SPECYFIKACJA

ISTOTNYCH WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie

PRZETARGU NIEOGRANICZONEGO

na podstawie art. 39 ustawy z 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 ze zm.), o wartości szacunkowej zamówienia poniżej 214 000 EURO.

Sygn. postępowania: EZP-240-89/2020

PRZEDMIOT ZAMÓWIENIA:

Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG - PIB

Pełnomocnik Dyrektora PIG-PIB
ds. Zamówień Publicznych

Mariola Siwek
Elektronicznie podpisany przez Mariola Siwek
Data: 2020.12.04 11:02:09 +01'00'

Użyte w niniejszym dokumencie skróty i sformułowania oznaczają:

1. „ustawa Pzp" – ustawę z 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 ze zm.);
2. „SIWZ" – niniejszą Specyfikację Istotnych Warunków Zamówienia;
3. „Zamawiający" lub „PIG-PIB" – Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy;
4. „Wykonawca" – zgodnie z definicją zawartą w art. 2 pkt 11) ustawy Pzp.

1. ZAMAWIAJĄCY

Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy

ul. Rakowiecka 4

00-975 Warszawa

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.

2. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie o udzielenie niniejszego zamówienia prowadzone jest w trybie przetargu nieograniczonego o szacunkowej wartości zamówienia poniżej 214 000 euro, zgodnie z przepisami ustawy Pzp.

3. OPIS PRZEDMIOTU ZAMÓWIENIA

3.1. Przedmiotem zamówienia jest **dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG - PIB**.

3.2. Szczegółowy zakres przedmiotu zamówienia został określony w:
- Załączniku nr 1 do SIWZ – „Opis przedmiotu zamówienia";
- Załączniku nr 2 do SIWZ – „Istotne postanowienia umowy".

3.3. Oznaczenie przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):
35120000-1 – Systemy i urządzenia nadzoru i bezpieczeństwa;
72611000-6 – Usługa wsparcia technicznego.

4. TERMIN WYKONANIA ZAMÓWIENIA

Termin realizacji zamówienia do dnia 31.12.2020 r. wraz ze świadczeniem wsparcia do dnia 31.12.2021 r.

5. INNE POSTANOWIENIA

5.1. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

5.2. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

5.3. Zamawiający nie zastrzega osobistego wykonania kluczowych części zamówienia przez Wykonawcę.

5.4. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej.

5.5. Zamawiający nie przewiduje ustanowienia dynamicznego systemu zamówień ani zawarcia umowy ramowej.

5.6. Zamawiający informuje, iż zgodnie z art. 24 aa ustawy Pzp, w pierwszej kolejności dokona oceny ofert a następnie zbada czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza według kryteriów oceny ofert określonych w SIWZ, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

5.7. Zamawiający nie przewiduje możliwości udzielenia zamówienia, o którym mowa w art. 67 ust. 1 pkt 7 ustawy Pzp.

6. WARUNKI UDZIAŁU W POSTĘPOWANIU

6.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają określone przez Zamawiającego warunki udziału w postępowaniu dotyczące:
  6.1.1. kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej,
  6.1.2. sytuacji ekonomicznej lub finansowej,
  6.1.3. zdolności technicznej lub zawodowej.

6.2. W zakresie „zdolności technicznej lub zawodowej" Wykonawca zobowiązany jest wykazać, że:
  6.2.1. w okresie ostatnich trzech 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.
  6.2.2. będzie dysponować zespołem osób, które zostaną skierowane do realizacji zamówienia, tj. co najmniej:
    6.2.2.1. jedną (1) osobą posiadającą ważny certyfikat administratora DLP,
    6.2.2.2. dwóch (2) osób posiadających ważny certyfikat administratora e-mail security,
    6.2.2.3. jedną (1) osobą posiadającą ważny certyfikat administratora web security.

  Każda z osób wskazanych w pkt. 6.2.2.1.-6.2.2.3. SIWZ może pełnić w zespole nie więcej niż dwie różne funkcje.

6.3. **Spełnianie warunków poprzez poleganie na potencjale „innych podmiotów".**
  6.3.1. Wykonawcy, w celu potwierdzenia spełniania warunków udziału w postępowaniu, mogą polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
  6.3.2. Jeżeli zdolności techniczne lub zawodowe podmiotu, na potencjale którego Wykonawca polega, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu, lub zachodzą wobec tych podmiotów podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13-22 i ust. 5 pkt 1 ustawy Pzp, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego:
    1) zastąpił ten podmiot innym podmiotem lub podmiotami lub
    2) zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe.

6.4. **Spełnianie warunków udziału przez konsorcjum.**
  W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum), warunki określone w pkt 6.2 SIWZ mogą zostać spełnione przez jednego Wykonawcę lub łącznie wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

6.5. **Zamawiający oceni spełnianie warunków udziału w postępowaniu na podstawie informacji zawartych w oświadczeniach i dokumentach.**

6.6. **Ocena spełniania warunków wymaganych od Wykonawców nastąpi wg formuły: „spełnia – nie spełnia".**

7. PODSTAWY WYKLUCZENIA

7.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 ustawy Pzp,

7.2. oraz którzy nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp, przy czym Zamawiający może wykluczyć Wykonawców w stosunku do których otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację ich majątku lub sąd zarządził likwidację ich majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (t.j. Dz. U. z 2020 r., poz. 814) lub których upadłość ogłoszono, z wyjątkiem Wykonawców, którzy po ogłoszeniu upadłości zawarli układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację ich majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (t.j. Dz. U. z 2020 r., poz. 1228 ze zm.).

7.3. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

7.4. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20 lub ust. 5 pkt 1 ustawy Pzp, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu Wykonawcy.
Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające dowody przedstawione na ww. podstawie.

7.5. W przypadkach, o których mowa w art. 24 ust. 1 pkt 19 ustawy Pzp, przed wykluczeniem Wykonawcy, Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji.

7.6. W celu potwierdzenia spełniania warunków udziału w postępowaniu przez Wykonawców składających wspólną ofertę przesłanka nie podlegania wykluczeniu z postępowania, określona w pkt. 7.1 i 7.2 SIWZ oceniana będzie odrębnie dla każdego z Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

8. WYKAZ OŚWIADCZEŃ W CELU WSTĘPNEGO POTWIERDZENIA, ŻE WYKONAWCA NIE PODLEGA WYKLUCZENIU ORAZ SPEŁNIA WARUNKI UDZIAŁU W POSTĘPOWANIU

8.1. Oświadczenie składane wraz z ofertą i jego zakres:
Wykonawca zobowiązany jest dołączyć do oferty aktualne na dzień składania ofert oświadczenie zawierające w szczególności informacje:

8.1.1. o tym, że Wykonawca spełnia warunki udziału w postępowaniu określone przez Zamawiającego w pkt 6 SIWZ,

8.1.2. o tym, że Wykonawca nie podlega wykluczeniu z powodów wskazanych w art. 24 ust. 1 pkt 13-22 i ust. 5 pkt 1 ustawy Pzp,

8.1.3. o innych podmiotach, na zasoby których Wykonawca powołuje się w celu wykazania spełnienia warunków udziału w postępowaniu, wraz z informacją dotyczącą podstaw wykluczenia innego podmiotu, o których mowa w art. 24 ust. 1 pkt 13–22 i ust. 5 pkt 1 ustawy Pzp – jeżeli dotyczy.

8.1.3.1. Wykonawca, który polega na zdolnościach innych podmiotów, zobowiązany jest udowodnić Zamawiającemu, że realizując zamówienie, będzie miał rzeczywisty dostęp do zasobów tych podmiotów w zakresie niezbędnym do należytego wykonania zamówienia, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. Z treści załączonych dokumentów powinien wynikać:

8.1.3.1.1. zakres dostępnych Wykonawcy zasobów innego podmiotu,

8.1.3.1.2. sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia,

8.1.3.1.3. zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia.

Szczegółowy zakres wymaganych informacji, które powinno zawierać ww. oświadczenie wskazany jest we wzorze zawartym w **Załączniku nr 4 do SIWZ**.

8.2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców (konsorcjum), oświadczenie składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te potwierdzają brak podstaw wykluczenia i spełnianie warunków udziału w postępowaniu w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

9. OŚWIADCZENIE O GRUPIE KAPITAŁOWEJ

Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji o Wykonawcach, którzy złożyli oferty w postępowaniu, zobowiązany jest przekazać Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej co inni Wykonawcy, którzy złożyli oferty w postępowaniu. W stosownej sytuacji, wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą, który złożył ofertę w tym samym postępowaniu, nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

UWAGA: W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dokument składa każdy z Wykonawców występujących wspólnie.

Zamawiający w dniu zamieszczenia informacji z otwarcia ofert udostępni wzór Informacji w odniesieniu do przynależności lub braku przynależności do grupy kapitałowej, w sytuacji gdy w postępowaniu zostały złożone co najmniej 2 oferty.

10. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW W CELU POTWIERDZENIA, ŻE WYKONAWCA NIE PODLEGA WYKLUCZENIU, SPEŁNIA WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ, ŻE OFEROWANE DOSTAWY SPEŁNIAJĄ WYMAGANIA OKREŚLONE PRZEZ ZAMAWIAJĄCEGO

10.1. Zamawiający w pierwszej kolejności dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. W przypadku gdy Zamawiający stwierdzi, że przeprowadzenie ww. procedury jest nieuzasadnione lub niecelowe może odstąpić od jej zastosowania.

Dla zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.

10.2. Zamawiający **wezwie Wykonawcę, którego oferta została oceniona jako najkorzystniejsza**, do złożenia w wyznaczonym, nie krótszym niż 5 dni terminie aktualnych na dzień złożenia następujących oświadczeń i dokumentów wymienionych w pkt 10.3 i 10.4 SIWZ (w razie konieczności także w pkt 10.7 i 10.9 SIWZ).

10.3. W celu potwierdzenia spełniania przez Wykonawcę warunków, o których mowa w pkt 6 SIWZ, Zamawiający żąda następujących dokumentów:

10.3.1. Wykazu dostaw wykonanych, w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów, czy zostały wykonane lub są wykonywane należycie - na formularzu zgodnym z treścią załącznika nr 5 do SIWZ (Wykaz dostaw).

Dowodami, o których wyżej mowa, są:

- referencje bądź inne dokumenty wystawione przez podmiot na rzecz którego dostawy były wykonywane;
- oświadczenie Wykonawcy – jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać referencji bądź innych dokumentów, o których wyżej mowa.

10.3.2. wykazu 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 informacją o podstawie do dysponowania tymi osobami – na formularzu zgodnym z treścią załącznika nr 6 do SIWZ (Wykaz osób);

10.4. W celu wykazania braku podstaw do wykluczenia Wykonawcy z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 5 pkt. 1 ustawy Pzp, Zamawiający żąda następujących dokumentów:

10.4.1. odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 5 pkt 1 ustawy Pzp. W tym zakresie zastosowanie ma art. 26 ust. 6 ustawy Pzp.

UWAGA: W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dokument składa każdy z Wykonawców występujących wspólnie.

10.5. Z treści złożonych dokumentów musi wynikać jednoznacznie, iż Wykonawca wykazał spełnianie warunków udziału w postępowaniu i brak podstaw do wykluczenia.

10.6. Nie wykazanie spełniania chociażby jednego warunku, skutkować będzie wykluczeniem Wykonawcy z postępowania.

10.7. **Wymogi szczególne w zakresie dokumentów dotyczących innego podmiotu żądane od Wykonawcy, którego oferta została oceniona jako najkorzystniejsza:**

W przypadku, gdy Wykonawca polega na zasobach innych podmiotów na zasadach określonych w art. 22a ustawy Pzp, Zamawiający żąda przedstawienia w odniesieniu do innego podmiotu:

10.7.1. odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp,

10.7.2. Stosownie do zakresu udostępnianych zasobów przez inny podmiot oraz warunków, których spełnianiu one służą, Wykonawca zobowiązany jest złożyć właściwe dokumenty tych podmiotów w celu wykazania spełnienia warunków udziału w postępowaniu przez Wykonawcę.

10.8. **Wymogi szczególne w zakresie dokumentów dotyczących Wykonawców wspólnie ubiegających się o zamówienie:** W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców (konsorcjum), dokumenty wymienione w pkt. 10.4 SIWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty wskazane w pkt 10.3. SIWZ składa ten Wykonawca-członek konsorcjum, który wykazuje spełnienie odpowiedniego warunku udziału w postępowaniu lub Wykonawcy wspólnie.

10.9. **Dokumenty Wykonawców spoza Rzeczypospolitej Polskiej**

10.9.1. Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej zamiast dokumentu, o którym mowa w pkt 10.4.1 SIWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości.

10.9.2. Dokumenty, o których mowa w pkt 10.9.1 SIWZ, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

10.9.3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania mają osoby, których dotyczą dokumenty, nie wydaje się dokumentów o których mowa w pkt 10.9.1. SIWZ, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania tej osoby. Przepisy pkt. 10.9.2. SIWZ stosuje się.

10.10. **Charakter/postać dokumentów lub oświadczeń:**

Zamawiający dopuszcza w postępowaniu dwie formy złożenia dokumentów lub oświadczeń tj. formę pisemną lub elektroniczną (nie dotyczy złożenia oferty oraz załączników).

Z uwagi na stan epidemii Zamawiający zaleca aby dokumenty i oświadczenia składane przez Wykonawcę w toku prowadzonego postępowania na wezwanie Zamawiającego oraz oświadczenie o którym mowa w pkt 9 SIWZ składane były w postaci elektronicznej, zgodnie z wymaganiami określonymi w pkt. 10.10.4-10.10.8 SIWZ.

Wymagania dotyczące formy pisemnej:

10.10.1. Dokumenty lub oświadczenia o których mowa w rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów *dokumentów*, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem. Pozostałe dokumenty lub oświadczenia składane są w oryginale.

10.10.2. Poświadczenie za zgodność z oryginałem następuje przez opatrzenie kopii dokumentu lub kopii oświadczenia, sporządzonych w postaci papierowej, własnoręcznym podpisem.

10.10.3. Wszelkie poprawki lub zmiany (skreślenie, itp.) w dokumentach lub oświadczeniach muszą być podpisane własnoręcznie przez uprawnioną osobę, w miejscu dokonanej poprawki lub zmiany. Naniesione zmiany muszą być czytelne.

Wymagania dotyczące formy elektronicznej:

10.10.4. Dokumenty lub oświadczenia o których mowa w rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów *dokumentów*, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia, składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem.

10.10.5. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawstwa, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.

10.10.6. Poświadczenie za zgodność z oryginałem elektronicznej kopii dokumentu lub oświadczenia, następuje przy użyciu kwalifikowanego podpisu elektronicznego.

10.10.7. W przypadku przekazywania przez Wykonawcę elektronicznej kopii dokumentu, podpisanie jej przez Wykonawcę albo przez podwykonawcę kwalifikowanym podpisem elektronicznym jest równoznaczne z poświadczeniem przez Wykonawcę albo przez podwykonawcę elektronicznej kopii dokumentu za zgodność z oryginałem.

10.10.8. W przypadku przekazywania przez Wykonawcę dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest równoznaczne z poświadczeniem przez Wykonawcę za zgodność z oryginałem wszystkich elektronicznych kopii dokumentów zawartych w tym pliku, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia albo przez podwykonawców.

10.11. **Reprezentacja i pełnomocnictwo**

10.11.1. W przypadku, gdy Wykonawcę reprezentuje pełnomocnik, do oferty należy dołączyć pełnomocnictwo podpisane przez osobę/osoby uprawnione do reprezentowania Wykonawcy. Treść pełnomocnictwa musi jednoznacznie wskazywać czynności, do wykonywania których pełnomocnik jest upoważniony (zakres umocowania). Pełnomocnictwo należy złożyć w oryginale lub kopii poświadczonej notarialnie za zgodność z oryginałem.

10.11.2. W przypadku Wykonawców składających wspólną ofertę, do oferty należy dołączyć pełnomocnictwo do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia (wystawione zgodnie z art. 23 ust. 2 ustawy Pzp). Treść pełnomocnictwa musi jednoznacznie wskazywać czynności, do wykonywania których pełnomocnik jest upoważniony (zakres umocowania).

Pełnomocnictwo należy złożyć w oryginale lub kopii poświadczonej notarialnie za zgodność z oryginałem.

10.11.3. Oferta musi być podpisana przez pełnomocnika/osobę umocowaną do reprezentowania Wykonawcy/Wykonawców.

10.12. **Wyjątki od obowiązku złożenia dokumentów:**

Wykonawca nie jest obowiązany do złożenia odpowiednich oświadczeń lub dokumentów, jeżeli:

10.12.1. Zamawiający 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.

10.12.2. Zamawiający posiada aktualne oświadczenia lub dokumenty dotyczące tego Wykonawcy (ze wskazaniem nazwy i numeru postępowania o udzielenie zamówienia publicznego – w formularzu Oferta).

11. SPOSÓB POROZUMIEWANIA SIĘ W POSTĘPOWANIU ORAZ OSOBY UPRAWNIONE DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

11.1. Komunikacja między Zamawiającym a Wykonawcami odbywa się za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2020 r., poz. 1041), osobiście, za pośrednictwem posłańca lub przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2020 r., poz. 344). Dokonany przez Wykonawcę wybór sposobu złożenia informacji/oświadczeń/dokumentów powinien uwzględniać obowiązek zachowania przez Wykonawcę wymagań w zakresie pisemnej formy oferty oraz obowiązku zachowania charakteru/postaci składanych dokumentów i oświadczeń określonych w pkt 8, 9 i 10 SIWZ.

11.2. Zamawiający dopuszcza również możliwość złożenia informacji/oświadczeń/dokumentów określonych w pkt. 9 i 10 SIWZ w formie elektronicznej za pomocą poczty elektronicznej (natalia.mosiadz@pgi.gov.pl). Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia publicznego. **Zamawiający nie dopuszcza możliwości elektronicznego złożenia oferty oraz załączników do oferty.**

11.3. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ. Zamawiający ma obowiązek udzielić odpowiedzi na pytania Wykonawcy, pod warunkiem, że wniosek o wyjaśnienie wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

11.4. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął w terminie późniejszym niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na wydłużenie biegu terminu składania wniosków o wyjaśnienie SIWZ, na które Zamawiający ma obowiązek udzielenia odpowiedzi.

11.5. Oświadczenie, wniosek, zawiadomienie, oraz informacje, w tym pytania do SIWZ i odpowiedzi uznaje się za złożone w chwili, w której wpłyną do adresata elektronicznie lub zostaną doręczone w inny sposób do siedziby Zamawiającego lub Wykonawcy. Przesyłając oświadczenie, wniosek, zawiadomienie oraz informacje, w tym pytania do SIWZ i odpowiedzi, elektronicznie, każda strona ma obowiązek potwierdzić wpływ (lub poinformować o braku wpływu) na żądanie drugiej strony.

11.6. Osobą uprawnioną do kontaktu z Wykonawcami jest:
Natalia Mosiądz (Biuro Zamówień Publicznych)
tel. +48 22 459 26 21

e- mail: natalia.mosiadz@pgi.gov.pl

11.7. Korespondencję dotyczącą prowadzonego postępowania należy kierować na adres Zamawiającego:
Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy
ul. Rakowiecka 4, 00-975 Warszawa
lub zgodnie z pkt. 11.2 SIWZ na adres poczty elektronicznej:
natalia.mosiadz@pgi.gov.pl

12. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium.

13. TERMIN ZWIĄZANIA OFERTĄ

Okres związania Wykonawcy złożoną ofertą wynosi 30 dni od upływu terminu składania ofert, określonego w pkt 15.2 SIWZ.

14. OPIS SPOSOBU PRZYGOTOWANIA OFERT

14.1. Wykonawca przedstawia ofertę o treści odpowiadającej treści SIWZ. Propozycje rozwiązań m.in. alternatywnych lub wariantowych nie będą brane pod uwagę, a oferta zostanie odrzucona na podstawie art. 89 ust. 1 pkt 2 ustawy Pzp.

14.2. Oferta musi zawierać co najmniej:
- 14.2.1. wypełniony formularz „Oferta", który stanowi załącznik nr 3 do SIWZ;
- 14.2.2. oświadczenie, o którym mowa w pkt. 8 SIWZ, które stanowi załącznik nr 4 do SIWZ;
- 14.2.3. dokument pełnomocnictwa (jeśli dotyczy);
- 14.2.4. zobowiązanie podmiotu trzeciego do udostępnienia zasobów, o których mowa w pkt 8.1.3.1. SIWZ (jeżeli dotyczy);
- 14.2.5. informację o podwykonawcach – jeśli Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcom zobowiązany jest wskazać części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podać nazwy firm podwykonawców w składanej ofercie;
- 14.2.6. w przypadku zastrzeżenia tajemnicy przedsiębiorstwa – stosowne wyjaśnienie, o którym mowa w pkt 14.23 SIWZ.

14.3. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia zgodnie z art. 23 ustawy Pzp.

14.4. Brak informacji, o której mowa w pkt 14.2.5. SIWZ, będzie uznany za stwierdzenie samodzielnego wykonania zamówienia przez Wykonawcę, który złożył ofertę.

14.5. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty oraz uczestnictwem w postępowaniu o udzielenie zamówienia publicznego.

14.6. Ofertę stanowi wypełniony i skonkretyzowany druk „OFERTA", którego wzór stanowi Załącznik nr 3 do SIWZ, z załączonymi dokumentami i oświadczeniami, wymaganymi niniejszą SIWZ.

14.7. Oferta wraz z załącznikami musi być sformułowana w języku polskim, w sposób czytelny, logiczny, pisemnie przy użyciu nośnika pisma nie ulegającego usunięciu bez pozostawienia śladów.

14.8. Zamawiający zaleca sporządzenie oferty na komputerze lub wypełnienie druków czytelnym pismem ręcznym.

14.9. 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.

14.10. W przypadku uzyskania dokumentów, o których mowa w pkt. 10.12.1 SIWZ w języku obcym, Zamawiający żąda od Wykonawcy przedstawienia tłumaczenia na język polski wskazanych przez Wykonawcę i pobranych samodzielnie przez Zamawiającego dokumentów.

14.11. Zamawiający informuje, że zamieszczane przez Zamawiającego na stronie internetowej wszelkie pliki zawierające edytowalne wersje SIWZ lub jej fragmentów należy traktować jedynie jako materiał pomocniczy, a wersjami obowiązującymi są zawsze wersje zamieszczone w formacie pdf lub xml.

14.12. Wykonawca może przepisać druki Zamawiającego, jednakże treść zawarta we wzorach Zamawiającego nie może ulec zmianie.
14.13. Zalecane jest, aby oferta była złożona na kolejno ponumerowanych stronach. Numeracja stron powinna rozpoczynać się od numeru 1, umieszczonego na pierwszej stronie oferty.
14.14. Oferta po jej otwarciu, w terminie wyznaczonym na termin otwarcia ofert, jest jawna i podlega udostępnieniu, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2020 r., poz. 1913), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępniane i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
14.15. Zamawiający wymaga aby oferta, wraz ze wszystkimi załącznikami, była podpisana przez osobę upoważnioną do reprezentowania Wykonawcy.
14.16. Zamawiający zaleca złożenie oferty w taki sposób, aby nie uległa zdekompletowaniu.
14.17. Oferty składane są w jednym egzemplarzu, w nieprzejrzystej i zamkniętej kopercie lub opakowaniu.
14.18. Koperta powinna być oznaczona oraz opisana w następujący sposób:

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

Oferta na „System filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB"
(Sygn. Postępowania: EZP-240-89/2020)

Nie otwierać przed godziną 10:30 dnia 14.12.2020 roku.

14.19. Konsekwencje złożenia oferty niezgodnie z ww. opisem ponosi Wykonawca.
14.20. W przypadku przekazania oferty do Zamawiającego osobiście za pośrednictwem operatora pocztowego lub posłańca, Wykonawca ponosi odpowiedzialność za datę i godzinę jej wpływu do Kancelarii Ogólnej PIG-PIB.
14.21. Wykonawca składa tylko jedną ofertę, w której może być zaoferowana tylko jedna cena. Jeżeli Wykonawca złoży więcej niż jedną ofertę, samodzielnie lub wspólnie z innymi Wykonawcami, wszystkie złożone przez niego oferty zostaną odrzucone.
14.22. Wykonawca może wprowadzić zmiany do oferty lub wycofać złożoną przez siebie ofertę. Dla uznania skuteczności wprowadzenia zmian do oferty, konieczne jest otrzymanie przez Zamawiającego pisemnego powiadomienia, podpisanego przez osoby uprawnione, o wprowadzeniu zmian do oferty, przed upływem ostatecznego terminu wyznaczonego do składania ofert. Dla uznania skuteczności wycofania złożonej oferty, konieczne jest otrzymanie przez Zamawiającego powiadomienia, podpisanego przez osoby uprawnione, o wycofaniu oferty, przed upływem ostatecznego terminu wyznaczonego do składania ofert.
14.23. Informacje zawarte w ofercie, stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji, co do których Wykonawca:
    14.23.1. zastrzegł, nie później niż w terminie składania ofert, że informacje stanowiące tajemnicę przedsiębiorstwa, nie mogą być udostępnione i muszą być oznaczone klauzulą: „NIE UDOSTĘPNIAĆ - INFORMACJE STANOWIĄ TAJEMNICĘ PRZEDSIĘBIORSTWA W ROZUMIENIU ART. 11 UST. 2 USTAWY O ZWALCZANIU NIEUCZCIWEJ KONKURENCJI" oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa - Wykonawca zobowiązany jest złożyć wraz z ofertą uzasadnienie zawierające w szczególności: określenie charakteru jaki mają zastrzeżone informacje, wskazanie działań jakie zostały podjęte przez Wykonawcę w celu zachowania poufności informacji zawartych w dokumentach oraz wskazanie czy informacje stanowiące tajemnicę przedsiębiorstwa zostały wcześniej ujawnione do wiadomości publicznej. 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.

14.23.2. Jednocześnie Zamawiający wskazuje, iż zgodnie z art. 8 ust. 3 ustawy Pzp, Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp.

14.23.3. Elementy oferty, które Wykonawca zamierza zastrzec jako tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji powinny zostać umieszczone w odrębnej, zaklejonej kopercie (lub zabezpieczone w inny sposób), opisanej „tajemnica przedsiębiorstwa", dołączonej do oryginału oferty. W treści oferty powinna zostać umieszczona informacja, że dany dokument jest zastrzeżony. Wykonawca zobowiązany jest wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa (art. 8 ust. 3 ustawy Pzp).

15. TERMIN I MIEJSCE SKŁADANIA I OTWARCIA OFERT

15.1. Oferty należy składać na adres:

Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy
ul. Rakowiecka 4, 00-975 Warszawa
Kancelaria Ogólna (parter budynku A, pok. 1) czynna w dni robocze od poniedziałku do piątku w godzinach 08:15-16:15

15.2. Termin składania ofert upływa **14.12.2020 r. o godz. 10:00**

15.3. Oferty dostarczone do Zamawiającego za pośrednictwem operatora pocztowego, osobiście lub posłańca będą zakwalifikowane do postępowania przetargowego pod warunkiem ich dostarczenia do terminu określonego w pkt 15.2 SIWZ. Decyduje data i godzina wpływu do Kancelarii Ogólnej PIG-PIB.

15.4. Zamawiający niezwłocznie zwraca ofertę, która została złożona po wyznaczonym terminie na składanie ofert.

15.5. Otwarcie złożonych ofert nastąpi w dniu **14.12.2020 r. o godz. 10:30,** w siedzibie Zamawiającego w bud. A, pok. nr 230.

15.6. Otwarcie ofert jest jawne.

15.7. Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie www.pgi.gov.pl/przetargi informacje dotyczące:

15.7.1. kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;

15.7.2. firm oraz adresów Wykonawców, którzy złożyli oferty w terminie;

15.7.3. ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach

– jeżeli dotyczy.

16. OPIS SPOSOBU OBLICZANIA CENY OFERTY

16.1. Wykonawca określi wszystkie ceny, zgodnie z Formularzem „Oferta" (Załącznik nr 3 do SIWZ).

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

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

16.4. Wszystkie płatności będą realizowane w złotych polskich, zgodnie z obowiązującymi przepisami. Zamawiający nie przewiduje rozliczeń w walutach obcych.

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

17. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM ZNACZENIA KRYTERIÓW I SPOSOBU OCENY OFERT

17.1. Ocenie zostaną poddane oferty nie podlegające odrzuceniu.

17.2. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującym kryterium i jego znaczeniem:

Numer kryterium	Nazwa kryterium	Waga podana w punktach
1	**Cena**	**100**

17.3. Liczba punktów przyznana poszczególnym ofertom zostanie obliczona z dokładnością do dwóch miejsc po przecinku albo z dokładnością wystarczającą do wykazania zróżnicowania ofert niepodlegających odrzuceniu.

17.4. Sposób obliczenia wartości punktowej w kryterium cena:

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

Maksymalna liczba punktów jaką może otrzymać Wykonawca w tym kryterium to 100.

17.5. Za ofertę najkorzystniejszą uznana zostanie oferta, która otrzyma najwyższą liczbę przyznanych punktów wg. ww. kryterium.

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

18.1. W przypadku, gdy jako najkorzystniejsza zostanie uznana oferta złożona przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, przed podpisaniem umowy Wykonawcy ci mogą zostać zobowiązani do przedłożenia Zamawiającemu umowy regulującej ich współpracę.

18.2. Zamawiający poinformuje Wykonawcę, którego oferta zostanie wybrana jako najkorzystniejsza, o miejscu i terminie zawarcia umowy.

18.3. Przed podpisaniem umowy Wykonawca powinien przedstawić pełnomocnictwo do jej podpisania, jeżeli nie wynika ono z załączonych do oferty dokumentów.

19. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

20. WARUNKI UMOWY O WYKONANIE ZAMÓWIENIA

20.1. Ogólne i szczegółowe warunki umowy, które uwzględnione będą w przyszłej umowie z wybranym w wyniku niniejszego postępowania Wykonawcą zamieszczone są w Istotnych postanowieniach umowy – stanowiących załącznik nr 2 do SIWZ.

20.2. Wszelkie pytania i wątpliwości dotyczące Istotnych postanowień umowy, będą rozpatrywane jak dla całej SIWZ, zgodnie z art. 38 ustawy Pzp.

20.3. Konieczność powierzenia podwykonawcom realizacji jakiegoś elementu zamówienia, wynikła w trakcie realizacji zamówienia, wymaga uzyskania uprzedniej pisemnej zgody Zamawiającego.

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

20.5. Przewidywane zmiany umowy i warunki ich wprowadzenia zostały określone w Istotnych postanowieniach umowy.

21. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁYGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

Wykonawcom i innym osobom, którzy mają lub mieli interes w uzyskaniu zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp, przysługują środki ochrony prawnej określone w Dziale VI ww. ustawy Pzp.

22. DANE OSOBOWE

22.1. 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:

22.1.1. 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

22.1.2. administrator wyznaczył inspektora ochrony danych, z którym może się Pani/Pan skontaktować w sprawach ochrony i przetwarzania danych osobowych pod adresem poczty elektronicznej: dane.osobowe@pgi.gov.pl lub pisemnie na adres siedziby PIG-PIB

22.1.3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn.: **Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB** (Sygn. postępowania: EZP-240-89/2020), prowadzonym w trybie przetargu nieograniczonego. Przetwarzanie danych osobowych będzie możliwe również w celu wykonania zadania realizowanego w interesie publicznym (podstawa prawna art. 6 ust. 1 lit. e RODO), w celach archiwalnych wobec prawnie uzasadnionego interesu zabezpieczenia i przechowania danych osobowych na wypadek prawnej potrzeby wykazania faktów (podstawa prawna art. 6 ust. 1 lit. f RODO) oraz w celach ustalenia, dochodzenia lub obrony przed roszczeniami, które mogą powstać w związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego (podstawa prawna art. 6 ust. 1 lit. f RODO). Ponadto w przypadku Wykonawcy, z którym zostanie zawarta umowa, podstawę przetwarzania danych stanowić będzie art. 6 ust. 1 lit. b RODO, ponieważ przetwarzanie będzie niezbędne do wykonania tej umowy

22.1.4. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp. Ponadto do Pani/Pana danych osobowych mogą mieć również dostęp podmioty przetwarzające dane osobowe w imieniu PIG-PIB tj. podmioty świadczące pomoc prawną, usługi informatyczne, kurierskie i pocztowe, archiwizacyjne i związane z niszczeniem dokumentów. Pani/Pana dane osobowe mogą być udostępnione również innym podmiotom, jeżeli obowiązek taki będzie wynikać z przepisów prawa

22.1.5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy 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. W przypadku zawarcia umowy z Wykonawcą, jego dane osobowe będą przechowywane przez czas trwania tej umowy, do momentu wygaśnięcia roszczeń związanych z wykonaniem zobowiązań umownych, chyba że niezbędny będzie dłuższy okres przetwarzania w przypadkach nakazanych prawem

22.1.6. obowiązek podania przez Paniq/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp

22.1.7. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO

22.1.8. posiada Pani/Pan:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczą-cych;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych*;
- 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**;

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

22.1.9. nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- 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.

---

* ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania 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.*

*****Wyjaśnienie:*** *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.*

23. POSTANOWIENIA KOŃCOWE

23.1. Do spraw nieuregulowanych w niniejszej SIWZ zastosowanie mają przepisy ustawy Pzp.

23.2. Wszelkie koszty związane z przygotowaniem oferty i udziałem w postępowaniu ponosi Wykonawca.

23.3. Wszystkie załączniki do niniejszej SIWZ stanowią jej integralną część.

24. ZAŁĄCZNIKI:

24.1. Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia;

24.2. Załącznik nr 2 do SIWZ – Istotne postanowienia umowy;

24.3. Załącznik nr 3 do SIWZ – Formularz „Oferta";

24.4. Załącznik nr 4 do SIWZ – Oświadczenie o spełnianiu warunków udziału w postępowaniu oraz braku podstaw do wykluczenia z postępowania;

24.5. Załącznik nr 5 do SIWZ – Wykaz dostaw;

24.6. Załącznik nr 6 do SIWZ – Wykaz osób.

Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa systemu filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla Państwowego Instytutu Geologicznego – Państwowego Instytutu Badawczego.

   1.1 System filtrowania i bezpieczeństwa ruchu stron WWW (FORCEPOINT TRITON) wraz z modułem WEB DLP lub równoważny dla około 950 użytkowników sieci LAN Zamawiającego.
   1.2 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.
   1.3 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. 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)

3. 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 zgłoszenia dokonanego przez Zamawiającego lub w razie braku potwierdzenia od czasu, w którym winna nastąpić reakcja Wykonawcy,
   - w przypadku ustania działania całego systemu, usunięcie awarii w czasie 48 godzin od daty potwierdzenia przyjęcia zgłoszenia,
   - Czas reakcji na zgłoszenie (potwierdzenie przyjęcia zgłoszenia) usterki to 1 dzień tj. najpóźniej do godz. 16.00 dnia następnego po dniu zgłoszenia.

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

5. Termin realizacji zamówienia do dnia 31.12.2020 r. wraz ze świadczeniem wsparcia do dnia 31.12.2021 r.

Opis równoważności:

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. Akacja (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 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.

Załącznik nr 2 do SIWZ

Istotne Postanowienia Umowy
Umowa nr CRZP-240-…./2020/część nr…

zawarta w dniu …… …….…… 2020 r. w Warszawie 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:
……
zwanym w dalszej części umowy **Zamawiającym** lub **PIG-PIB,**
a
*(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 trybie przetargu nieograniczonego (EZP-240-81/2020) pn.: **Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB**" z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 z późn. zm.) – dalej „ustawa Pzp" – została zawarta Umowa o następującej treści:

§ 1. Przedmiot Umowy

1. Na zasadach określonych w dokumentacji przetargowej, niniejszej Umowie i załącznikach do

niej, Zamawiający zleca i zobowiązuje się kupić, a Wykonawca zobowiązuje się do sprzedaży i dostarczenia Zamawiającemu **licencji do oprogramowania systemów filtrowania i bezpieczeństwa ruchu stron WWW oraz ochrony danych DLP** szczegółowo określonych rzeczowo, ilościowo i finansowo w Opisie przedmiotu zamówienia oraz w Ofercie Wykonawcy z dnia ……., które stanowią odpowiednio **Załączniki nr 1 i nr 2** do Umowy**.**

2. Ponadto, Wykonawca zobowiązuje się - przez okres i na zasadach określonych w Opisie przedmiotu zamówienia – do świadczenia wsparcia technicznego (maintenance), 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 w module ochrony poczty.
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. Zamawiający dopuszcza aby Wykonawca dostarczył pliki instalacyjne wraz z dokumentacją i kluczami licencyjnymi na nośnikach DVD.
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

1. Wykonawca zobowiązuje się dostarczyć licencje oprogramowania wraz z dokumentami potwierdzającymi prawo Zamawiającego do asysty technicznej (Certyfikat Asysty Technicznej) w terminie do 31 grudnia 2020 r. oraz do świadczenia wsparcia technicznego (§ 1 ust. 2) przez okres wskazany w Opisie przedmiotu zamówienia (Załącznik nr 1).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)*.
2. Oprogramowanie dostarczone będzie do Zamawiającego w sposób następujący:
   1) do siedziby Zamawiającego w Warszawie, ul. Rakowiecka 4 poprzez przekazanie oprogramowania na nośniku wraz z dokumentami potwierdzającymi udzielenie licencji, lub

2) 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.

3. W przypadku, o którym mowa w ust. 2 pkt 1 powyżej, dostawę należy zrealizować w dni robocze tj. od poniedziałku do piątku (za wyjątkiem dni ustawowo wolnych od pracy) w godzinach: 8:00-16:00, po uprzednim zawiadomieniu, wskazanego w § 5 ust. 3 przedstawiciela Zamawiającego, o planowanej dostawie. Zawiadomienie powinno nastąpić z wyprzedzeniem 1 dnia roboczego.

§ 3. Wartość Przedmiotu Umowy

1. Z tytułu należytego i zgodnego z niniejszymi warunkami wykonania przez Wykonawcę Umowy, Zamawiający zobowiązuje się zapłacić, zgodnie z ofertą Wykonawcy stanowiącą Załącznik nr 2 do Umowy, wynagrodzenie łączne w wysokości:

   wynagrodzenie netto: …….. zł (słownie:…… 00/100)
   wynagrodzenie brutto: …… zł (słownie: …… 00/100).

2. Wynagrodzenie, o którym mowa w ust. 1, obejmuje wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej i zgodnej z niniejszą Umową oraz obowiązującymi przepisami realizacji Umowy, w tym w szczególności koszt zakupu licencji oprogramowania wraz ze wsparciem technicznym oraz koszty dostawy do siedziby Zamawiającego.

§ 4. Warunki płatności

1. Płatność będzie dokonana na podstawie prawidłowo wystawionej faktury wystawionej na Zamawiającego (Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy, ul. Rakowiecka 4, 00-975 Warszawa), przelewem, na konto Wykonawcy podane na prawidłowo wystawionej fakturze VAT (albo, w przypadku konieczności zastosowania mechanizmu podzielonej płatności – na rachunki bankowe Wykonawcy, w tym rachunek VAT Wykonawcy, wskazane na fakturze), w terminie 30 dni od dnia doręczenia faktury Zamawiającemu wraz z oryginałem Protokołu odbioru podpisanego bez zastrzeżeń przez Zamawiającego.
2. Płatność uważa się za zrealizowaną w dniu wypływu środków pieniężnych z konta Zamawiającego.
3. W razie wystąpienia opóźnienia w płatności Zamawiający zapłaci Wykonawcy odsetki ustawowe.
4. 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.
5. 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 2020 roku poz.935 z późn. zm.) posiada status dużego przedsiębiorcy.

§ 5. Odbiory

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 zdanie drugie*.

3. Do podpisywania Protokołów odbioru upoważnione są:
   - ze strony Zamawiającego: p……, tel. ……, e-mail: ……;
   - ze strony Wykonawcy: p……, tel. ……, e-mail: ……
4. Zmiana osób wskazanych w ust. 3 i ich danych teleadresowych, nie wymaga zmiany Umowy i następuje po uprzednim zawiadomieniu drugiej strony w formie pisemnej lub elektronicznej.
5. W przypadku stwierdzenia w toku procedury odbiorowej wad, braków lub innych zastrzeżeń do przedmiotu Umowy (m.in. wobec negatywnie zakończonej próby uruchomienia oprogramowania), Wykonawca zobowiązuje się do ich usunięcia w terminie uzgodnionym przez Strony. W takim przypadku za datę wykonania Umowy uważa się datę dokonania przez Wykonawcę wszelkich poprawek i uzupełnień lub usunięcia wad, zgłoszonych przez Zamawiającego.

§ 6. Wsparcie techniczne

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) pod numerem tel.: ……
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.
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 „Instrukcję instalacji".
8. Wykonawca udziela Zamawiającemu gwarancji na świadczoną usługę na zasadach określonych umową licencyjną producenta oprogramowania systemowego, która będzie dołączona do Umowy.
9. Wszelkie zmiany konfiguracyjne w oprogramowaniu Wykonawca zobowiązany jest dokumentować, a dokumentację pełnej konfiguracji przekazywać Zamawiającemu w wersji elektronicznej.
10. 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 3** do Umowy.
11. Szczegółowy zakres wsparcia technicznego oraz terminy i zasady realizacji określa OPZ.
12. Wsparcie techniczne będzie świadczone w języku polskim.

§ 7. Autorskie prawa majątkowe

1. W ramach wynagrodzenia, o którym mowa w § 2 ust. 1 powyżej, Wykonawca udziela Zamawiającemu licencji na korzystanie z oprogramowania. Licencja na oprogramowanie zostanie udzielona zgodnie z warunkami licencyjnymi producenta oprogramowania.

2. Wykonawca oświadcza, że posiada wszelkie niezbędne uprawnienia do realizacji przedmiotu niniejszej Umowy.
3. Wykonawca zapewnia, iż wskutek wykonania niniejszej Umowy nie dojdzie do naruszenia praw osób trzecich, w szczególności praw twórców i właściciela praw autorskich. W przypadku zgłoszenia wobec Zamawiającego roszczeń o naruszenie praw osób trzecich objętych powyższym zapewnieniem, Wykonawca podejmie na swój koszt wszelkie środki obrony Zamawiającego przed takimi roszczeniami oraz zarzutami i spowoduje, że Zamawiający będzie od nich zwolniony, a także pokryje wszelkie koszty i straty, jak poniesie Zamawiający z tego tytułu, w tym także wynikające z konieczności pozyskania oprogramowania zgodnego z Umową oraz szkód wynikających z niemożliwości korzystania z oprogramowania.

§ 8. Gwarancja

1. Wykonawca udziela gwarancji jakości na dostarczone nośniki i klucze licencyjne na okres 3 miesięcy od dnia podpisania przez Zamawiającego Protokołu odbioru „bez zastrzeżeń".
2. Gwarancja musi być zgodna z gwarancją udzielaną przez producenta oprogramowania i obejmować gwarancje prawidłowego działania programów, nośników oraz działania elementów sprzętowych oprogramowania (*kluczy sprzętowych*).
3. Wykonawca wykona zobowiązania wynikające z gwarancji jakości w ciągu 5 dni od daty powiadomienia go przez Zamawiającego o stwierdzonej wadzie.
4. Za wadę uznaje się w szczególności fizyczne uszkodzenie nośników, na których dostarczono oprogramowanie, uszkodzenie klucza sprzętowego USB, jak również nieprawidłowości w działaniu oprogramowania, tj. działanie w sposób niezgodny ze specyfikacją oprogramowania.

§ 9. Kary umowne

1. Wykonawca zapłaci Zamawiającemu, w terminie 7 dni od dnia otrzymania dokumentu stwierdzającego obciążenie, kary umowne:
   1) z tytułu zwłoki Wykonawcy w dostarczeniu przedmiotu Umowy w terminie, o którym mowa w § 2 ust. 1 – w wysokości 0,5% wynagrodzenia brutto za wykonanie przedmiotu Umowy (§ 3 ust. 1), liczonej za każdy dzień zwłoki, jednak nie więcej niż 15 % łącznej kwoty wynagrodzenia, o którym mowa w § 3 ust. 1 powyżej,
   2) w przypadku braku reakcji na zgłoszenie, w terminie wskazanym w § 6 ust. 4 Umowy – w wysokości 200 zł,
   3) każdorazowo z tytułu zwłoki Wykonawcy w wykonywaniu obowiązków wynikających ze wsparcia technicznego ponad terminy określone w Załączniku nr 1 - w wysokości 0,5% wynagrodzenia brutto za wykonanie przedmiotu Umowy (§ 3 ust. 1), liczonej za każde rozpoczęte 24 godziny zwłoki, jednak nie więcej niż 15 % łącznej kwoty wynagrodzenia, o którym mowa w § 3 ust. 1 powyżej.
   4) za odstąpienie Wykonawcy od Umowy z przyczyn leżących po jego stronie - w wysokości 15 % łącznego wynagrodzenia brutto, o którym mowa w § 3 ust. 1 powyżej.
   5) za odstąpienie Zamawiającego od Umowy z przyczyn leżących po stronie Wykonawcy - w wysokości 15 % łącznego wynagrodzenia brutto, o którym mowa w § 3 ust. 1 powyżej.
2. Zamawiający może dochodzić na zasadach ogólnych odszkodowania przenoszącego wysokość zastrzeżonych kar umownych.

§ 10. Zmiany w Umowie

1. Zamawiający przewiduje możliwość wprowadzenia zmian postanowień zawartej Umowy w stosunku do treści przedłożonej w niniejszym postępowaniu Oferty, w następującym zakresie:
   1) zmiany przepisów mających zastosowanie przy wykonaniu Umowy; w szczególności zmiany stawki podatku od towarów i usług;
   2) poprawy jakości lub innych parametrów charakterystycznych dla danego elementu objętego przedmiotem zamówienia 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 zamówienia, 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;

3) zmiany terminu realizacji lub terminów płatności w przypadku:

a) wstrzymania przez Zamawiającego realizacji przedmiotu Umowy, niewynikającego z winy Wykonawcy,

b) jeżeli Wykonawca zgłosi przeszkodę w realizacji zadania zawinioną przez Zamawiającego;

c) 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 terminowość realizacji Umowy;

- w zakresie dostosowania Umowy do tych zmian;

4) zmiany wysokości naliczonej Wykonawcy kary umownej, w przypadku, gdy zobowiązanie Wykonawcy zostało w znacznej części wykonane i Zamawiający nie poniósł szkody.

2. Zmiana treści Umowy może nastąpić, jeśli oprogramowanie, którego dotyczy licencja, zostało wycofane z rynku, a proponowane oprogramowanie w wersji wyższej tego samego producenta posiada funkcjonalność, cechy i parametry nie gorsze niż oprogramowanie wycofane, w takim wypadku warunki realizacji Umowy i cena pozostają bez zmian.
3. Ponadto, zmiana Umowy może dotyczyć zasad przetwarzania danych osobowych, w przypadku, o którym mowa w § 13 ust. 9 poniżej.
4. Każda zmiana Umowy może nastąpić jedynie za zgodą obu stron wyrażoną na piśmie w formie aneksu pod rygorem nieważności, z zastrzeżeniem postanowień § 5 ust. 4.

§ 11. Odstąpienie od Umowy

1. Zamawiający może odstąpić od Umowy w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. W takim przypadku odstąpienie od Umowy powinno nastąpić w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.
2. W przypadku, o którym mowa w ust. 1 powyżej, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
3. Zamawiający jest uprawniony do odstąpienia od Umowy (w całości lub części), ze skutkiem na dzień złożenia Wykonawcy oświadczenia (ex nunc), jeżeli:

1) pozostaje w zwłoce z dostarczeniem przedmiotu Umowy o 3 dni ponad termin określony § 2 ust. 1;

2) zwłoka z realizacją wsparcia technicznego lub czas reakcji przekroczy o 72 godziny terminy określone w Załączniku nr 1;

3) Wykonawca nie wykonuje Umowy lub wykonuje ją nienależycie (w innych niż wskazane w pkt 1 i 2 przypadkach), po uprzednim wyznaczeniu Wykonawcy dodatkowego terminu na terminowe/należyte wykonanie zobowiązania;

4) zostanie wydany nakaz zajęcia majątku lub otwarta likwidacja Wykonawcy, w zakresie uniemożliwiającym wykonywanie przedmiotu niniejszej Umowy;

5) Wykonawca – choćby tylko faktycznie – zaprzestanie prowadzenia działalności.

4. 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.
5. Odstąpienie od Umowy, na zasadach określonych w ust. 3 powyżej, może nastąpić w terminie do 13 miesięcy od dnia zawarcia Umowy.

§ 12. Zachowanie poufności

1. Wszelkie informacje, co do których Strona powzięła wiadomość w związku z wykonaniem bądź zawarciem niniejszej Umowy, objęte są klauzulą poufności w czasie trwania niniejszej Umowy, jak również po jej ustaniu Strona nie może bez zgody Strony Ujawniającej wyrażonej na piśmie, w jakikolwiek sposób wykorzystywać, rozpowszechniać lub udostępniać osobom trzecim informacji lub materiałów zdobytych, powstałych lub przekazanych przez Stronę Ujawniającą podczas realizacji niniejszej Umowy(„informacje poufne").
2. Stronie Otrzymującej nie wolno, bez uprzedniej pisemnej zgody Strony Ujawniającej, wykorzystywać jakichkolwiek dokumentów lub informacji, pozyskanych w związku z realizacją niniejszej Umowy w celach innych niż wykonanie Umowy.
3. Zobowiązania do zachowania poufności zawarte w niniejszym paragrafie nie mają zastosowania do informacji poufnych, które:
   1) zgodnie z prawem znajdują się w posiadaniu Strony przed ich otrzymaniem od drugiej Strony,
   2) zostały lub będą podane do wiadomości publicznej w sposób inny, niż poprzez działanie lub zaniechanie Strony Otrzymującej,
   3) zostały niezależnie uzyskane od osoby trzeciej, która deklaruje, iż posiada prawo do rozpowszechniania takich informacji w momencie ich uzyskania przez Stronę Otrzymującą, lub
   4) zostały niezależnie opracowane przez Stronę Otrzymującą bez odniesienia do lub polegania na Informacjach Poufnych przekazanych przez Stronę Ujawniającą w ramach niniejszej Umowy,
   5) zostały ujawnione zgodnie z wymogami prawa po uprzednim pisemnym powiadomieniu drugiej Strony.

§ 13. Ochrona danych osobowych

1. Strony oświadczają, że przetwarzanie w zakresie udostępnionych im przez drugą Stronę Umowy danych osobowych dokonywane będzie przez każdą ze Stron jako administratora danych osobowych w celu realizacji przedmiotu Umowy oraz dochodzenia wynikających z niej ewentualnych roszczeń z uwzględnieniem wymogów określonych w rozporządzeniu 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), opublikowanego w Dz. Urz. UE z 04.05.2016 L 119/1, zwanego dalej RODO, jak również na podstawie innych obowiązujących przepisów mających zastosowanie do ochrony danych osobowych.
2. Wykonanie Umowy nie wiąże się z przetwarzaniem danych osobowych w rozumieniu RODO, z zastrzeżeniem przetwarzania w zakresie danych osobowych Wykonawcy, w sytuacji gdy jest on osobą fizyczną (w tym osobą fizyczną prowadzącą działalność gospodarczą), a także danych osobowych osób, które Wykonawca wskazał ze swej strony do realizacji Umowy.
3. Administratorem danych osobowych przekazanych przez Wykonawcę jest Zamawiający: Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy (PIG-PIB), ul. Rakowiecka 4, 00-975 Warszawa, tel. (+48) 22 45 92 000, fax. tel. (+48) 22 45 92 001, email biuro@pgi.gov.pl. Zamawiający wyznaczył Inspektora Ochrony Danych, z którym można się skontaktować w sprawach ochrony i przetwarzania danych osobowych pod adresem poczty elektronicznej: dane.osobowe@pgi.gov.pl lub pisemnie na adres siedziby Zamawiającego.
4. Dane osobowe udostępnione Zamawiającemu przez Wykonawcę będą przetwarzane w celu

zawarcia i realizacji niniejszej Umowy (podstawa art. 6 ust. 1 lit a lub lit. b RODO), jak również w celach archiwalnych wobec prawnie uzasadnionego interesu zabezpieczenia i przechowania danych osobowych na wypadek prawnej potrzeby wykazania faktów (podstawa prawna art. 6 ust. 1 lit. f RODO) oraz w celu ustalenia, dochodzenia lub obrony przed roszczeniami, które mogą powstać w związku z zawarciem i realizacją Umowy (podstawa prawna art. 6 ust. 1 lit. f RODO).

5. Odbiorcami danych osobowych udostępnionych Zamawiającemu przez Wykonawcę mogą być podmioty świadczące pomoc prawną, usługi informatyczne, kurierskie i pocztowe, archiwizacyjne, jak również inne podmioty, jeżeli obowiązek taki będzie wynikać z przepisów prawa.
6. Dane osobowe udostępnione Zamawiającemu przez Wykonawcę będą przetwarzane przez czas trwania Umowy, do momentu wygaśnięcia roszczeń związanych z wykonaniem zobowiązań umownych, chyba że niezbędny będzie dłuższy okres przetwarzania w przypadkach nakazanych prawem.
7. Osoby, który dane osobowe zostały udostępnione Zamawiającemu, posiadają na zasadach określonych w RODO prawo dostępu, sprostowania, ograniczenia przetwarzania, prawo sprzeciwu, prawo do usunięcia i przenoszenia danych osobowych, jak również prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych. W odniesieniu do udostępnionych Zamawiającemu danych osobowych nie będą podejmowane decyzje w sposób zautomatyzowany, stosownie do art. 22
8. Wykonawca zobowiązuje się do poinformowania osób, które będą uczestniczyć w wykonaniu niniejszej Umowy, o przetwarzaniu ich danych osobowych przez Zamawiającego wyłącznie w celach związanych z realizacją tej Umowy i na zasadach określonych powyżej.
9. W przypadku, gdyby w trakcie wykonania Umowy powstała konieczność powierzenia danych osobowych drugiej stronie Umowy, Strony określą odrębnie zasady ich powierzenia.

§ 14. Postanowienia końcowe

1. Ewentualne spory wynikłe z realizacji niniejszej Umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.
2. Niniejsza Umowa wchodzi w życie w dniu jej podpisania przez Strony.
3. Niniejsza Umowa została zawarta w 3 egzemplarzach, 2 egzemplarze dla Zamawiającego i 1 egzemplarz dla Wykonawcy.

Załączniki:

1. Załącznik nr 1 - Opis przedmiotu zamówienia;
2. Załącznik nr 2 - Wniosek o nadanie/ zmianę /cofnięcie/ uprawnień dostępowych do systemów informatycznych;
3. Załącznik nr 3 - Oferta Wykonawcy z dnia …….2020 r.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 2 do Umowy

Wniosek nadania-cofnięcia uprawnień

A. DANE IDENTYFIKACYJNE

1. **Komórka organizacyjna PIG-PIB:**
2. **Wnioskujący:**
   2.1. Imię i Nazwisko ……
   2.2. Stanowisko ……

3. **Typ operacji:** przyznanie ☐ zmiana ☐ odebranie ☐
4. **Dane osoby, której dotyczy wniosek:**
   4.1. Imię ……..
   4.2. Nazwisko ……..
   4.3. Stanowisko/Rola ……..
   4.4. Rodzaj umowy od dnia ……. do dnia…….
5. **Miejsce pracy:**
   5.1. Pokój nr, budynek ……..
   5.2. nr telefonu ……..……
6. **Certyfikat niekwalifikowany PIG-PIB** data ważności – …….

B. DOSTĘPY DO APLIKACJI I DYSKÓW SIECIOWYCH

1. Dostęp zgodnie z Polityką Bezpieczeństwa Informacji PIG-PIB w zależności od umowy:

☐ Użytkownik „PRACOWNIK NA UMOWĘ O PRACĘ” : *na okres do dnia:……*

☐ Użytkownik „PRACOWNIK NA UMOWĘ O PRACĘ - TELEPRACA”: *na okres do dnia:……*

☐ Użytkownik „PRACOWNIK NA UMOWĘ ZLECENIE/ O DZIEŁO”: *na okres do dnia:……*

☐ Użytkownik „STAŻYSTA/PRAKTYKANT”: *na okres do dnia:……*

☐ Użytkownik „UMOWA ZEWNĘTRZNA”: *na okres do dnia:……*

☐ Użytkownik „GOŚĆ”: *na okres do dnia:……*

2. Dostęp zdalny

☐ *na okres do dnia:……*

3. Inne aplikacje (wypisać z podaniem nazwy i okresu jeżeli jest inny niż wynikający z umowy)

……

☐ *na okres do dnia:……*

Oświadczam, iż zapoznałem/am się z Procedurą bezpiecznego użytkowania Systemów Teleinformatycznych PIG-PIB i zobowiązuję się do jego przestrzegania.

data *podpis i pieczęć przełożonego*

C. WERYFIKACJA WŁAŚCICIELA ZASOBU

Właściciel merytoryczny zasobu wskazuje kategorię danych, do których pracownik otrzymuje dostęp:

☐ KRYTYCZNE ☐ WAŻNE
☐ STANDARDOWE ☐ ZWYKŁE

Akceptacja/odmowa akceptacji:

……..…….
data, podpis i pieczęć Właściciela Zasobu

Akceptacja/odmowa akceptacji:

……..
data, podpis i pieczęć pracownika komórki odpowiedniej ds. cyberbezpieczeństwa

Załącznik nr 3 do SIWZ

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

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

O F E R T A

Nawiązując do ogłoszenia o przetargu nieograniczonym (sygn. postępowania: EZP-240-89/2020) na:

Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem 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 istotnych warunków zamówienia za cenę brutto:

…….. zł netto (słownie: ……..… złotych)

…….. zł brutto (słownie: ……..… złotych)

2. Oświadczamy, że:

1) Zapoznaliśmy się z treścią SIWZ, a w szczególności z opisem przedmiotu zamówienia i z postanowieniami umowy, ze zmianami i wyjaśnieniami treści SIWZ oraz że wykonamy zamówienie na warunkach i zasadach określonych tam przez Zamawiającego, dokładając najwyższej staranności.
2) 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.
3) Przedmiot umowy realizowany będzie zgodnie z zapisami Istotnych postanowień umowy.
4) Przedmiot zamówienia zostanie wykonany zgodnie z terminem określonym w pkt. 4 SIWZ.

5) Akceptujemy warunki płatności określone w SIWZ.
6) Akceptujemy warunki gwarancji określone w SIWZ.
7) Otrzymaliśmy konieczne informacje do przygotowania oferty. Akceptujemy wskazany w SIWZ termin związania ofertą, w razie wybrania naszej oferty zobowiązujemy się do podpisania umowy na warunkach zawartych w SIWZ w miejscu i terminie wskazanym przez Zamawiającego.
8) Informacje i dokumenty zawarte w ofercie na stronach od …. do …. stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ujawniane pozostałym uczestnikom postępowania (wypełnić jeśli dotyczy).
(Zamawiający wskazuje, iż zgodnie z art. 8 ust. 3 ustawy Pzp Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp).
9) 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.).
10) Jesteśmy/nie jesteśmy mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem[1].
11) zamówienie wykonamy samodzielnie*/ Część zamówienia *(określić zakres przewidywany do powierzenia podwykonawcom)*…….. zamierzamy powierzyć podwykonawcom*.

Firma, adres podwykonawcy	Zakres przewidywany do powierzenia podwykonawcy

**niepotrzebne skreślić*

12) Informujemy o dostępności wymaganych w SIWZ oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy Pzp:

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

13) Wszelką korespondencję w dotyczącą niniejszego zamówienia należy kierować na:

Imię i nazwisko	
Instytucja	
Adres	
Nr telefonu	
Adres e-mail	

14) Na ..... kolejno ponumerowanych stronach składamy całość oferty. Załącznikami do niniejszej oferty, stanowiącymi jej integralną cześć są:
    1) ……
    2) ……

[1] Zgodnie z zaleceniem Komisji Europejskiej z dnia 6 maja 2003 r. dot. definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw:
Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.
Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.
Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR *lub* roczna suma bilansowa nie przekracza 43 milionów EUR.

3) ……

**odpowiednio skreślić albo wypełnić*

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania Wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych)	Miejscowość i data

Załącznik nr 4 do SIWZ

I. OŚWIADCZENIE WYKONAWCY O SPEŁNIANIU 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.:
Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB (sygn. postępowania: EZP-240-89/2020), spełniamy warunki o których mowa w pkt 6 SIWZ.

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data:

II. INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW*:

Oświadczamy, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w pkt 6.2 SIWZ, polegamy na zasobach następującego/ych podmiotu/ów: ……..……..…….., w następującym zakresie: ……..…… ……. *(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)*.

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data:

* wypełnić i załączyć do oferty (w przypadku nie polegania na zasobach innych podmiotów – zaleca się wpisać – nie dotyczy)

III. OŚWIADCZENIE
O BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA

My niżej podpisani, działając w imieniu i na rzecz:

.....

.....

.....
(nazwa /firma/ i adres Wykonawcy)

niniejszym oświadczamy, że ubiegając się o zamówienie publiczne pn.:
Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB (sygn. postępowania: EZP-240-89/2020),
1)* nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 pkt 13-22 oraz ust. 5 pkt 1 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz.1843 ze zm.).

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data:

2)* zachodzą w stosunku do nas podstawy wykluczenia z postępowania na podstawie art. …… ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp)*. Jednocześnie oświadczamy, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjęliśmy następujące środki naprawcze:
……

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data:

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

IV. OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA*:

Oświadczamy, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: ……..…… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)* nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data:

* wypełnić i załączyć do oferty jeśli dotyczy

Załącznik nr 5 do SIWZ

……..
Nazwa (firma) wykonawcy albo wykonawców
ubiegających się wspólnie o udzielenie zamówienia

WYKAZ DOSTAW

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego pn.: **Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB** (sygn. postępowania: EZP-240-89/2020)**,** oświadczamy, że w ciągu ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie, zrealizowaliśmy następujące usługi zgodnie z warunkiem opisanym w punkcie 6.2. niniejszej SIWZ:

Przedmiot zamówienia	**Podmiot na rzecz, którego były realizowane dostawy**	**Wartość zamówienia brutto (zł)**	**Daty wykonania**
Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem	…… *(firma)* …… …… *(adres)*		od…… *(dd/mm/rrrr)* do…… *(dd/mm/rrrr)*

**należy wypełnić / skreślić*
***W razie potrzeby należy dodać kolejne wiersze.*

W załączeniu dokumenty potwierdzające, że wyżej wyszczególnione dostawy zostały zrealizowane należycie.

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data:

Załącznik nr 6 do SIWZ

……
Nazwa (firma) wykonawcy albo wykonawców
ubiegających się wspólnie o udzielenie zamówienia

WYKAZ OSÓB

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego na: **Dostawa licencji do systemów filtrowania i bezpieczeństwa ruchu stron WWW, ochrony danych DLP oraz poczty wraz ze wsparciem dla PIG – PIB** (sygn. postępowania EZP-240-89/2020), oświadczamy, że do realizacji zamówienia będziemy dysponować następującymi osobami zgodnie z warunkiem określonym w pkt. 6.2. SIWZ

Imię i nazwisko	**Posiadane certyfikaty:**	**Podstawa do dysponowania ww. osobą**
	Certyfikat administratora DLP	własny/udostępniony*
	Certyfikat administratora e-mail security	własny/udostępniony*
	Certyfikat administratora web security	własny/udostępniony*

**należy wypełnić / skreślić*
***W razie potrzeby należy dodać kolejne wiersze.*

Lp.	Nazwisko i imię osoby (osób) uprawnionej(ych) do reprezentowania wykonawcy lub posiadającej (ych) pełnomocnictwo	Podpis(y) osoby(osób) uprawnionej(ych):	Miejscowość i data: