenia Wykonawcy oświadczenia (ex nunc), w razie:
   1) wystąpienia zwłoki Wykonawcy w realizacji Umowy o 7 dni ponad termin określony w § 2 ust. 1 Umowy;
   2) w innych przypadkach niewykonywania lub nienależytego wykonywania obowiązków wynikających z Umowy, po uprzednim wezwaniu Wykonawcy do realizacji obowiązków zgodnie z Umową;
   3) zostanie wydany nakaz zajęcia majątku lub otwarta likwidacja Wykonawcy, w zakresie uniemożliwiającym wykonywanie Umowy;
   4) Wykonawca – choćby tylko faktycznie – zaprzestanie prowadzenia działalności;
   5) w przypadkach i na warunkach określonych w art. 456 ustawy Pzp.
2. Odstąpienie od Umowy na zasadach opisanych w niniejszym paragrafie może nastąpić w okresie obowiązywania Umowy, przedłużonym o 30 dni.
3. W przypadku odstąpienia od Umowy postanowienia dotyczące kar umownych, możliwości dochodzenia odszkodowania przenoszącego wysokość zastrzeżonych kar umownych, poufności, ochrony danych osobowych i właściwości sądu pozostają w mocy.

§ 10. Prawa własności intelektualnej

1. Wykonawca zapewnia, że przysługuje mu nieograniczone prawo do udzielenia bezterminoweji niewyłącznej licencji na dedykowane Oprogramowanie dla Sprzętu, o którym mowa w § 1 Umowy, uprawniającej do korzystania z Oprogramowania w zakresie pól eksploatacji pozwalających Zamawiającemu na korzystanie z Oprogramowania w najszerszym możliwym zakresie funkcjonalności i z możliwości technicznych Sprzętu i z dniem bezusterkowego odbioru Sprzętu w ramach wynagrodzenia, którym mowa w § 3 ust. 1 Umowy udziela Zamawiającemu niezbędnej licencji lub zobowiązuje się do potwierdzenia licencji Oprogramowania, potwierdzających prawo Zamawiającego do używania Oprogramowania (za pomocą dokumentów licencyjnych, sporządzonych według standardu przyjętego przez producenta dostarczonego Sprzętu lub w inny sposób, zgodnie z wymaganiami producenta) uprawniającej Zamawiającego w szczególności do korzystania z Oprogramowania na następujących polach eksploatacji:
   1) wprowadzanie i zapisywanie w pamięci komputerów,
   2) odtwarzanie,
   3) przechowywanie,
   4) sporządzanie kopii zapasowej (kopii bezpieczeństwa) nośników instalacyjnych i nośników z zainstalowanym Oprogramowaniem,
   5) wyświetlanie,
   6) przystosowywanie,
   7) instalowanie i deinstalowanie Oprogramowania pod warunkiem zachowania liczby udzielonych licencji,
   8) korzystanie z oprogramowania na wszystkich polach funkcjonalności,
   9) korzystanie i modyfikowanie dokumentów oraz danych wytworzonych przy pomocy Oprogramowania.
2. Licencje/sublicencje na korzystanie z Oprogramowania mogą zostać wypowiedziane nie wcześniej niż po upływie 20 lat od ich udzielenia, przy czym okres wypowiedzenia nie może być krótszy niż 5 lat.
3. Wykonawca oświadcza, że dostarczone przez niego Oprogramowanie, nie narusza jakichkolwiek praw osób trzecich, zwłaszcza w zakresie przepisów o wynalazczości, znakach towarowych, prawach autorskich i prawach pokrewnych oraz nieuczciwej konkurencji, i że posiada prawo do udzielania licencji/sublicencji lub odsprzedaży Oprogramowania, które Wykonawca dostarczył w ramach Umowy, zgodnie z postanowieniami ust. 1 i przejmuje w tym zakresie odpowiedzialność w przypadku roszczeń osób trzecich.
4. Wykonawca uprawnia Zamawiającego do swobodnego dokonywania zmian w zakresie przydzielania poszczególnych licencji/sublicencji pracownikom Zamawiającego.
5. Wykonawca oświadcza, że aktualizacja Oprogramowania, nie powoduje zmian pól eksploatacji określonych w ust. 1 niniejszego paragrafu.

§ 11. Poufność

1. Umowa jest jawna i może podlegać udostępnieniu na zasadach określonych w przepisach o dostępie do informacji publicznej (art. 18 ustawy Pzp). Z zastrzeżeniem tego wymogu Strony zobowiązują się do przestrzegania przy realizacji przedmiotu Umowy wszystkich postanowień zawartych w obowiązujących przepisach związanych z ochroną danych osobowych, a także ochroną informacji poufnych oraz ochroną tajemnicy przedsiębiorstwa.
2. Wykonawca zobowiązuje się do zachowania w poufności wszelkich niepodlegających upublicznieniu informacji dotyczących Zamawiającego oraz jego pracowników, współpracowników i podmiotów z Zamawiającym współpracujących, jakie Wykonawca uzyska w toku wykonywania przedmiotu Umowy.
3. Wykonawca zobowiązuje się do nieujawniania i do nieudostępniania osobom trzecim żadnej niepodlegającej upublicznieniu informacji, którą nabył bezpośrednio lub pośrednio w trakcie trwania lub w wyniku wykonania

Umowy. Niniejsze postanowienie obejmuje również dane osobowe administrowane przez pracowników Zamawiającego, kody źródłowe Oprogramowania i baz danych, dane z baz danych i aplikacji, wszelkie dane dostępowe IT, wszelkie poufne dokumenty i informacje finansowe, marketingowe, handlowe, techniczne, konsultingowe i inne, w tym informacje i dokumenty, które Wykonawca sporządził, przetworzył lub otrzymał w związku z realizacją Umowy. W razie jakichkolwiek wątpliwości, co do charakteru danej informacji, przed jej ujawnieniem lub uczynieniem dostępną, Strona zwróci się do drugiej Strony o wskazanie, czy informację tę ma traktować jako poufną.

4. Informacji poufnej nie stanowi informacja powszechnie znana w chwili ujawnienia, legalnie otrzymana od strony trzeciej bez zastrzeżenia poufności oraz ujawniona przez Stronę za uprzednią pisemną zgodą drugiej Strony, co do której obowiązek przekazania wynika z przepisów prawa, orzeczenia lub wezwania właściwych władz.
5. Wykonawcy nie wolno, bez uprzedniej pisemnej zgody Zamawiającego, wykorzystywać jakichkolwiek dokumentów, do których ma dostęp w wyniku wykonywania Umowy, w innych celach niż do jej wykonywania.
6. Obowiązek określony w ust. 2 i 3 nie dotyczy:
   1) publicznie dostępnych,
   2) informacji, które były znane Stronie przed otrzymaniem od drugiej Strony i nie były objęte zobowiązaniem do poufności względem jakiegokolwiek podmiotu,
   3) obowiązku ujawnienia wynikającego z odpowiednich ustaw i rozporządzeń.
7. Zobowiązanie do zachowania poufności nie stoi na przeszkodzie ujawnieniu informacji na uprawnione żądanie sądu lub organu administracji oraz w postępowaniu sądowym lub administracyjnym, jeżeli jest to potrzebne dla jego rozstrzygnięcia i przy zachowaniu możliwych środków ochrony ujawnianych informacji przed ich publicznym rozpowszechnieniem.
8. Wykonawca odpowiada za podjęcie i zapewnienie wszelkich niezbędnych środków zapewniających dochowanie zasady poufności, określonej w ust. 2 i 3, przez swoich pracowników i podwykonawców.
9. Wykonawca zobowiązuje się do przestrzegania przepisów dot. ochrony danych osobowych, jeśli dane takie pozyska w trakcie lub w związku z wykonaniem przedmiotu Umowy.
10. Osoby będące w dyspozycji Wykonawcy, uzyskujące wgląd w dane osobowe administrowane przez Zamawiającego, zobowiązane są posiadać przeszkolenie z zakresu ochrony danych osobowych, zostać upoważnione przez Zamawiającego do przetwarzania danych osobowych oraz podpisać indywidualne zobowiązanie do zachowania w tajemnicy danych osobowych.
11. Wykonawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy wszelkich wewnętrznych uregulowań Zamawiającego.
12. W chwili, gdy dane, w których posiadanie wszedł Wykonawca nie będą już konieczne do świadczenia przez niego usług na rzecz Zamawiającego, a także na każde żądanie Zamawiającego, Wykonawca zwróci Zamawiającemu wszelkie nośniki zawierające dane lub zniszczy dane, przy zachowaniu obowiązujących w tym zakresie przepisów. W żadnym przypadku nośniki, na których znajdowały się dane nie mogą zostać udostępnione osobom trzecim bez uprzedniego usunięcia danych z takich nośników w sposób zatwierdzony przez Zamawiającego na piśmie.
13. Wykonawca, po wykonaniu Umowy w zakresie świadczenia usługi asysty, zobowiązuje się do zwrotu wszelkich dokumentów, które otrzymał od Zamawiającego w trakcie realizacji Umowy oraz do potwierdzonego pisemnie usunięcia z nośników oraz Oprogramowania Wykonawcy (m.in. serwerów, urządzeń teleinformatycznych, programów, baz danych, skrzynek e-mail) wszelkich cyfrowych danych, dokumentów, kodów, dostępów oraz jakichkolwiek innych danych jakie pozyskał lub przetworzył cyfrowo podczas wykonywania Umowy. Analogiczne obowiązki ma Wykonawca względem wyżej wymienionych dokumentów i zawartości nośników po wykonaniu gwarancji czy wykonaniu prac wynikających z rękojmi, jeżeli w okresie świadczenia tych prac, wejdzie w posiadanie dokumentów lub jakichkolwiek cyfrowych danych, dokumentów, kodów, dostępów oraz jakichkolwiek innych danych jakie pozyskał lub przetworzył cyfrowo.

§ 12. Ochrona danych osobowych

1. Zamawiający udostępnia Wykonawcy dane osobowe w celu i zakresie niezbędnym do wykonania Umowy na
2. podstawie art. 6 ust. 1 lit. b i f RODO
3. Wykonawca zobowiązuje się do przetwarzania udostępnionych przez Zamawiającego danych osobowych zgodnie z przepisami prawa powszechnie obowiązującego o ochronie danych osobowych, w szczególności z przepisami Rozporządzenia Parlamentu Europejskiego i Rady z dnia 26 kwietnia 2016 r w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwane dalej „RODO”.
4. Wykonawca oświadcza, że stosuje powszechnie obowiązujące przepisy prawa o ochronie danych osobowych.
5. Zakres udostępnianych danych osobowych obejmuje dane pracowników w zakresie: imienia, nazwiska, adresu mailowego, numeru telefonu.
6. Udostępnione przez Zamawiającego dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu realizacji Umowy w zakresie o którym mowa w §1.

7. Wykonawca zobowiązuje się, przy przetwarzaniu udostępnionych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, w szczególności zgodnie z art. 32 RODO. Wykonawca poinformuje na piśmie Zamawiającego o zastosowanych środkach technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych zgodnie z art. 32 RODO.
8. Wykonawca zobowiązuje się dołożyć należytej staranności przy przetwarzaniu udostępnionych danych osobowych.
9. Wykonawca zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
   1) otrzymają pisemne upoważnienia do przetwarzania danych osobowych;
   2) będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
   3) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora;
   4) zobowiążą się do bezterminowego zachowania w tajemnicy danych osobowych oraz stosowanych przez Wykonawcę sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z odpowiednich przepisów.
10. Wykonawca zobowiązuje się do zachowania w tajemnicy udostępnionych danych osobowych także po ustaniu Umowy.
11. Wykonawca, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Zamawiającym w wywiązaniu się z obowiązków określonych w art. 32–36 RODO.
12. W przypadku stwierdzenia naruszenia ochrony danych osobowych, w szczególności o którym mowa w art. 4 pkt 12 RODO, Wykonawca zobowiązuje się do bezzwłocznego poinformowania Zamawiającego, w formie pisemnej oraz dodatkowo na adres mailowy iod@pgi.gov.pl , o tym fakcie w okresie do 24 godzin, wskazując okoliczności i zakres naruszenia.
13. Jeżeli Wykonawca realizując Umowę zleci podwykonawcom prace, w trakcie których będą przetwarzane dane osobowe, odpowiednio powierzy im, za zgodą Zamawiającego, w drodze umowy zawartej na piśmie, przetwarzanie tych danych na warunkach zgodnych z postanowieniami Umowy. W przypadku zlecenia prac podwykonawcom, Wykonawca odpowiada za szkody, jakie powstaną wobec Zamawiającego lub osób trzecich na skutek przetwarzania przez podwykonawców danych osobowych niezgodnie z Umową lub przepisami prawa powszechnie obowiązującego.
14. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym
15. Wykonawca zapewni w okresie obowiązywania Umowy pełną ochronę danych osobowych oraz zgodność ze wszelkimi obecnymi oraz przyszłymi przepisami prawa dotyczącymi ochrony danych osobowych i prywatności.
16. Wykonawcy nie przysługuje wynagrodzenie za wykonywanie obowiązków wynikających z niniejszego paragrafu.
17. W sprawach nieuregulowanych w niniejszym paragrafie zastosowanie mają przepisy RODO.
18. Wykonawca oświadcza, że akceptuje postanowienia umowne w zakresie ochrony danych osobowych.

§ 13. INNE POSTANOWIENIA

1. Wykonawca oświadcza, że nie zachodzi wobec niego podstawa wykluczenia przewidziana w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2022 r. poz. 835) oraz art. 5k Rozporządzenia (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie.
2. W trakcie realizacji Umowy Zamawiający uprawniony jest do wykonywania czynności kontrolnych wobec Wykonawcy odnośnie spełnienia przez Wykonawcę warunku, o którym mowa w ust. 1, w szczególności do:
   1) żądania oświadczeń i dokumentów w zakresie spełniania przez Wykonawcę ww. wymogu i dokonywania ich oceny;
   2) żądania wyjaśnień w przypadku wątpliwości w zakresie potwierdzenia przez Wykonawcę spełnienia wskazanego powyżej wymogu.
3. Niezłożenie przez Wykonawcę w wyznaczonym przez Zamawiającego terminie żądanych przez Zamawiającego dokumentów lub wyjaśnień w celu potwierdzenia spełnienia przez Wykonawcę wymogu, o którym mowa w ust. 1, traktowane będzie jako niewłaściwe wykonywanie Umowy.
4. Przedmiotowe zamówienie finansowane jest przez Ministra Infrastruktury (Dotujący).
   5. Wykonawca oświadcza, że zobowiązuje się do poddania kontroli prowadzonej przez Dotującego, przekazania dokumentacji Dotującemu, złożenia wyjaśnień Dotującemu oraz umożliwienia wejścia upoważnionych pracowników Dotującego na teren realizowania zamówienia/zadnia objętego finansowaniem.

§ 14. Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą Umową stosuje się przepisy prawa obowiązujące w Polsce.
2. Ewentualne spory wynikłe z realizacji Umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.
3. Wszelkie zmiany i uzupełnienia Umowy, o ile w jej treści nie postanowiono inaczej, wymagają formy pisemnej pod rygorem nieważności.
4. Umowa wchodzi w życie w dniu jej podpisania przez Strony, w przypadku jeżeli podpisy Stron nie są złożone jednocześnie Umowa wchodzi w życie z momentem złożenia ostatniego podpisu - jeśli dotyczy.
5. Umowa została zawarta w 3 egzemplarzach, 2 egzemplarze dla Zamawiającego i 1 egzemplarz dla Wykonawcy / umowa zawarta w postaci elektronicznej i opatrzona przez każdą ze Stron kwalifikowanym podpisem elektronicznym.

6. Do Umowy dołączono następujące załączniki, które stanowią jej integralną cześć:

=

Załącznik nr 1 – Opis przedmiotu zamówienia,
Załącznik nr 2 – Oferta Wykonawcy z dnia ……,
Załącznik nr 3 – Protokół Odbioru
Załącznik nr 4 – Wniosek na ustanowienie dla Wykonawcy zdalnego dostępu do serwera Zamawiającego
Załącznik nr56 - Wydruk KRS/CEDIG z dnia ……. 2022 r.

Załącznik nr 3 do SWZ

Dane Wykonawcy / Wykonawców występujących wspólnie	
Adres Wykonawcy: kod, miejscowość, ulica, nr lokalu	
Województwo:	
Osoba do kontaktu: Nr telefonu:	
E-mail:	
REGON:	
NIP:	

Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy
ul. Rakowiecka 4
00-975 Warszawa

OFERTA

Nawiązując do ogłoszenia o zamówieniu, oznaczenie sprawy EZP.26.178.2022 pn.:

Usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB

My niżej podpisani działając w imieniu i na rzecz:

……..

(nazwa (firma) dokładny adres Wykonawcy/Wykonawców) (w przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia należy podać nazwy(firmy) i adresy wszystkich tych Wykonawców)

1. Oferujemy wykonanie przedmiotowego zamówienia, określonego w specyfikacji warunków zamówienia za cenę:

Lp.	Przedmiot zamówienia	Wartość netto	Kwota podatku VAT	Wartość brutto
1	**Usługa licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB – Zamówienie podstawowe**			
2	**Usługa licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB – Zamówienie opcjonalne**			
	Razem:		**xxxxx**	

2. Oświadczamy, że:

1) Jesteśmy*:

mikroprzedsiębiorstwem	
małym przedsiębiorstwem	
średnim przedsiębiorstwem[1]	
jednoosobową działalnością gospodarczą	
osobą fizyczną nieprowadzącą działalnością gospodarczą	
inny rodzaj	

**należy zaznaczyć rodzaj Wykonawcy*

2) Zamówienie zrealizujemy:

☐ bez udziału podwykonawców;

☐ z udziałem niżej wskazanych podwykonawców

Lp.	Firma podwykonawcy	Część zamówienia, której wykonanie Wykonawca zamierza powierzyć podwykonawcy
1.		
…		

3) zapoznaliśmy się z treścią SWZ, a w szczególności z opisem przedmiotu zamówienia i z projektowanymi postanowieniami umowy oraz ze zmianami i wyjaśnieniami treści SWZ oraz, że wykonamy zamówienie na warunkach i zasadach określonych tam przez Zamawiającego;

4) wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r.) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu;

5) otrzymaliśmy konieczne informacje do przygotowania oferty. Uważamy się za związanych niniejszą ofertą przez czas wskazany w SWZ, w przypadku uznania naszej oferty za najkorzystniejszą zobowiązujemy się do podpisania umowy na warunkach zawartych w SWZ w miejscu i terminie wskazanym przez Zamawiającego;

6) następujące informacje i dokumenty zawarte w ofercie w stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ujawniane pozostałym uczestnikom postępowania:

- …….

- …….

należy wpisać nazwy plików stanowiących tajemnicę przedsiębiorstwa – jeżeli dotyczy*.

7) świadom (-i) odpowiedzialności karnej oświadczam (-y), że załączone do oferty dokumenty opisują stan prawny i faktyczny aktualny na dzień złożenia niniejszej oferty (art. 297 k.k.);

8) załącznikami do niniejszej oferty, stanowiącymi jej integralną cześć są:

1) ……

2) ……

Niniejszy plik należy opatrzyć kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną

[1] Definicja MŚP zawarta jest w załączniku I do Rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. Wyodrębnia się następujące kategorie przedsiębiorstw: 1. Średnie przedsiębiorstwo: a) zatrudnia mniej niż 250 pracowników oraz b) jego roczny obrót nie przekracza 50 mln euro lub roczna suma bilansowa nie przekracza 43 mln euro; 2. Małe przedsiębiorstwo: a) zatrudnia mniej niż 50 pracowników oraz b) jego roczny obrót nie przekracza 10 mln euro lub roczna suma bilansowa nie przekracza 10 mln euro; 3. Mikroprzedsiębiorstwo: a) zatrudnia mniej niż 10 pracowników oraz b) jego roczny obrót nie przekracza 2 mln euro lub roczna suma bilansowa nie przekracza 2 mln euro.

Załącznik nr 4 do SWZ

OŚWIADCZENIE O NIEPODLEGANIU WYKLUCZENIU
ORAZ SPEŁNIENIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

My, niżej podpisani, działając w imieniu i na rzecz:

……

……
(nazwa /firma/ i adres Wykonawcy/ Wykonawców wspólnie ubiegających się o udzielenie zamówienia)

niniejszym oświadczamy, że ubiegając się o zamówienie publiczne pn. **Usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB** (oznaczenie sprawy: EZP.26.178.2022)

1) spełniamy* / nie spełniamy* warunków o których mowa w pkt 7 SWZ;
2) nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4 ustawy Pzp a także w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835) są aktualne na dzień złożenia oświadczenia;
3) zachodzą w stosunku do nas podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp) lub w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835). Jednocześnie oświadczamy, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjęliśmy następujące środki naprawcze: ……
4) informujemy o dostępności wymaganych w SWZ podmiotowych środkach dowodowych:

Nazwa oświadczenia lub dokumentu	Adres internetowy na której dokument lub oświadczenie dostępne jest w formie elektronicznej, wydający urząd lub organ/numer lub nazwa postępowania o udzielenie zamówienia publicznego

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższym oświadczeniu są aktualne i zgodne z prawem oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia oświadczenie składa każdy z Wykonawców oddzielnie.

** niepotrzebne skreślić*

Niniejszy plik należy opatrzyć kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną

Załącznik nr 5 do SWZ

ZOBOWIĄZANIE

innych podmiotów do oddania do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia

My niżej podpisani

……
(imię i nazwisko składającego zobowiązanie)

posiadając upoważnienie do reprezentowania:

……
(*nazwa i adres podmiotu oddającego do dyspozycji zasoby)*

zobowiązujemy się, iż w przypadku gdy Wykonawcy:

……
(nazwa i adres Wykonawcy składającego ofertę)

zostanie udzielone zamówienie publiczne pn. **Usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB** (oznaczenie sprawy: EZP.26.178.2022), do oddania temu Wykonawcy do dyspozycji niezbędnych zasobów, zgodnie z art. 118 ustawy Pzp, polegającego na wykorzystaniu

……

W celu udowodnienia, że Wykonawca, tj.:
……
(nazwa i adres Wykonawcy składającego ofertę)

będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący podmiot, który reprezentuję(emy) z Wykonawcą gwarantuje rzeczywisty dostęp do ich zasobów – oświadczamy, co następuje:

1. odnośnie zakresu dostępnych Wykonawcy zasobów podmiotu który reprezentujemy:

   ……

2. odnośnie sposobu i okresu udostępnienia Wykonawcy i wykorzystania przez niego zasobów, które udostępniamy przy wykonywaniu zamówienia publicznego:

   - sposób - ……

   - okres - ……

3. odnośnie informacji, czy i w jakim zakresie podmiot, który reprezentujemy, tj. podmiot na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących doświadczenia zrealizuje usługi, których wskazane zdolności dotyczą:

   ……

Niniejszy plik należy opatrzyć kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną

Załącznik nr 6 do SWZ

Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia

Jako Wykonawcy wspólnie ubiegający się o udzielenie zamówienia w postępowaniu pn. **Usługa wsparcia i subskrypcji dla licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB** (oznaczenie sprawy: EZP.26.178.2022), oświadczamy, że warunek udziału w postępowaniu, o którym mowa w punkcie 7.3. SWZ dotyczący zdolności technicznej lub zawodowej spełnia:

……

(wskazanie firmy i adresu Wykonawcy spełniającego warunek)

Oświadczamy, że wskazany powyżej Wykonawca wykona zakres zamówienia polegający na:
……..
……
……..

1) Wykonawca …… (wskazanie firmy i adresu Wykonawcy) zrealizuje zamówienie w zakresie: ……
   ……
   ……
2) Wykonawca …… (wskazanie firmy i adresu Wykonawcy) zrealizuje zamówienie w zakresie: ……
   ……
   ……

Niniejszy plik należy opatrzyć kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną

Załącznik nr 7 do SWZ

OŚWIADCZENIE

PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY

O NIEPODLEGANIU WYKLUCZENIU ORAZ SPEŁNIENIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

My niżej podpisani, działając w imieniu i na rzecz:

.....

.....

(nazwa /firma/ i adres Wykonawcy podmiot udostępniający zasoby)

Oświadczamy, że w postępowaniu pn.: „**Usługa licencji do systemów filtrowania i bezpieczeństwa ruchu WWW, ochrony poczty elektronicznej, ochrony danych DLP, oraz ochrony DLP dla aplikacji chmurowych wraz ze wsparciem technicznym dla PIG-PIB** (oznaczenie sprawy: EZP.26.178.2022):

1. spełniamy następujące warunki udziału w postępowaniu określone przez Zamawiającego w zakresie:

   1) ……

   2) ……

   3) ……

2. nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4 ustawy Pzp,

3. nie podlegamy wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835)

4. zachodzą w stosunku do nas podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp)*. Jednocześnie oświadczamy, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjęliśmy następujące środki naprawcze:

……

5. informujemy o dostępności wymaganych w SWZ podmiotowych środkach dowodowych:

Nazwa oświadczenia lub dokumentu	Adres internetowy na której dokument lub oświadczenie dostępne jest w formie elektronicznej, wydający urząd lub organ/numer lub nazwa postępowania o udzielenie zamówienia publicznego

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższym oświadczeniu są aktualne i zgodne z prawem oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia oświadczenie składa każdy z Wykonawców oddzielnie.

** niepotrzebne skreślić*

Niniejszy plik należy opatrzyć kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną