



SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

dla postępowania prowadzonego w trybie przetargu nieograniczonego

dla zamówienia o szacunkowej wartości powyżej progów unijnych

na

„Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA”

nr PN-22/2021

wraz z informacją z art. 222 ust. 4 – kwota, jaką zamawiający zamierza przeznaczyć na sfinansowanie zamówienia.

SPIS TREŚCI

ROZDZIAŁ I –ZAMAWIAJĄCY	3
ROZDZIAŁ II – TRYB UDZIELENIA ZAMÓWIENIA	3
ROZDZIAŁ III – KRÓTKI OPIS PRZEDMIOTU ZAMÓWIENIA	3
ROZDZIAŁ IV – WSPÓLNY SŁOWNIK ZAMÓWIEŃ (CPV).....	4
ROZDZIAŁ V – TERMIN REALIZACJI ZAMÓWIENIA	4
ROZDZIAŁ VI – ZAMÓWIENIA CZĘŚCIOWE	4
ROZDZIAŁ VII – OFERTA WARIANTOWA.....	4
ROZDZIAŁ VIII – OFERTA WSPÓLNA	4
ROZDZIAŁ IX – INFORMACJE O PRZEPROWADZENIU AUKCJI ELEKTRONICZNEJ	4
ROZDZIAŁ X – ZAMÓWIENIA NA DODATKOWE DOSTAWY.....	4
ROZDZIAŁ XI – PODWYKONAWSTWO	5
ROZDZIAŁ XII – INFORMACJE O ZATRUDNIENIU NA PODSTAWIE UMOWY O PRACĘ.....	5
ROZDZIAŁ XIII – INFORMACJE O FINANSOWANIU ZAMÓWIENIA	5
ROZDZIAŁ XIV – PODSTAWY WYKLUCZENIA ORAZ WARUNKI UDZIAŁU W POSTĘPOWANIU	5
ROZDZIAŁ XV – OŚWIADCZENIA, DOKUMENTY ORAZ SPOSÓB ICH ZŁOŻENIA, W TYM INFORMACJA O PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH, ORAZ WYKAZ PODMIOTOWYCH ŚRODKÓW DOWODOWYCH	9
ROZDZIAŁ XVI – WADIUM.....	13
ROZDZIAŁ XVII	13
I. OPIS SPOSOBU PRZYGOTOWANIA OFERT ORAZ WYMAGANIA FORMALNE DOTYCZĄCE SKŁADANYCH OŚWIADCZEŃ I DOKUMENTÓW	13
II. INFORMACJA O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ.....	16
ROZDZIAŁ XVIII – TERMIN ZWIĄZANIA OFERTĄ	17
ROZDZIAŁ XIX	17
I. MIEJSCE I TERMIN SKŁADANIA OFERT	17
II. MIEJSCE ORAZ TERMIN OTWARCIA OFERT	18
ROZDZIAŁ XX – OPIS SPOSOBU OBLICZENIA CENY OFERTY	18
ROZDZIAŁ XXI –OPIS KRYTERIÓW Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT	19
WAGA KRYTERIUM	19
ROZDZIAŁ XXII – INFORMACJE O FORMALNOŚCIACH JAKICH NALEŻY DOPEŁNIĆ PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY	21
ROZDZIAŁ XXIII –ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY	21
ROZDZIAŁ XXIV – POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ	22
ROZDZIAŁ XXV – KLAUZULA INFORMACYJNA	22
ROZDZIAŁ XXVI – ZAŁĄCZNIKI	24

Rozdział I –Zamawiający

Kancelaria Prezesa Rady Ministrów

Aleje Ujazdowskie 1/3, 00-583 Warszawa

NIP 526-16-45-000

Strona internetowa zamawiającego, na której prowadzone jest postępowanie, i na której udostępniane będą zmiany i wyjaśnienia treści Specyfikacji Warunków Zamówienia (dalej: SWZ) oraz inne dokumenty bezpośrednio związane z postępowaniem o udzielenie zamówienia: <https://www.gov.pl/web/premier/postepowania-wszczete2>

Ofertę należy złożyć za pomocą Miniportalu: <https://miniportal.uzp.gov.pl/>

e-mail: wzp@mc.gov.pl

Rozdział II – Tryb udzielenia zamówienia

1. Postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 132 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.) (dalej: ustawa pzp).
2. Zamawiający zgodnie z art. 139 ust. 1 ustawy pzp najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej wykonawcy, którego oferta została najwyżej oceniona, w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.
3. Postępowanie prowadzone jest w języku polskim.

Rozdział III – Krótki opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa oprogramowania systemowego wraz z licencjami niezbędnymi do zapewnienia środowiska ZPA, w tym środowisk badawczych, części centralnej ZPA realizowanych w rozwiązaniu Zintegrowana Platforma Analityczna wraz z usługami wsparcia technicznego. Licencje będą wdrożone przez Partnera projektu.
Zakres przedmiotu zamówienia obejmuje:
 - a) dostawę przedmiotu zamówienia w terminie wskazanym w formularzu ofertowym,
 - b) udzielenie gwarancji jakości na dostarczony przedmiot umowy na okres 12 miesięcy,
 - c) zapewnienie wsparcia technicznego.
2. Zamówienie jest podzielone na 5 części:
 - część 1: Dostawa oprogramowania wraz z licencjami na systemy operacyjne:
 - a) Systemu operacyjnego typu *desktop* (instalowanych na stacjach roboczych) w ilości 50 szt.;
 - b) Licencje dla usług terminalowych w ilości 90 szt.,
 - c) Licencje do usług serwerowych w ilości 150 szt..
 - część 2: Dostawa oprogramowania wraz z licencjami UTM:
 - a) Oprogramowanie UTM w ilości 1 szt.;
 - b) Oprogramowanie do składowania i analizy logów systemu UTM w ilości 1 szt.
 - część 3: Dostawa oprogramowania wraz z licencjami kluczy szyfrujących:
 - a) Oprogramowanie do zarządzania kluczami szyfrującymi w ilości 2 szt.;
 - b) Oprogramowanie do realizacji operacji pseudonimizacji w ilości 2 szt.
 - część 4: Dostawa oprogramowania wraz z licencjami na narzędzia programistyczne:
 - a) Oprogramowanie wspomagające tworzenie Bazy Wiedzy w ilości 1 szt.;
 - b) Oprogramowanie do repozytorium kodu źródłowego w ilości 1 szt.

- część 5: Dostawa licencji oprogramowania do monitorowania użytkowników, infrastruktury i obsługi haseł:
 - a) Serwer monitorowania sesji zdalnych i wsparcia zdalnego dla użytkowników w ilości 1 szt.;
 - b) System do samodzielnej obsługi haseł w ilości 1 szt.;
 - c) Serwer monitorowania SLA w ilości 1 szt.
- 3. Opis przedmiotu zamówienia (dalej: opis przedmiotu zamówienia, szczegółowy opis przedmiotu zamówienia, OPZ lub SOPZ) stanowi Załącznik nr 1 do SWZ, a zamówienie będzie realizowane na warunkach określonych w Projektowanych postanowieniach umowy, stanowiących Załącznik nr 2 do SWZ.
- 4. Postępowanie oznaczone jest nr PN-22/2021.

Rozdział IV – Wspólny słownik zamówień (CPV)

CPV: 48000000-8 - Pakiety oprogramowania i systemy informatyczne;
72611000-6 - Usługi w zakresie wsparcia technicznego .

Rozdział V – Termin realizacji zamówienia

Zamówienie będzie realizowane przez okres 36 miesięcy od dnia zawarcia umowy, w tym dostawa przedmiotu zamówienia wyniesie maksymalnie 8 dni roboczych od dnia podpisania umowy.

Rozdział VI – Zamówienia częściowe

Zamawiający dopuszcza możliwości składania ofert na 1 lub więcej części.

Rozdział VII – Oferta wariantowa

Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

Rozdział VIII – Oferta wspólna

Zamawiający dopuszcza możliwość wspólnego ubiegania się o przedmiotowe zamówienie.

Rozdział IX – Informacje o przeprowadzeniu aukcji elektronicznej

Zamawiający nie zamierza dokonać wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

Rozdział X – Zamówienia na dodatkowe dostawy

Zamawiający przewiduje możliwość udzielenia zamówień, o których mowa art. 214 ust. 1 pkt 8 ustawy pzp.

Zamówienia polegające na dodatkowych dostawach w wysokości do:

1. 10% wartości zamówienia dla części 1,
2. 10% wartości zamówienia dla części 2,
3. 10% wartości zamówienia dla części 3,
4. 10% wartości zamówienia dla części 4,
5. 10% wartości zamówienia dla części 5,

Dodatkowe dostawy będą odzwierciedlać przedmiot zamówienia podstawowego w danej części i nie przekroczą wartości podanych powyżej.

Zamówienia te zostaną udzielone na podstawie odrębnej umowy.

Zarówno Zamawiającemu, jak i Wykonawcy nie przysługuje roszczenie o zawarcie umowy na ww. usługi, jest to jedynie prawna możliwość zawarcia umowy z dotychczasowym Wykonawcą w toku odrębnego postępowania.

Rozdział XI – Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.
2. Zamawiający oczekuje wskazania przez wykonawcę w ofercie, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom wraz z podaniem nazw ewentualnych podwykonawców, jeżeli są już znani.

Rozdział XII – Informacje o zatrudnieniu na podstawie umowy o pracę

Zamawiający nie przewiduje konieczności zatrudnienia na podstawie umowy o pracę osób realizujących przedmiotowe zamówienie.

Rozdział XIII – Informacje o finansowaniu zamówienia

1. Kwota, jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia w:
 - część 1: Dostawa oprogramowania wraz z licencjami na systemy operacyjne, to 150.225,64 zł brutto,
 - część 2: Dostawa oprogramowania wraz z licencjami UTM, to 110.511,81zł brutto,
 - część 3: Dostawa oprogramowania wraz z licencjami kluczy szyfrujących, to 1.185.586,21 zł brutto,
 - część 4: Dostawa oprogramowania wraz z licencjami na narzędzia programistyczne, to 918.412,34 zł brutto,
 - część 5: Dostawa licencji oprogramowania do monitorowania użytkowników, infrastruktury i obsługi haseł, to 320.500,59 zł brutto.
2. Zamówienie finansowane jest ze środków Unii Europejskiej w ramach Projektu „Zintegrowania Platforma Analityczna” realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa nr 2 „E-administracja i otwarty rząd” Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej”.
Zamawiający przewiduje, iż może unieważnić postępowanie o udzielenie zamówienia, jeżeli środki, które zamierza przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostaną mu przyznane.
3. Wszystkie rozliczenia pomiędzy Zamawiającym a wykonawcą będą podlegały regułom dotyczącym wydatkowania i kwalifikowalności wydatków środków w ramach Programu Operacyjnego Polska Cyfrowa.

Rozdział XIV – Podstawy wykluczenia oraz warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

- a) nie podlegają wykluczeniu;
 - b) spełniają warunki udziału w postępowaniu, o ile zostały one określone przez zamawiającego.
1. Z postępowania o udzielenie zamówienia zamawiający wykluczy wykonawcę :
 - 1.1. w oparciu o obligatoryjne podstawy wykluczenia określone w art. 108 ust. 1 ustawy pzp, z zastrzeżeniem art. 110 ust. 2 ustawy pzp;

- 1.2. w oparciu o fakultatywne podstawy wykluczenia określone w art. 109 ust. 1 pkt 4 ustawy pzp:
 - w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
2. Wykonawca może zostać wykluczony przez zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
3. Zgodnie z art. 112 ust. 2 ustawy pzp, o udzielenie Zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki dotyczące:
 - 3.1 zdolności do występowania w obrocie gospodarczym:

Zamawiający nie wskazuje warunku.
 - 3.2 uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:

Zamawiający nie wskazuje warunku.
 - 3.3 sytuacji ekonomicznej lub finansowej:

Zamawiający nie wskazuje warunku.
 - 3.4 zdolności technicznej i zawodowej:

Zamawiający uzna warunek za spełniony, jeżeli wykonawca wykaże się:

 - **w zakresie części 1: Dostawa oprogramowania wraz z licencjami na systemy operacyjne,**

należytym wykonaniem, a w przypadku świadczeń okresowych lub ciągłych również wykonywaniem, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **co najmniej 2 dostaw, polegających na dostawie oprogramowania wraz z licencjami systemów operacyjnych, o wartości co najmniej 40 000,00 zł brutto każda.** W przypadku wykazania się przez Wykonawcę doświadczeniem w zakresie dostawy wykonywanej (będącej w trakcie realizacji), Zamawiający uzna warunek za spełniony, jeżeli do upływu terminu składania ofert dostawa została wykonana należycie na kwotę co najmniej 40 000,00 zł brutto każda,
 - **w zakresie części 2: Dostawa oprogramowania wraz z licencjami UTM,**

należytym wykonaniem, a w przypadku świadczeń okresowych lub ciągłych również wykonywaniem, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **co najmniej 2 dostaw, polegających na dostawie oprogramowania wraz z licencjami UTM, o wartości co najmniej 30 000,00 zł brutto każda.** W przypadku wykazania się przez Wykonawcę doświadczeniem w zakresie dostawy wykonywanej (będącej w trakcie realizacji), Zamawiający uzna warunek za spełniony, jeżeli do upływu terminu składania ofert dostawa została wykonana należycie na kwotę co najmniej 30 000,00 zł brutto każda,
 - **w zakresie części 3: Dostawa oprogramowania wraz z licencjami kluczy szyfrujących,**

należytych wykonaniem, a w przypadku świadczeń okresowych lub ciągłych również wykonywaniem, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **co najmniej 2 dostaw, polegających na dostawie oprogramowania wraz z licencjami kluczy szyfrujących, o wartości co najmniej 240 000,00 zł brutto każda**. W przypadku wykazania się przez Wykonawcę doświadczeniem w zakresie dostawy wykonywanej (będącej w trakcie realizacji), Zamawiający uzna warunek za spełniony, jeżeli do upływu terminu składania ofert dostawa została wykonana należycie na kwotę co najmniej 240 000,00 zł brutto każda,

- **w zakresie części 4: Dostawa oprogramowania wraz z licencjami na narzędzia programistyczne,**

należytych wykonaniem, a w przypadku świadczeń okresowych lub ciągłych również wykonywaniem, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **co najmniej 2 dostaw, polegających na dostawie oprogramowania wraz z licencjami narzędzi programistycznych, o wartości co najmniej 180 000,00 zł brutto każda**. W przypadku wykazania się przez Wykonawcę doświadczeniem w zakresie dostawy wykonywanej (będącej w trakcie realizacji), Zamawiający uzna warunek za spełniony, jeżeli do upływu terminu składania ofert dostawa została wykonana należycie na kwotę co najmniej 180 000,00 zł brutto każda,

- **w zakresie części 5: Dostawa licencji oprogramowania do monitorowania użytkowników, infrastruktury i obsługi haseł.**

należytych wykonaniem, a w przypadku świadczeń okresowych lub ciągłych również wykonywaniem, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **co najmniej 2 dostaw, polegających na dostawie oprogramowania wraz z licencjami do monitorowania użytkowników, infrastruktury i obsługi haseł, o wartości co najmniej 70 000,00 zł brutto każda**. W przypadku wykazania się przez Wykonawcę doświadczeniem w zakresie dostawy wykonywanej (będącej w trakcie realizacji), Zamawiający uzna warunek za spełniony, jeżeli do upływu terminu składania ofert dostawa została wykonana należycie na kwotę co najmniej 70 000,00 zł brutto każda.

5. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu lub kryteriów selekcji, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
6. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.

7. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 8, potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa, w szczególności:
 - 7.1 zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
 - 7.2 sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
 - 7.3 czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy, których wskazane zdolności dotyczą.
8. Wzór zobowiązania podmiotu udostępniającego zasoby stanowi Załącznik nr 4 do SWZ.
9. Zamawiający oceni, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt 4 ustawy pzp, oraz, jeżeli to dotyczy, kryteriów selekcji, a także zbada, czy nie zachodzą wobec tego podmiotu podstawy Wykluczenia, które zostały przewidziane względem wykonawcy. W tym celu wykonawca:
 - 9.1 składa wraz z ofertą zobowiązanie innego podmiotu do udostępnienia niezbędnych zasobów wykonawcy - zgodnie z Załącznikiem nr 4 do SWZ;
 - 9.2 składa wraz z ofertą Jednolity Europejski Dokument Zamówienia (JEDZ) dotyczący tych podmiotów, w zakresie wskazanym w Części II Sekcji C JEDZ (Informacje na temat polegania na zdolności innych podmiotów);
 - 9.3 w terminie określonym w Rozdziale VII na wezwanie zamawiającego, przedkłada w odniesieniu do tych podmiotów oświadczenia i dokumenty tam wskazane.
10. Jeżeli zdolności techniczne lub zawodowe, podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, zamawiający żąda, aby wykonawca w terminie określonym przez zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
11. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał w danym zakresie na zdolnościach podmiotów udostępniających zasoby.
12. Ocena spełniania wymaganych przez zamawiającego warunków w zakresie braku podstaw wykluczenia będzie oparta na zasadzie spełnia/nie spełnia, na podstawie określonych w Rozdziale XIV SWZ oświadczeń i dokumentów.
13. Zamawiający wymaga, aby przedmiot zamówienia był świadczony przez Wykonawcę, który posiada uprawnienia do sprzedaży zaoferowanych produktów, tj. autoryzację producenta do sprzedaży licencji producenta klientom sektora publicznego.

Za klientów sektora publicznego Zamawiający uznaje podmioty nie działające w celu generowania zysków, który należy do jednej z poniższych kategorii:

- a) Ponadnarodowe wszystkie organizacje/instytucje, które pełnią dostrzegalną rolę regulacyjną lub legislacyjną dla wielu rządów narodowych;
- b) Krajowe i wszystkie organizacje/instytucje rządowe lub pokrewne, które są zarządzane na poziomie krajowym lub pokrewnym i mają kompetencje do rządzenia na poziomie całego kraju lub państwa. Kategoria ta obejmuje ciała

- parlamentarne i organy sądownictwa upoważnione do ustalania lub decydowania o zasadach prawa;
- c) Regionalne, rozumiane jako pośredni poziom w strukturze rządzenia, który nie obejmuje całego kraju, lecz składa się z wielu obszarów władz lokalnych działających w obrębie swojej jurysdykcji do rządzenia. Kategoria ta obejmuje wszystkie organizacje/instytucje państwowe, które są zarządzane na poziomie regionalnym i noszą różne nazwy: Regiony, Départements, Stany, Lander, Hrabstwa (Okręgi), Województwa.
 - d) Lokalne najniższy poziom samorządów wybieralnych oraz powiązanych jednostek administracji. Kategoria ta obejmuje wszystkie organizacje/instytucje państwowe, które są zarządzane na poziomie miasta i gminy;
 - e) Każda organizacja, która odpowiada w szczególności wobec i podlega ostatecznej kontroli uznanego Rządu Państwowego (w praktyce dla wszystkich Rządów demokratycznych oznacza to podleganie jurysdykcji wybieralnego Ministra).

W przypadku podmiotów, które wprowadzie generują zyski, lecz pod innymi względami podpadają pod jedną z powyższych kategorii, stosowane są następujące dodatkowe kryteria:

- a) Czy całość przychodów przypada państwu? (czy część jest pobierana także przez prywatnych udziałowców?)
- b) Czy dany podmiot jest zwolniony z podatku dochodowego od osób prawnych?
- c) Czy podmiot jest przynajmniej w 50% finansowany przez państwo? (tzn. czy z działalności komercyjnej pochodzi mniej niż 50% jego budżetu?)
- d) W jaki sposób uregulowane są kwestie celów/statusu/charakteru podmiotu w jego statucie/celach?

Jeżeli odpowiedź na wszystkie pierwsze trzy pytania brzmi „tak”, to dany podmiot jest uprawniony do korzystania z cen dla sektora publicznego. Niezależnie od powyższego, jeżeli Rząd danego kraju publikuje definicję lub listę podmiotów określającą, jakie podmioty uważane są za upoważnione podmioty sektora publicznego, to wówczas taka definicja lub lista ma pierwszeństwo przed powyższą definicją.

Rozdział XV – Oświadczenia, dokumenty oraz sposób ich złożenia, w tym informacja o przedmiotowych środkach dowodowych, oraz wykaz podmiotowych środków dowodowych

1. W zakresie nieuregulowanym ustawą pzp lub niniejszą SWZ do oświadczeń i dokumentów składanych przez wykonawcę w postępowaniu, zastosowanie mają:
 - 1.1 przepisy rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 r. poz. 2415);
 - 1.2 przepisy rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w

postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz.U. z 2020 r. poz. 2452).

2. **Każdy z wykonawców zobowiązany jest złożyć wraz z ofertą:**

2.1 **wypełniony Formularz oferty** podpisany kwalifikowanym podpisem elektronicznym, zawierający wszelkie informacje zawarte we wzorze stanowiącym załącznik nr 3 do SWZ;

2.2 **oświadczenie o spełnianiu warunków udziału w postępowaniu i braku podstaw do wykluczenia w formie jednolitego europejskiego dokumentu zamówienia (JEDZ)** - sporządzone według wzoru stanowiącego załącznik nr 9 do SWZ i podpisane kwalifikowanym podpisem elektronicznym; W przypadku wykonawców występujących wspólnie oświadczenie JEDZ składa każdy z wykonawców w zakresie w jakim wykazuje spełnienie warunków udziału w postępowaniu i brak podstaw wykluczenia;

2.3 **dokument potwierdzający wniesienie wadium;**

2.4 oraz - jeżeli dotyczy:

- a) **Pełnomocnictwo** upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik (w oryginale tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub elektronicznej kopii opatrzonej kwalifikowanym podpisem elektronicznym przez mocodawcę lub notariusza);
- b) **Pełnomocnictwo** do reprezentowania wszystkich wykonawców wspólnie ubiegających się o udzielenie zamówienia (w oryginale tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub elektronicznej kopii opatrzonej kwalifikowanym podpisem elektronicznym przez mocodawcę lub notariusza);
- c) **Oświadczenie** podmiotu udostępniającego zasoby dotyczące udostępnienia zasobów
- d) **Oświadczenie podmiotu udostępniającego zasoby** w formie jednolitego europejskiego dokumentu zamówienia (**JEDZ**) w zakresie w jakim wykazuje spełnienie warunków udziału w postępowaniu i brak podstaw do wykluczenia.

3. Jednolity Europejski Dokument Zamówienia (JEDZ), stanowi Załącznik nr 2 do Rozporządzenia Wykonawczego Komisji (EU) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającego standardowy formularz jednolitego europejskiego dokumentu zamówienia. Informacje zawarte w JEDZ stanowią wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

4. Zamawiający informuje, że instrukcję wypełnienia ESPD oraz edytowalną wersję formularza JEDZ można znaleźć pod adresem: <https://www.uzp.gov.pl/baza-wiedzy/prawo-zamowien-publicznych-regulacje/prawo-krajowe/jednolity-europejski-dokument-zamowienia>. Zamawiający zaleca wypełnienie JEDZ za pomocą serwisu dostępnego pod adresem: <https://espd.uzp.gov.pl/>.

W tym celu przygotowany przez zamawiającego Jednolity Europejski Dokument Zamówienia (ESPD) w formacie *.xml, stanowiący Załącznik nr 9 do SWZ, należy zaimportować do wyżej wymienionego serwisu oraz postępując zgodnie z zamieszczoną tam instrukcją wypełnić wzór elektronicznego formularza JEDZ, z zastrzeżeniem poniższych uwag:

- 4.1 w Części II Sekcji D JEDZ (Informacje dotyczące podwykonawców, na których zdolności wykonawca nie polega) wykonawca oświadcza czy zamierza zlecić osobom trzecim podwykonawstwo jakiegokolwiek części zamówienia (w przypadku twierdzącej odpowiedzi podaje ponadto, o ile jest to wiadome, wykaz proponowanych podwykonawców), natomiast wykonawca nie jest zobowiązany do przedstawienia w odniesieniu do tych podwykonawców odrębnych JEDZ;
- 4.2 w Części IV zamawiający żąda jedynie ogólnego oświadczenia dotyczącego wszystkich kryteriów kwalifikacji (**sekcja α**), bez wypełniania poszczególnych Sekcji A, B, C i D;
- 4.3 Część V (Ograniczenie liczby kwalifikujących się kandydatów) należy pozostawić niewypełnioną.
- 5 Zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni, aktualnych na dzień złożenia następujących podmiotowych środków dowodowych:
- 5.1 wykazu zrealizowanych dostaw, o których mowa w Rozdziale XIV, pkt. 3 ppkt 3.4 niniejszego SWZ, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane. Wzór wykazu stanowi Załącznik nr 7 do SWZ;
- 5.2 dowodów (np. referencji) określających, że dostawy, o których mowa w Rozdziale XIV, pkt. 3 ppkt 3.4 niniejszego SWZ zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy wykonanych dostaw;
- 5.3 oświadczenia wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy pzp, o braku przynależności do tej samej grupy kapitałowej w rozumieniu Ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów. Wzór oświadczenia stanowi Załącznik nr 6 do SWZ;
- 5.4 informacji z Krajowego Rejestru Karnego sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem w zakresie:
- a) art. 108 ust. 1 pkt 1 i 2 ustawy pzp;
- b) art. 108 ust. 1 pkt 4 ustawy pzp;
- 5.5 oświadczenia wykonawcy o aktualności informacji, o którym mowa w art. 125 ust. 1 ustawy pzp, w zakresie o których mowa w:
- a) art. 108 ust. 1 pkt 3 ustawy pzp;
- b) art. 108 ust. 1 pkt 4 ustawy pzp;
- c) art. 108 ust. 1 pkt 5 ustawy pzp;
- d) art. 108 ust. 1 pkt 6 ustawy pzp.
- Wzór oświadczenia stanowi Załącznik nr 5 do SWZ;

- 5.6 odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy pzp, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
6. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast:
- 1) informacji z Krajowego Rejestru Karnego, o której mowa w pkt 5.4 – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w pkt 5.4
 - 2) odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w pkt 5.6 – składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
 - 3) dokument, o którym mowa w pkt. 6 tier 1), powinien być wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem. Dokumenty, o których mowa w pkt 6 tier 2) powinny być wystawione nie wcześniej niż 3 miesiące przed ich złożeniem;
 - 4) Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w 6 tier 1) i 2), lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy. Przepis pkt 6 tier 3) stosuje się.
7. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1, dane umożliwiające dostęp do tych środków.
8. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jedynie jeżeli wykonawca wskaże oraz potwierdzi prawidłowość i aktualność podmiotowych środków dowodowych.
8. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, zamawiający może na każdym etapie postępowania wezwać wykonawcę lub wszystkich wykonawców, do złożenia wszystkich, lub niektórych podmiotowych środków dowodowych aktualnych na dzień ich złożenia.

9. Zamawiający oczekuje aby każdy przedstawiony dokument w języku innym niż polski był przedstawiony wraz z tłumaczeniem przysięgłym na język polski.

Rozdział XVI – Wadium

2. Wykonawca przed upływem terminu składania ofert zobowiązany jest wnieść wadium w wysokości:
- a) dla części 1: 3.000,00 zł (trzy tysiące złotych i 00/100),
 - b) dla części 2: 2.000,00 zł (dwa tysiące złotych i 00/100),
 - c) dla części 3: 20.000,00 (dwadzieścia tysięcy złotych i 00/100),
 - d) dla części 4: 20.000,00 (dwadzieścia tysięcy złotych i 00/100),
 - e) dla części 5: 7.000,00 (siedem tysięcy złotych i 00/100)
2. Wadium może być wnoszone w formach wskazanych w art. 97 ust. 7 ustawy Pzp.
3. Wadium wnoszone w pieniądzu należy wpłacić na rachunek bankowy Kancelarii Prezesa Rady Ministrów nr **81 1010 1010 0034 9213 9120 0000**, z adnotacją: „Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA” nr PN-22/2021- Wadium, część nr (**podać numer części której dotyczy wadium**).
4. W przypadku wniesienia wadium w pieniądzu, za moment wniesienia uznaje się moment uznania rachunku zamawiającego. W przypadku wniesienia wadium przelewem zaleca się, aby wykonawca załączył do oferty potwierdzenie dokonania przelewu.
5. Jeżeli wadium jest wnoszone w formie gwarancji lub poręczenia, wykonawca przekazuje zamawiającemu wraz z ofertą oryginał gwarancji lub poręczenia, w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym przez wystawcę poręczenia lub gwarancji w formacie umożliwiającym odczyt dokumentu.
6. Wadium powinno zostać przekazane zamawiającemu drogą komunikacji elektronicznej za pośrednictwem ePuap przy użyciu systemu miniPortal, przed upływem terminu składania ofert (tj. przed upływem dnia i godziny wyznaczonej jako ostateczny termin składania ofert). Zamawiający zaleca aby wadium zostało złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik wadium” a następnie, wraz z plikami stanowiącymi część oferty, skompresowane do jednego pliku archiwum (ZIP). Jeżeli wykonawca przesyła wadium poza ofertą, np. mailem, powinno ono być oznaczone w sposób umożliwiający jednoznaczne przypisanie go do konkretnego postępowania.
7. Dokument poręczenia lub gwarancji powinien zawierać informację o udzieleniu poręczenia lub gwarancji na rzecz zamawiającego tytułem zapłaty wadium w postępowaniu o udzielenie zamówienia na „Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA” nr PN-22/2021. Dokument poręczenia/gwarancji powinien być ważny przez okres związania ofertą oraz stanowić zobowiązanie poręczyciela lub gwaranta do nieodwołalnej, bezwarunkowej, płatnej na pierwsze żądanie zamawiającego wypłaty wadium w przypadkach określonych w art. 98 ust. 6 Pzp.
8. Zwrot albo zatrzymanie wadium nastąpi zgodnie z art. 98 Pzp.

Rozdział XVII

I. Opis sposobu przygotowania ofert oraz wymagania formalne dotyczące składanych oświadczeń i dokumentów

1. Wykonawca składa ofertę za pośrednictwem *Formularza do złożenia, zmiany, wycofania oferty lub wniosku* dostępnego na ePUAP i udostępnionego również na miniPortalu. Formularz do zaszyfrowania oferty przez wykonawcę jest dostępny dla wykonawców na miniPortal, w szczegółach danego postępowania. W formularzu oferty wykonawca zobowiązany jest podać adres poczty elektronicznej oraz skrzynki ePUAP, przy pomocy których prowadzona będzie korespondencja związana z postępowaniem.
2. Ofertę należy sporządzić zgodnie z wymogami zawartymi w niniejszej SWZ, w języku polskim, w postaci elektronicznej w następujących formatach danych: .txt, .rtf, .pdf, .doc, .docx, .odt
Oferta musi być podpisana – pod rygorem nieważności - kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnione do reprezentacji wykonawcy. Sposób złożenia oferty, w tym zaszyfrowania oferty opisany został w Regulaminie korzystania z miniPortalu i Instrukcji użytkownika systemu miniPortal-ePUAP. Ofertę należy złożyć w oryginale.
3. Zamawiający zaleca składanie podpisów elektronicznych dla dokumentów .pdf w formacie PAdES, a innych niż .pdf w formacie XAdES. Zamawiający dopuszcza formaty archiwów .zip, .7z, .rar i inne, pod warunkiem możliwości ich otwarcia programem 7-Zip.
4. Do oferty należy dołączyć Jednolity Europejski Dokument Zamówienia (JEDZ) w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę. Sposób zaszyfrowania oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
5. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa” a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. W odniesieniu do każdej z zastrzeżonych informacji wykonawca jest zobowiązany wykazać, że:
 - informacja ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub inny posiadający wartość gospodarczą,
 - informacja jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie jest powszechnie znana osobom zwykle zajmującym się tym rodzajem informacji albo nie jest łatwo dostępna dla takich osób,
 - jest uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.Zamawiający oceni, czy zastrzeżone przez wykonawcę informacje stanowią tajemnicę przedsiębiorstwa (w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, lub są jawne na podstawie przepisów ustawy pzp lub odrębnych przepisów) w oparciu o konkretny stan faktyczny.
6. Zamawiający informuje, że badając zasadność zastrzeżenia konkretnej informacji nie będzie brał pod uwagę cytowanych przez wykonawcę ogólnych wyroków czy dowodzenia, że niezbędnym działaniem podjętym w celu nieujawnienia informacji do wiadomości publicznej jest fakt, że wykonawca zastrzegł ją w ofercie.
7. Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem formularza do złożenia, zmiany, wycofania oferty lub wniosku

- dostępnego na ePUAP i udostępnionych również na miniPortal. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortal.
8. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
 9. Wykonawca może złożyć tylko jedną ofertę. Treść oferty musi odpowiadać treści SWZ.
 10. Formularz Oferty oraz oświadczenie JEDZ muszą być złożone w oryginale.
 11. Zamawiający zaleca ponumerowanie stron oferty.
 12. Jeżeli wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
 13. Postanowień ust. 12 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
 14. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym wykonawca przekazuje wraz z tłumaczeniem na język polski.
 15. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy pzp lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej "dokumentami potwierdzającymi umocowanie do reprezentowania", zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej "upoważnionymi podmiotami", jako dokument elektroniczny, przekazuje się ten dokument.
 16. W przypadku gdy dokumenty, o których mowa w pkt. 15, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu (elektroniczna kopia dokumentu) opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
 17. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 16, może dokonać notariusz lub w przypadku: podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania - odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
 - 17.2. przedmiotowych środków dowodowych - odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;
 - 17.3. innych dokumentów, odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które go dotyczą.
 18. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe niewystawione przez upoważnione podmioty, oraz pełnomocnictwo

- przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.
19. W przypadku gdy dokumenty, o których mowa w pkt 18, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym.
20. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 19, może dokonać notariusz lub w przypadku:
- 20.1. podmiotowych środków dowodowych - odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
- 20.2. przedmiotowego środka dowodowego, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy pzp, lub zobowiązania podmiotu udostępniającego zasoby - odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;
- 20.3. pełnomocnictwa – mocodawca.
- II. Informacja o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej**
1. Komunikacja między zamawiającym a wykonawcami w szczególności składanie oświadczeń, wniosków, zawiadomień, (w tym przekazywanie dokumentów składanych na żądanie zamawiającego) oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem dedykowanego formularza dostępnego na Elektronicznej Platformie Usług Administracji Publicznej (ePUAP) oraz udostępnionego przez miniPortal -
Formularz do komunikacji:
<https://miniportal.uzp.gov.pl>
<https://epuap.gov.pl/wps/portal>
lub poczty elektronicznej na adres: wzp@mc.gov.pl.
Korespondencja przesyłana za pomocą Formularza do komunikacji nie może być szyfrowana.
2. Oferta wykonawcy wraz z załącznikami przekazywana jest **tylko przy użyciu ePUAPu** za pośrednictwem dedykowanego *Formularza do złożenia, zmiany, wycofania oferty lub wniosku*.
3. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.
4. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP
<https://miniportal.uzp.gov.pl/WarunkiUslugi>
https://miniportal.uzp.gov.pl/Instrukcja_uzytkownika_miniPortal-ePUAP.pdf
<https://epuap.gov.pl/wps/portal/strefa-klienta/regulamin>

- Wykonawca zainteresowany złożeniem oferty, winien zapoznać się z aktualnymi wytycznymi technicznymi zawartymi w ww. regulaminach.
5. Wykonawca składając ofertę oświadcza, że zapoznał się z instrukcją użytkownika systemu miniPortal-ePUAP i regulaminem korzystania z systemu miniPortal.
 6. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty lub wniosku oraz do komunikacji wynosi 150 MB.
 7. Oferty, oświadczenia, o których mowa w art. 125 ust. 1 ustawy pzp, podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust. 3 ustawy pzp, przedmiotowe środki dowodowe, pełnomocnictwo, sporządza się w postaci elektronicznej w formatach danych: .txt, .rtf, .pdf, .doc, .docx, .odt i przekazuje przy użyciu środków komunikacji elektronicznej określonych dla danych dokumentów odpowiednio w pkt 1 lub 2.
 8. Informacje, oświadczenia lub dokumenty, inne niż określone w pkt 7, przekazywane w postępowaniu, sporządza się w postaci elektronicznej, w formatach danych określonych w punkcie powyżej lub jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej, określonych w pkt 1.
 9. Do kontaktu z wykonawcami uprawnione są następujące osoby: Piotr Zduńczyk e-mail: wzp@mc.gov.pl, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, w godzinach: 08:15-16:15.

Rozdział XVIII – Termin związania ofertą

1. Wykonawca jest związany ofertą **do dnia 25.09.2021 r.** .Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, zamawiający przed upływem terminu związania ofertą zwróci się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 60 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

Rozdział XIX

I. Miejsce i termin składania ofert

1. Wykonawca składa ofertę za pośrednictwem Formularza do złożenia lub wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Formularz do zaszyfrowania oferty przez wykonawcę jest dostępny dla wykonawców na miniPortalu, w szczegółach danego postępowania.
2. Sposób złożenia oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
3. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie **do dnia 28.06.2021 r., do godz. 11:00**
4. Wykonawca może złożyć tylko jedną ofertę.

5. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
6. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem Formularza do wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.
7. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

II. Miejsce oraz termin otwarcia ofert

1. Otwarcie ofert nastąpi **w dniu 28.06.2021 r., o godzinie 11:30**
2. Otwarcie ofert jest niejawne.
3. Otwarcie ofert następuje przez użycie mechanizmu do odszyfrowania ofert dostępnego po zalogowaniu w zakładce Deszyfrowanie na miniPortalu i następuje przez wskazanie pliku do odszyfrowania.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
 - 4.1 nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
 - 4.2 cenach lub kosztach zawartych w ofertach.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

Rozdział XX – Opis sposobu obliczenia ceny oferty

1. Cena oferty jest ceną wynikającą z wypełnionego Formularza oferty, stanowiącego Załącznik nr 3 do SWZ.
2. Cena oferty musi być wyższa niż 0 zł, wyrażona w złotych polskich (PLN) cyfrowo i słownie, i określona z dokładnością do 1 grosza (tj. do dwóch miejsc po przecinku) w rozumieniu ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz. U. z 2017 r. poz. 1830 ze zm.).
3. Wykonawca określi cenę oferty z uwzględnieniem wszelkich kosztów niezbędnych do zrealizowania zamówienia wynikających wprost z SWZ, Opisu przedmiotu zamówienia oraz ujmie wszystkie inne koszty i składniki w nich niezawarte, a bez których nie można wykonać zamówienia.
4. Wykonawca jest zobowiązany do uzyskania wszelkich niezbędnych informacji, które są konieczne do prawidłowej wyceny przedmiotu zamówienia i zawarcia umowy, gdyż wyklucza się możliwość roszczeń wykonawcy związanych z błędnym skalkulowaniem ceny lub pominięciem elementów niezbędnych do prawidłowego wykonania umowy.
5. Nie dopuszcza się wariantowości cen.
6. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług,

zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.

Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

7. Zamawiający jest podatnikiem zarejestrowanym jako czynny podatnik podatku od towarów i usług.
8. Cena oferty brutto obejmuje wynagrodzenie za przeniesienie majątkowych praw autorskich do utworów, które powstaną lub mogą powstać w ramach realizacji umowy, jeżeli w danym postępowaniu powstaną lub mogą powstać utwory w rozumieniu ustawy o prawach autorskich i prawach pokrewnych.
9. Cena ogółem brutto, określona przez wykonawcę w formularzu oferty, posłuży do rozliczenia wynagrodzenia, zgodnie z zapisami PPU.
10. Wykonawca zobowiązany jest do poinformowania zamawiającego, czy wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego, a jeśli tak, do:
 - 10.1 wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
 - 10.2 wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
 - 10.3 wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.
11. Jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego, dla celów zastosowania kryterium ceny zamawiający doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.
12. Zamawiający nie udziela zaliczek.

Rozdział XXI –Opis kryteriów z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty zamawiający będzie kierował się nw. kryteriami oceny, przypisując im odpowiednio wagi procentowe. Przyjmuje się, że 1% wagi kryterium = 1 punkt. Wszystkie obliczenia będą dokonywane z dokładnością do dwóch miejsc po przecinku, a zaokrąglenie zostanie dokonane zgodnie z ogólnie przyjętymi zasadami matematyki.
 - 1.1. Do oceny ofert w zakresie każdej z pięciu części, zamawiający przyjął kryteria określone w SWZ i Ogłoszeniu wraz ze wskazaniem jego znaczenia (wagą wyrażoną w % udziale w ocenie oferty). Szczegółowe zasady oceny ofert zostały przedstawione poniżej. Ocenie podlegają tylko oferty odpowiadające treści SWZ.

Nr.	Nazwa kryterium	Waga kryterium
1.	Cena brutto („C”)	60 %
2.	Czas dostawy („Cd”)	40 %

1.2. Kryterium: CENA (60% wagi oceny) (C)

Z tytułu niniejszego kryterium maksymalna liczba punktów wynosi 60. Ocenie w ramach kryterium w zakresie każdej z części podlega łączna cena za realizację przedmiotu zamówienia w danej części.

Oferta o najkorzystniejszej (najniższej) cenie w zakresie danej części uzyska 60 pkt.

Pozostałe ceny obliczone dla badanych ofert, zostaną porównane z ofertą o najkorzystniejszej (najniższej) cenie, stosując poniższy wzór:

$$C = C_n / C_m \times 60 \%$$

Gdzie:

m – oznacza kolejną badaną ofertę,

C – oznacza liczbę punktów przyznaną danej ofercie w kryterium cena,

C_n – oznacza oferowaną najniższą cenę oferty,

C_m – oznacza oferowaną cenę w badanej ofercie,

100 – wskaźnik stały,

60% - procentowe znaczenie kryterium ceny.

1.3. Czas dostawy „Cd” - (40 % wagi oceny)

Przez kryterium „czas dostawy” zamawiający rozumie czas dostawy oprogramowania od dnia podpisania umowy.

Zamawiający dokona oceny ofert w przedmiotowym postępowaniu na podstawie terminu dostawy określonego przez Wykonawców w *Formularzu ofertowym*.

W kryterium „czas dostawy” oferta może otrzymać maksymalnie 40 pkt. Punkty w przedmiotowym kryterium zostaną przyznane zgodnie z poniższą tabelą.

Czas dostawy oprogramowania od dnia podpisania umowy	Liczba punktów, którą może uzyskać Wykonawca
do 3 dni roboczych	40 pkt
4 do 5 dni roboczych	20 pkt
6 do 7 dni roboczych	10 pkt
8 dni roboczych	0 pkt

Jeżeli Wykonawca nie poda ilości dni, w trakcie których zobowiąże się do dostarczenia oprogramowania, Zamawiający uzna, iż jest to 8 dni roboczych i przyzna 0 pkt. w kryterium.

1.4. Ocena łączna

Dla każdej oferty wyniki oceny z tytułu kryteriów zostaną obliczone według poniższego wzoru:

$$S = C + Cd$$

Gdzie:

- S - wynik oceny (suma punktów),
C - liczba punktów uzyskanych w kryterium „Cena brutto”,
Cd - liczba punktów uzyskanych w kryterium „Czas dostawy”,
2. Za ocenioną, jako najkorzystniejszą, uznana zostanie oferta, która uzyska największą łączną liczbę punktów w kryteriach określonych powyżej.
 3. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
 4. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, zamawiający wybiera ofertę z najniższą ceną lub najniższym kosztem.
 5. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa w ust. 4, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych zawierających nową cenę lub koszt.

Rozdział XXII – Informacje o formalnościach jakich należy dopełnić po wyborze oferty w celu zawarcia umowy

1. Przed zawarciem umowy wykonawca będzie zobowiązany:
 - 1.1 podać zamawiającemu dane niezbędne do sporządzenia umowy, w tym kwoty netto oraz stawki podatku VAT, jeżeli będą wymagane. Kwoty podanego wynagrodzenia muszą odpowiadać kwotom podanym w ofercie lub wynikać z ewentualnych poprawek, o których mowa w art. 223 ust. 2 ustawy pzp;
 - 1.2 wnieść zabezpieczenie należytego wykonania umowy, w celu pokrycia roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
2. W przypadku wyboru oferty złożonej przez wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający zastrzega sobie prawo żądania, przed podpisaniem umowy w sprawie udzielenia zamówienia publicznego, umowy regulującej współpracę tych wykonawców, w tym również umowy spółki cywilnej.

Rozdział XXIII –Zabezpieczenie należytego wykonania umowy

1. Wykonawca przed zawarciem umowy wnieść zabezpieczenie należytego wykonania umowy w wysokości 5 % ceny całkowitej podanej w ofercie, w formie określonej w art. 450 ust. 1 ustawy pzp.
2. Zabezpieczenie należytego wykonania umowy, wniesione w pieniądzu, wykonawca wpłaci na rachunek zamawiającego: 10 1130 1062 0019 9404 5820 0005, w tytule przelewu wpisując: „**Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA – Zabezpieczenie dla części** (wpisać numer części, której dotyczy zabezpieczenie)”.
3. Zabezpieczenie należytego wykonania umowy wnoszone w formie poręczenia lub gwarancji powinno obejmować okres obowiązywania umowy oraz okres przewidziany na jego zwrot i zawierać zobowiązanie gwaranta/poręczyciela do nieodwołalnej, bezwarunkowej, płatnej na pierwsze żądanie wypłaty na rzecz zamawiającego kwoty zabezpieczenia, po otrzymaniu przez gwaranta/poręczyciela oświadczenia o niewykonaniu lub nienależytym wykonaniu przez wykonawcę zobowiązań wobec zamawiającego wynikających z zawartej umowy.

4. Zabezpieczenie należytego wykonania umowy zostanie zwrócone wykonawcy w terminie 30 dni od dnia wykonania zamówienia i uznania przez zamawiającego za należycie wykonane.

Rozdział XXIV – Pouczenie o środkach ochrony prawnej

1. Środki ochrony prawnej przysługują wykonawcy lub innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy pzp.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia w konkursie przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
 - 3.1. niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
 - 3.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo w postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Odwołanie wobec treści ogłoszenia lub treści dokumentów zamówienia wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej.
6. Odwołanie wnosi się w terminie:
 - 6.1 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej;
 - 6.2 15 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 6.1.
7. Odwołanie w przypadkach innych, niż określone w pkt 5 i 6, wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie, za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
9. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” ustawy pzp.

Rozdział XXV – Klauzula informacyjna

Klauzula informacyjna wynikająca z art. 13 rozporządzenie 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 uchylecia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
(Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”,**

Zgodnie z art. 13 ust. 1 - 3 ww. rozporządzenia informuję, że:

1. administratorem Pani/Pana danych osobowych jest Kancelaria Prezesa Rady Ministrów, Aleje Ujazdowskie 1/3, 00-583 Warszawa, adres e-mail: IOD@mc.gov.pl;
2. Dane kontaktowe do Inspektora Ochrony Danych: Inspektor Ochrony Danych, Minister Cyfryzacji, Aleje Ujazdowskie 1/3, e-mail: IOD@mc.gov.pl;
3. Pani lub Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego do którego odnosi się niniejszy dokument Specyfikacji Warunków Zamówienia oraz w celu wywiązania się z obowiązku prawnego ciążącego na Administratorze, wynikającego z przepisów o archiwizacji;
4. odbiorcami Pani lub Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy pzp oraz dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej, w szczególności do podmiotów prowadzących działalność kontrolną wobec KPRM;
5. Dane osobowe są przekazywane do podmiotów przetwarzających dane w imieniu administratora danych osobowych tj. Centrum Obsługi Administracji Rządowej, JSK Internet (BIP);
6. Pani lub Pana dane osobowe będą przechowywane, zgodnie z art. 98 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 oraz po jej zakończeniu zgodnie z przepisami dotyczącymi archiwizacji;
7. obowiązek podania przez Panią lub Pana danych osobowych bezpośrednio Pani lub 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 uPzp;
8. w odniesieniu do Pani lub Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
9. posiada Pani lub Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani lub Pana dotyczących,
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani lub Pana danych osobowych^[1],

[1] 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.

- c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO[2],
- d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani lub Pan, że przetwarzanie danych osobowych Pani lub Pana dotyczących narusza przepisy RODO;

10. nie przysługuje Pani lub Panu:

- a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
- b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
- c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani lub Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Rozdział XXVI – ZAŁĄCZNIKI

1. Opis przedmiotu zamówienia;
2. Projektowane postanowienia umowy;
3. Formularz oferty;
4. Oświadczenie o udostępnieniu potencjału;
5. Oświadczenie o aktualności danych zawartych w JEDZ
6. Oświadczenie o braku przynależności do grupy kapitałowej;
7. Wykaz zrealizowanych dostaw;
8. Oświadczenie o spełnieniu warunków udziału w postępowaniu i braku podstaw do wykluczenia z postępowania, w formie JEDZ.

[2] 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.

Załącznik nr 1 do SWZ - Opis przedmiotu zamówienia.**Załącznik nr 1 do SIWZ**

1. Przedmiotem zamówienia jest dostawa oprogramowania systemowego wraz z licencjami niezbędnymi do zapewnienia środowiska ZPA, w tym środowisk badawczych, części centralnej ZPA realizowanych w rozwiązaniu Zintegrowana Platforma Analityczna wraz z usługami wsparcia technicznego, świadczonego w okresie 24 miesięcy. Licencje będą wdrożone przez Partnera projektu.
2. Zakres przedmiotu zamówienia obejmuje:
 - a) dostawę przedmiotu umowy do siedziby Zamawiającego w terminie wskazanym w formularzu ofertowym,
 - b) udzielenie gwarancji jakości na dostarczony przedmiot umowy na okres 12 miesięcy,
 - c) zapewnienie wsparcia technicznego od dnia zawarcia umowy przez okres 24 miesięcy. Wsparcie techniczne rozumiane jest jako usługi w zakresie pomocy technicznej, aktualizacji oraz usuwania błędów w świadczonym oprogramowaniu.
3. Wszystkie elementy zamówienia muszą spełniać poniższe warunki licencyjne:
 - a) Licencje muszą pochodzić z oficjalnego kanału sprzedaży producenta oprogramowania.
 - b) Licencje muszą być objęte wsparciem technicznym producenta przez okres 24 miesięcy.
 - c) Licencje muszą umożliwiać wykonywanie kopii oprogramowania (nośników) na potrzeby świadczenia usług wsparcia oprogramowania.
 - d) Licencje muszą umożliwiać wykonywanie kopii zapasowych oprogramowania na zasadach określonych przez producenta oprogramowania.
 - e) Licencja musi umożliwiać dokonanie cesji na inny podmiot z sektora rządowego.
 - f) Nie dopuszcza się licencji pochodzących z rynku wtórnego.
 - g) Zapewniony komplet dokumentacji licencyjnej (warunki korzystania licencji w wersji elektronicznej, umowa licencyjna) warunki pomocy technicznej dostęp do portalu umożliwiającego pobieranie kluczy i nośników.
4. Wszystkie elementy przedmiotu umowy muszą spełniać poniższe warunki dotyczące wsparcia technicznego:
 - a) Oprogramowanie musi mieć realizowane wsparcie techniczne na standardowych warunkach producenta oprogramowania.
 - b) Oprogramowanie musi umożliwić bezpłatne korzystanie z wydanych przez producenta najnowszych wersji oprogramowania, aktualizacji oraz poprawek bezpieczeństwa przez okres 36 miesięcy.
 - c) Zakup oprogramowania musi dać dostęp do centrum pomocy technicznej 24x7 przez okres 36 miesięcy.
 - d) Zakup oprogramowania musi dać dostęp elektroniczny do baz wiedzy, dokumentacji, biuletynów i informacji na temat oprogramowania.
5. Przedmiot zamówienia został podzielony na 5 części:
 - a) Część 1: Dostawa oprogramowania wraz z licencjami na systemy operacyjne:
 - i. Systemu operacyjnego typu *desktop* (instalowanych na stacjach roboczych) w ilości 50 szt.;

- ii. Licencje dla usług terminalowych w ilości 90 szt.;
 - iii. Licencje do usług serwerowych w ilości 150 szt.
 - b) Część 2: Dostawa oprogramowania wraz z licencjami UTM:
 - i. Oprogramowanie UTM w ilości 1 szt.;
 - ii. Oprogramowanie do składowania i analizy logów systemu UTM w ilości 1 szt..
 - c) Część 3: Dostawa oprogramowania wraz z licencjami kluczy szyfrujących:
 - i. Oprogramowanie do zarządzania kluczami szyfrującymi w ilości 2 szt.;
 - ii. Oprogramowanie do realizacji operacji pseudonimizacji w ilości 2 szt.;
 - d) Część 4: Dostawa oprogramowania wraz z licencjami na narzędzia programistyczne:
 - i. Oprogramowanie wspomagające tworzenie Bazy Wiedzy w ilości 1 szt.;
 - ii. Oprogramowanie do śledzenia błędów oraz zarządzania projektem w ilości 1 szt.;
 - iii. Oprogramowanie do repozytorium kodu źródłowego w ilości 1 szt.;
 - e) Część 5: Dostawa licencji oprogramowania do monitorowania użytkowników, infrastruktury i obsługi haseł:
 - i. Serwer monitorowania sesji zdalnych i wsparcia zdalnego dla użytkowników w ilości 1 szt.;
 - ii. System do samodzielnej obsługi haseł w ilości 1 szt.;
 - iii. Serwer monitorowania SLA w ilości 1 szt.
6. ZPA jest Projektem realizowanym przez Kancelarię Prezesa Rady Ministrów (Lidera Projektu) wspólnie z Partnerami:
- 1) Ministerstwo Zdrowia;
 - 2) Ministerstwo Edukacji i Nauki;
 - 3) Ministerstwo Rodziny i Polityki Społecznej;
 - 4) Uniwersytet Warszawski;
 - 5) Szkoła Główna Handlowa w Warszawie;
 - 6) Sieć Badawcza Łukasiewicz – Instytut Technik Innowacyjnych EMAG.
7. ZPA będzie centralnym rozwiązaniem analitycznym, klasy Business Intelligence, operującym na danych będących w dyspozycji jednostek administracji publicznej, danych gromadzonych i tworzonych przez administrację publiczną oraz danych dostępnych z innych źródeł.
8. Głównym celem projektu jest podniesienie skuteczności działań administracji w wybranych obszarach problemów społecznych i gospodarczych, poprzez wsparcie procesów decyzyjnych za pomocą informacji analitycznej wysokiej jakości.
9. Projekt Zintegrowanej Platformy Analitycznej będzie realizował również poniżej wymienione cele szczegółowe:
- 1) Udostępnienie w jednym miejscu narzędzi analitycznych wspierających procesy decyzyjne w administracji publicznej.
 - 2) Opracowanie wzorców dostępu do danych oraz analiz dla kluczowych obszarów społecznych i gospodarczych.
 - 3) Stworzenie technicznych i organizacyjnych możliwości dialogu społecznego i współpracy środowisk naukowych w rozwoju analityki państwa i podnoszeniu efektywności rozwiązywania problemów społecznych.
 - 4) Usystematyzowanie metod technicznych i zasad dostępu do kluczowych zasobów informacyjnych państwa dla celów analitycznych, wraz z wdrożeniem spójnego

- systemu bezpieczeństwa, metod dostępu do danych, udostępniania do celów analitycznych.
- 5) Udostępnienie danych administracji publicznej do badań naukowych wspierających podejmowanie decyzji przez twórców polityk publicznych przy równoczesnym zapewnieniu właściwej ochrony dla przetwarzanych danych.
10. W ramach projektu ZPA poszczególne badania będą realizowane w ramach odseparowanych środowisk badawczych (sandbox'ów). Środowiska będą zapewniane w modelu wirtualnych stacji roboczych, a dostęp do nich będzie zapewniany przy pomocy mechanizmów zdalnego dostępu.
11. Wymagania funkcjonalne dla środowiska badawczego powodują, że będzie ono skonfigurowane w taki sposób, aby dostęp do Internetu był ograniczony. Należy mieć na uwadze to, że cecha ta może ograniczyć diagnostykę działania usług, w tym również usługi aktualizacji oprogramowania.
12. Tworzenie środowisk badawczych będzie się odbywać w sposób ustandaryzowany. W ramach powoływania środowiska badawczego jego użytkownicy będą mogli wnioskować o zapewnienie odpowiednich parametrów technicznych takich jak: maszyny wirtualne, przepustowość sieci, pamięć masowa i moc obliczeniowa oraz o zapewnienie odpowiednich narzędzi analitycznych (open source oraz płatnych), które umożliwią realizację zaplanowanych badań. Zamawiający planuje zapewnienie szerokiego zakresu narzędzi analitycznych, które umożliwią prowadzenie diagnoz w zakresie różnych problemów społecznych i ekonomicznych. W tym celu w ramach Platformy ZPA przewiduje się przeprowadzenie szeregu analiz na dużych zbiorach danych przy zastosowaniu różnych metod statystycznych i analitycznych.
13. Oprogramowanie musi mieć zapewnione usługi wsparcia technicznego na zasadach opisanych poniżej:
- 1) Usługi będą świadczone przez Wykonawcę w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z Oprogramowania.
 - 2) W ramach świadczonej usługi Wykonawca zapewni:
 - a) dostęp Zamawiającego do usługi wsparcia technicznego w trybie 24h na dobę 7 dni w tygodniu przez 365 dni w roku,
 - b) możliwość zgłaszania przez Zamawiającego błędów drogą telefoniczną lub elektroniczną za pośrednictwem poczty e-mail lub strony WWW,
 - c) dostęp do uaktualnień i poprawek udostępnianych przez producenta oraz obsługi serwisowej (nowe edycje produktów, wydania uzupełniające, aktualizacje, poprawki programistyczne).
14. Dostawę oprogramowania należy zrealizować w godzinach pracy Zamawiającego, od poniedziałku do piątku (z wyjątkiem dni ustawowo wolnych od pracy), a w razie konieczności również poza tymi godzinami, zgodnie z potrzebami określonymi na bieżąco przez Zamawiającego.
15. O planowanym terminie dostarczenia przedmiotu Umowy (dzień i godzina) Wykonawca powiadomi Zamawiającego (faksem lub e-mailem) z co najmniej dwudniowym wyprzedzeniem.
16. Odbiór oprogramowania będzie podlegał na stwierdzeniu jego zgodności z Umową w zakresie liczby oraz parametrów funkcjonalnych. Z czynności odbioru zostanie sporządzony protokół odbioru.

17. Dostarczone przez Wykonawcę oprogramowanie musi być fabrycznie nowe i w przypadku przekazania licencji na nośnikach CD/DVD – zapakowane.
18. Dostarczone przez Wykonawcę oprogramowanie musi pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności jego pochodzenia (np.: oryginalny nośnik, certyfikat autentyczności, kod aktywacyjny, itp.), jeśli jest to niezbędne dla nabycia przez Zamawiającego praw do tego oprogramowania lub jego uruchomienia.
19. W ramach dostawy części 1 przedmiotu Umowy Wykonawca dostarczy oprogramowanie o następujących parametrach:

Część 1: Oprogramowanie wraz z licencjami na systemy operacyjne:

Opis oprogramowania	System operacyjny typu <i>desktop</i> (instalowany na stacjach roboczych)
Warunki licencji	1. Licencje muszą być zapewnione w modelu na urządzenie. 2. Licencje muszą być zapewnione na czas nieograniczony. 3. Oprogramowanie systemowe będzie uruchamiane w przestrzeni wirtualnej – oprogramowanie i licencja musi to umożliwiać. 4. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 24 mc. aktywności subskrypcji.
Cechy oprogramowania	1. Oprogramowanie musi być dostępne w wersji polskiej. 2. Oprogramowanie musi zapewniać pełną integrację z oprogramowaniem systemowym systemu uwierzytelniania opisanego w niniejszym dokumencie. 3. Oprogramowanie musi pozwalać na zarządzanie komputerami poprzez oprogramowanie systemowe systemu uwierzytelniania opisanego w niniejszym dokumencie. 4. Zainstalowany system operacyjny nie może wymagać aktywacji za pomocą telefonu lub Internetu. 5. Oprogramowanie musi pozwalać na pełne uruchomienie bazy danych Systemu Bazy Danych dostarczanego w ramach niniejszego zamówienia. 6. Oprogramowanie musi posiadać pełną obsługę ActiveX. 7. Oprogramowanie musi umożliwiać pełne uruchomienie oprogramowania biurowego np.: MS Office: 2010, 2013, 2016 w wersjach standard oraz pro (w tym MS Access). 8. Oprogramowanie musi umożliwiać zdalną automatyczną instalację, konfigurację, administrowania oraz aktualizowania systemu. 9. Oprogramowanie musi mieć publicznie znany cykl życia przedstawiony przez producenta i dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. 10. Oprogramowanie musi pozwalać na pracę w różnych sieciach komputerowych (sieci lokalne LAN, Internet), w tym także automatyczne rozpoznawanie sieci i ich ustawień bezpieczeństwa. 11. Wszystkie ww. funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji systemu operacyjnego

Opis oprogramowania	Licencje dla usług terminalowych
Warunki licencji	1. Pakiet wymaganych licencji terminalowych: min. 90 jednoczesnych sesji pulpitu zdalnego.

	2. Licencja musi zezwalać na uruchomienie oprogramowania na maszynie wirtualnej posiadającej 24 rdzeni. 3. Licencja musi pozwalać na zmianę wersji oprogramowania na niższą z zachowaniem wsparcia technicznego. 4. Licencja musi umożliwiać przeniesienie oprogramowania na inny serwer fizyczny 5. Licencja musi pozwalać na instalację oprogramowania na serwerze wyposażonym w 24 rdzeni fizycznych 6. Licencja musi zawierać prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych. 7. Oprogramowanie, w ramach dostarczonej licencji musi zawierać prawo do użytkowania i dostępu do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. 8. Licencja musi uprawnian do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.
Cechy oprogramowania	1. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. 2. Licencja musi być zgodna z oprogramowaniem, które wykorzysta 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość budowania klastrów składających się z 64 węzłów. 4. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. 5. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość automatycznej weryfikacji cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 6. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 7. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 8. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

	9. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 10. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 11. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wykorzystania standard http/2. 13. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14. Licencja musi być zgodna z oprogramowaniem, które musi mieć dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych. 15. Licencja musi być zgodna z oprogramowaniem, które musi mieć zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 16. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 17. Licencja musi być zgodna z oprogramowaniem, które musi posiadać mechanizmy logowania oparte o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 18. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 19. Licencja musi być zgodna z oprogramowaniem, które musi zapewniać wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 20. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 21. Licencja musi być zgodna z oprogramowaniem, które musi zapewniać dostępność bezpłatnych narzędzi producenta systemu
--	---

	umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 22.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać dostęp do, pochodzącego od producenta systemu serwisu zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 23.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 24.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Licencja musi być zgodna z oprogramowaniem, które musi zapewniać podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Licencja musi być zgodna z oprogramowaniem, które musi zapewniać usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi. i) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
--	---

	j) Serwis udostępniania stron WWW. k) Wsparcie dla protokołu IP w wersji 6 (IPv6), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. n) Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. o) Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. p) Mechanizmy wirtualizacji mające wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. 25.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów. 26.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28.Licencja musi być zgodna z oprogramowaniem, które musi dostarczać mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. 29.Licencja musi być zgodna z oprogramowaniem, które musi pozwalać na instalację poprawek poprzez wgranie ich do obrazu instalacyjnego.
--	--

	30.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 31.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 32.Licencja musi być zgodna z oprogramowaniem, które musi posiadać wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. 33.Licencja musi być zgodna z oprogramowaniem, które musi dostarczać mechanizmy pozwalające na blokadę dostępu nieznanym procesów do chronionych katalogów.
Inne wymagania	1. Licencje muszą być związane ze zorganizowany systemem szkoleń z materiałami edukacyjnymi w języku polskim. 2. Wszystkie wymienione w tabeli parametry, role, funkcje, itp. oprogramowania muszą być objęte dostarczoną licencją (licencjami) i zawarte w dostarczonej Zamawiającemu wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

Opis oprogramowania	Licencje dostępne do usług serwerowych
Warunki licencji	1. Pakiet licencji powinien pozwalać na jednoczesne połączenie min. 150 użytkowników. 2. Licencja musi być zgodna z oprogramowaniem, które musi zezwalać na uruchomienie oprogramowania na maszynie wirtualnej posiadającej 24 rdzeni. 3. Licencja musi pozwalać na zmianę wersji oprogramowania na niższą z zachowaniem wsparcia technicznego. 4. Licencja musi umożliwiać przeniesienie oprogramowania na inny serwer fizyczny 5. Licencja musi pozwalać na instalację oprogramowania na serwerze wyposażonym w 24rdzeni fizycznych 6. Licencja musi zawierać prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych. 7. Oprogramowanie, w ramach dostarczonej licencji musi zawierać prawo do użytkowania i dostępu do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. 8. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.
Cechy oprogramowania	1. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. 2. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.

	3. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość budowania klastrów składających się z 64 węzłów. 4. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. 5. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość automatycznej weryfikacji cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 6. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 7. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 8. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 9. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 10. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 11. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12. Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wykorzystania standard http/2. 13. Licencja musi być zgodna z oprogramowaniem, które musi zawierać wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14. Licencja musi być zgodna z oprogramowaniem, które musi mieć dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykami na monitorach dotykowych.
--	--

	15.Licencja musi być zgodna z oprogramowaniem, które musi mieć zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 16.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 17.Licencja musi być zgodna z oprogramowaniem, które musi posiadać mechanizmy logowania oparciu o: c) Login i hasło, d) Karty z certyfikatami (smartcard), e) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 18.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 19.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 20.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 21.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 22.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać dostęp do, pochodzącego od producenta systemu serwisu zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 23.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 24.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Licencja musi być zgodna z oprogramowaniem, które musi zapewniać podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Licencja musi być zgodna z oprogramowaniem, które musi zapewniać usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy,
--	--

	komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi. i) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. j) Serwis udostępniania stron WWW. k) Wsparcie dla protokołu IP w wersji 6 (IPv6), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. n) Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. o) Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. p) Mechanizmy wirtualizacji mające wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
--	--

	v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. 25.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 26.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 27.Licencja musi być zgodna z oprogramowaniem, które musi dostarczać mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. 28.Licencja musi być zgodna z oprogramowaniem, które musi pozwalać na instalację poprawek poprzez wgranie ich do obrazu instalacyjnego. 29.Licencja musi być zgodna z oprogramowaniem, które musi zapewniać mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30.Licencja musi być zgodna z oprogramowaniem, które musi posiadać możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31.Licencja musi być zgodna z oprogramowaniem, które musi posiadać wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. 32.Licencja musi być zgodna z oprogramowaniem, które musi dostarczać mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów.
--	---

20. W ramach dostawy części 2 przedmiotu zamówienia Wykonawca dostarczy oprogramowanie o następujących parametrach:

Część 2: Dostawa oprogramowania wraz z licencjami UTM:

Opis oprogramowania	Oprogramowanie UTM
Warunki licencji	1. Licencja/licencje muszą upoważniać do korzystania z aktualnych baz funkcji ochronnych producenta. Powinny obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.

	2. Wsparcie producenta 24/7
Cechy oprogramowania	1. Oprogramowanie realizując funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT, transparentnym. 2. Oprogramowanie po zakupieniu dodatkowych, opcjonalnych licencji, musi zapewniać możliwość budowy minimum 2 oddzielnych (logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. 3. Oprogramowanie musi umożliwiać zdefiniowanie co najmniej 9 administratorów systemu. 4. Oprogramowanie musi wspierać IPv4 oraz IPv6 w zakresie: - Firewall. - Ochrony w warstwie aplikacji. - Protokołów routingu dynamicznego. <u>Redundancja, monitoring i wykrywanie awarii</u> 5. W przypadku oprogramowania pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 6. Oprogramowanie musi zapewniać monitoring i wykrywanie uszkodzenia elementów programowych systemów zabezpieczeń oraz łącz sieciowych. 7. Oprogramowanie musi zapewniać monitoring stanu realizowanych połączeń VPN. 8. Oprogramowanie musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. <u>Interfejsy, Dyski, Procesory, Pamięć</u> 9. Oprogramowanie musi obsługiwać co najmniej 24 interfejsów sieciowych oraz wspierać powierzchnię dyskową o pojemności 2 TB. 10. Oprogramowanie musi obsługiwać nieograniczoną ilość pamięci RAM oraz ilość procesorów: 1. 11. W ramach funkcji Firewall musi być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. <u>Parametry wydajnościowe</u> 12. Oprogramowanie w zakresie Firewall'a musi obsługiwać nie mniej niż 85.000 nowych połączeń na sekundę. 13. Oprogramowanie musi zapewniać przepustowość Stateful Firewall: nie mniej niż 12 Gbps. 14. Oprogramowanie w zakresie Firewall z włączoną funkcją Kontroli Aplikacji musi mieć przepustowość nie mniej niż 2 Gbps. 15. Oprogramowanie musi mieć wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA1: nie mniej niż 1 Gbps. 16. Oprogramowanie musi mieć wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Mix - minimum 1 Gbps.

	17.Oprogramowanie musi mieć wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Kontrola Aplikacji, Antywirus - minimum 700 Mbps. <u>Funkcje Systemu Bezpieczeństwa</u> 18.Oprogramowanie musi zapewniać kontrolę dostępu - zaporą ogniową klasy Stateful Inspection. 19.Oprogramowanie musi zapewniać kontrolę aplikacji. 20.Oprogramowanie musi zapewniać poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 21.Oprogramowanie musi zapewniać ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 22.Oprogramowanie musi zapewniać ochrona przed atakami - Intrusion Prevention System. 23.Oprogramowanie musi zapewniać kontrolę stron WWW. 24.Oprogramowanie musi zapewniać kontrolę zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP. 25.Oprogramowanie musi zapewniać zarządzanie pasmem (QoS, Traffic shaping). 26.Oprogramowanie musi posiadać mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 27.Oprogramowanie musi mieć dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 100 tokenów sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 28.Oprogramowanie musi posiadać możliwość analiza ruchu szyfrowanego protokołem SSL/TLS 1.3 oraz SSH. <u>Polityki, Firewall</u> 29.Oprogramowanie musi zapewniać możliwość kreowania polityka Firewall z uwzględnieniem adresów IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 30.Oprogramowanie musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a) Translację jeden do jeden oraz jeden do wielu. b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 31.W ramach oprogramowanie musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. <u>Połączenia VPN</u> 32.Oprogramowanie musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 33.Oprogramowanie musi zapewniać wsparcie dla IKE v1 oraz v2. 34.Oprogramowanie musi zapewniać obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). 35.Oprogramowanie musi zapewniać obsługę protokołu Diffiego-Hellman grup 19 i 20.
--	--

	36.Oprogramowanie musi zapewniać wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 37.Oprogramowanie musi zapewniać możliwość tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 38.Oprogramowanie musi zapewniać monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 39.Oprogramowanie musi zapewniać możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 40.Oprogramowanie musi zapewniać obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 41.Oprogramowanie musi posiadać mechanizm „Split tunneling” dla połączeń Client-to-Site. 42.Oprogramowanie musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 43.Oprogramowanie musi pozwalać na pracę w trybie portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie oprogramowanie musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. 44.Oprogramowanie w trybie pracy tunel musi mieć możliwość włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 45.Oprogramowanie dla modułów: IPSec VPN oraz SSL VPN musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. <u>Routing i obsługa łączy WAN</u> 46.W zakresie routingu rozwiązanie powinno zapewniać obsługę: 47.Routingu statycznego. 48.Policy Based Routing. 49.Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 50.System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. <u>Zarządzanie pasmem</u> 51.System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 52.Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 53.System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. <u>Kontrola Antywirusowa</u> 54.Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 55.System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 56.System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
--	--

	<u>Ochrona przed atakami</u> 57.Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 58.Ochrona przed atakami na aplikacje pracujące na niestandardowych portach. 59.Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 60.Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 61.System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 62.Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 63.Wykrywanie i blokowanie komunikacji C&C do sieci botnet. <u>Kontrola aplikacji</u> 64.Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 65.Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 66.Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 67.Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 68.Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. <u>Kontrola WWW</u> 69.Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 70.W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 71.Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 72.Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 73.System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 74.Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
--	---

	<u>Uwierzytelnianie użytkowników w ramach sesji</u> 75. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 76. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 77. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji z komponentem umożliwiającym autoryzację użytkowników oraz przy zastosowaniu innych mechanizmów: RADIUS lub API. <u>Zarządzanie</u> 78. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 79. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 80. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 81. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 82. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 83. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. <u>Logowanie:</u> 84. System musi mieć możliwość logowania lokalnego lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 85. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanych, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 86. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 87. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	88. Dostarczone oprogramowanie UTM musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.

	89. Dopuszcza się, aby poszczególne elementy wchodzące w oprogramowania UTM były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: ESXi v6.0 lub wyższe
--	--

Opis oprogramowania	Oprogramowanie do składowania i analizy logów UTM
Warunki licencji	1. Licencja musi pozwalać na przechowanie minimum do 2GB na dzień. 2. Licencja musi pozwalać na przechowanie logów do minimum 1TB.
Cechy oprogramowania	<u>Interfejsy, Dysk:</u> 1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 1 TB. <u>Parametry wydajnościowe:</u> 2. System musi być w stanie przyjmować minimum 2 GB logów na dzień. 3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10000 systemów. 4. Rozwiązanie nie może posiadać ograniczeń co do ilości RAM i vCPU <u>Logowanie</u> 5. Podgląd logowanych zdarzeń w czasie rzeczywistym. 6. Możliwość przeglądania logów historycznych z funkcją filtrowania. 7. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a) Listę najczęściej wykrywanych ataków. b) Listę najbardziej aktywnych użytkowników. c) Listę najczęściej wykorzystywanych aplikacji. d) Listę najczęściej odwiedzanych stron www. e) Listę krajów, do których nawiązywane są połączenia. f) Listę najczęściej wykorzystywanych polityk Firewall. g) Informacje o realizowanych połączeniach IPSec. 8. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 9. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem protokołu logowania do serwera SYSLOG. 10. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi umożliwiać szyfrowanie transmisji. 11. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi

	być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. 12. Musi istnieć możliwość logowania do serwera SYSLOG. <u>Raportowanie</u> 13. W zakresie raportowania system musi zapewniać: 14. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. 15. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 16. Funkcję definiowania własnych raportów. 17. Możliwość spolszczenia raportów. 18. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. <u>Korelacja logów</u> 19. W zakresie korelacji zdarzeń system musi zapewniać: 20. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 21. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 22. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: a) Malware. b) Aplikacje sieciowe. c) Email. d) IPS. e) Traffic. f) Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. <u>Zarządzanie</u> 23. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. 24. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 25. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
--	---

21. W ramach dostawy części 3 przedmiotu zamówienia Wykonawca dostarczy oprogramowanie o następujących parametrach:

Część 3: Dostawa oprogramowania wraz z licencjami kluczy szyfrujących:

Opis oprogramowania	Oprogramowanie do zarządzania kluczami szyfrującymi
Warunki licencji	1. Licencja na dostarczone oprogramowanie musi być dostarczona w postaci licencji bezterminowej na użytkownię.

Wsparcie techniczne	1. Oprogramowanie musi być wdrożone w konfiguracji klastrowej z replikacją kluczy, zasad i informacji konfiguracyjnych w czasie rzeczywistym – umożliwiając pełne przywracanie po awarii i ciągłość biznesową. 2. Wsparcie producenta na okres 24 mc., zawierające pomoc techniczną
Cechy oprogramowania	1. Oprogramowanie musi zapewnić: a) generować symetryczne i asymetryczne klucze kryptograficzne, b) generować dane poufne c) generować certyfikaty X.509; 2. Oprogramowanie musi zapewnić dystrybucję, dezaktywację i usuwanie kluczy; 3. Oprogramowanie powinno posiadać funkcjonalność automatyzowania kluczowych operacji na kluczach związanych z ich wygaśnięciem i rotacją w oparciu o polityki zarządzania kluczami; 4. Oprogramowanie zapewnia kontrolę dostępu do kluczy; 5. Oprogramowanie musi posiadać funkcjonalność pozwalającą na tworzenie kopii zapasowych i przywracanie zawartości kryptograficznej oraz konfiguracji kryptograficznej oprogramowania; 6. Kopia zapasowa musi być chroniona (przynajmniej za pomocą hasła). 7. Rozwiązanie musi wykonywać kopie zapasowe na żądanie i zgodnie z harmonogramem 8. Oprogramowanie musi posiadać możliwość integracji ze sprzętowym modułem bezpieczeństwa (HSM) posiadającym certyfikację FIPS 140-2 Level3 lub wyższą; 9. Oprogramowanie musi mieć możliwość przechowywania, co najmniej 25000 kluczy kryptograficznych; 10. Oprogramowanie musi obsługiwać wiele serwerów i aplikacji z wielu lokalizacji w sieci. Rozwiązanie musi obsługiwać jednocześnie do 100 serwerów lub aplikacji i do 1000 połączeń. 11. Oprogramowanie powinno umożliwiać zdalną administrację za pośrednictwem WebUI, CLI i interfejsu RestAPI 12. Oprogramowanie musi zapewniać integrację poprzez następujące API / interfejsy: NAE-XML, KMIP, REST API. 13. Oprogramowanie powinno oferować możliwości zarządzania kluczami, które można zintegrować z produktami szyfrującymi innych dostawców oferującymi: a) Technologię szyfrowania aplikacji – integracja poprzez API, b) Technologię szyfrowanie bazy danych, w tym natywne szyfrowanie bazy danych (np. transparentne szyfrowanie danych dostępne w rozwiązaniach MS SQL Server i Oracle Database), c) Technologię szyfrowania plików w systemie plików, d) Produkty wspierające standard OASIS Key Management Interoperability Protocol (KMIP); 14. Oprogramowanie w zakresie zarządzania musi: a) obsługiwać operacje obejmujące wiele wdrożeń i produktów szyfrujących, jednocześnie zapewniając administratorom

	ograniczone role zdefiniowane dla ich zakresu obowiązków, ze scentralizowanej konsoli zarządzania, b) musi pozwalać na tworzenie lokalnych użytkowników z dostępem administracyjnym oraz wykorzystywać istniejące usługi katalogowe zgodne z LDAP do mapowania użytkowników dla dostępu administracyjnego, c) pozwalać na tworzenie lokalnych użytkowników z dostępem do kluczy oraz wykorzystywać istniejące katalogi LDAP lub AD do mapowania użytkowników dla dostępu do kluczy; 15.Oprogramowanie musi umożliwiać szczegółowe rejestrowanie i śledzenie audytu wszystkich kluczowych zmian stanu, dostępu administratora oraz zmian zasad 16.Zapisy audytowe muszą być bezpiecznie przechowywane i podpisane w celu niezaprzeczalności. Zdarzenia audytu mogą być wykorzystywane przez wiodące narzędzia klasy SIEM innych firm przekazywane za pośrednictwem SYSLOG. 17.Oprogramowanie musi posiadać mechanizm alarmów pozwalający na powiadamianie administratorów, gdy stan uruchomionego Oprogramowania lub jednego z jego węzłów nie jest w dobrej kondycji lub nie jest skonfigurowany bezpiecznie i należy go zbadać. Rozwiązanie musi umożliwiać ustawienie alarmu dla następujących zdarzeń: a) przestrzeń przechowywania (dysk) jest pełna b) węzeł klastra jest wyłączony lub niedostępny c) wyłączony TLS dla NAE-XML d) (opcja) nieodstępny jest HSM
Inne wymagania	1. Oprogramowanie musi być dostarczone jako maszyna wirtualna, możliwe do umieszczenia w następujących platformach wirtualnych i chmurowych: VMware ESXi 6.0 lub wyższy. Uruchomione oprogramowanie musi działać w trybie dostępności na poziomie minimum 95% 2. W przypadku wielu rozwiązań szyfrujących zintegrowanych z Oprogramowaniem, kluczami należy zarządzać centralnie, bez zauważalnego wpływu na wydajność całości

Opis oprogramowania	Oprogramowanie do realizacji operacji pseudonimizacji.
Warunki licencji	- Oprogramowanie musi być dostarczone z licencją pozwalającą na jego bezterminowe użytkowanie - Oprogramowanie musi być dostarczone wraz ze wszystkimi niezbędnymi licencjami pozwalającymi na podłączenie dwóch serwerów aplikacyjnych korzystających z przekształcania danych.
Wsparcie techniczne	- Oprogramowanie musi być wdrożone w konfiguracji klastrowej z replikacją zasad i informacji konfiguracyjnych w czasie rzeczywistym - umożliwiając pełne przywracanie po awarii i ciągłość biznesową. - Wsparcie producenta na okres 24 mc., zawierające pomoc techniczną

Cechy oprogramowania	1. System musi oferować niezawodne funkcje szyfrowania, maskowania i pseudonimizacji danych z użyciem kluczy symetrycznych i asymetrycznych za pomocą zdefiniowanych profili przekształcania danych. 2. Oprogramowanie musi mieć możliwość stworzenia, co najmniej 1000 szablonów przekształcania danych. 3. Szablon przekształcania danych musi pozwalać na zdefiniowanie, co najmniej następujących parametrów: a. nazwy szablonu, b. grupy użytkowników, którzy mogą wykorzystać szablon, c. sposobu przekształcania danych, d. zestawu znaków, e. wyboru czy przekształcanie ma być nieodwracalne. 4. Oprogramowanie musi obsługiwać wiele serwerów i aplikacji z wielu lokalizacji w sieci. Rozwiązanie musi obsługiwać jednocześnie do 10 serwerów / aplikacji i 100 połączeń. 5. Oprogramowanie powinno umożliwiać zdalną administrację za pośrednictwem WebUI, CLI i interfejsu API REST. 6. Oprogramowanie musi zapewniać integrację poprzez następujące interfejsy API / interfejsy: RestAPI w połączeniu szyfrowanym. 7. Oprogramowanie musi pracować w oparciu o szablony przekształcania danych, które definiują parametry operacji przekształcania, wykorzystywane przez interfejs RestAPI 8. Oprogramowanie musi oferować, co najmniej następujące zestawy znaków: a. wszystkie cyfry, b. wszystkie znaki alfanumeryczne, c. wszystkie znaki drukowalne zestawu ASCII, d. dowolny zdefiniowany zestaw w oparciu o UNICODE. 9. Oprogramowanie musi oferować, co najmniej następujące sposoby przekształcania danych: a. losowy RANDOM, b. z zachowaniem formatu przetwarzanych danych (FPE): FF1 i FF3, c. wybrany dla zapisu daty. 10. Konto użytkownika może być wykorzystane do administracji oprogramowaniem lub być wykorzystywane przez zewnętrzny proces/usługę przy dostępie do szablonu przekształcania danych. 11. Oprogramowanie prawidłowo zainstalowane i skonfigurowane musi pozwala na 100 000 transakcji konwersji danych na sekundę przypadających na jedną instancję oprogramowania (maszynę wirtualną). 12. Oprogramowanie musi posiadać możliwość wdrożenia w konfiguracji klastrowej wysokiej dostępności z równoważeniem obciążenia i z replikacją konfiguracji - umożliwiając pełne przywracanie po awarii i ciągłość operacyjną. 13. Konto użytkownika może być wykorzystane do administracji oprogramowaniem lub być wykorzystywane przez zewnętrzny
-----------------------------	---

	proces/usługę przy dostępie do szablonu przekształcania danych. 14. Oprogramowanie musi umożliwiać szczegółowe rejestrowanie wykonanych operacji przekształcania danych. 15. Musi istnieć możliwość skierowania zarejestrowanych zdarzeń audytowanych i przekształcania danych do zewnętrznych narzędzi klasy SIEM za pośrednictwem SYSLOG. 16. Kopia zapasowa i przywracanie a. Oprogramowanie musi umożliwiać tworzenie kopii zapasowych i przywracanie, b. Kopia zapasowa musi być chroniona (przynajmniej za pomocą hasła), c. Oprogramowanie musi wykonywać kopie zapasowe na żądanie i zgodnie z harmonogramem.
Inne wymagania	1. Oprogramowanie musi być dostarczone jako maszyna wirtualna do obsługi następujących platform wirtualnych i chmurowych: VMware ESXi 6.0 lub wyższy. 2. System musi posiadać możliwość integracji z Oprogramowaniem do zarządzania kluczami szyfrującymi w zakresie pobierania, generacji i przechowywania kluczy szyfrujących.

22. W ramach dostawy części 4 przedmiotu zamówienia Wykonawca dostarczy oprogramowanie o następujących parametrach:

Część 4: Dostawa oprogramowania wraz z licencjami na narzędzia programistyczne:

Opis oprogramowania	Oprogramowanie wspomagające tworzenie Bazy Wiedzy
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 500 użytkowników; 2. Licencja musi zawierać prawo do instalacji na własnym serwerze. 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 24 mc. aktywności subskrypcji.
Cechy oprogramowania	1. Oprogramowanie musi posiadać interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi posiadać możliwość tworzenia, edycji oraz usuwania stron; 3. Oprogramowanie musi posiadać możliwość tworzenia, edycji i usuwania stron różnych kategorii: pustych stron, notatek, wymagań, raportów, decyzji, zadań dla innych osób, innych; 4. Oprogramowanie musi posiadać możliwość komentowania stron; 5. Oprogramowanie musi posiadać możliwość tworzenia powiadomień o zmianach na edytowanych stronach; 6. Oprogramowanie musi posiadać możliwość importu treści z plików doc, docx; 7. Oprogramowanie musi posiadać możliwość przypisywania stronom etykiet (ang. label); 8. Oprogramowanie musi posiadać możliwość wyświetlania stron posiadających odpowiednie etykiety;

	9. Oprogramowanie musi posiadać możliwość katalogowania stron w przestrzenie lub zbiory; 10. Oprogramowanie musi posiadać możliwość wyszukiwania treści; 11. Oprogramowanie musi posiadać możliwość przywoływania osoby, od której wymagane jest wprowadzenie dodatkowych informacji; 12. Oprogramowanie musi posiadać możliwość korzystania z predefiniowanych szablonów stron: „Plan projektu”, „Notatki ze spotkania”, „Plan wprowadzenia produktu na rynek”, „Profil klienta”, „Plan marketingowy”, „Retrospektywa”, „Wymagania produktowe”, „Decyzja”, „Samouczek”, „OKR”, „Plakat projektu”, „Cele, sygnały, wskaźniki”, „Analiza konkurencji”, „Raport z rozmowy z klientem”, „Marketingowy wpis na blogu”, „Kampania marketingowa”, „Schemat komunikacji” lub analogicznych; 13. Oprogramowanie musi posiadać możliwość definiowania uprawnień do przeglądania, dodawania, edycji i komentowania na poziomie przestrzeni (zbioru) oraz pojedynczej strony; 14. Oprogramowanie musi posiadać możliwość definiowania uprawnień dostępu z poziomu panelu; 15. Oprogramowanie musi posiadać możliwość synchronizacji katalogu użytkowników z systemem uwierzytelniania opisanym w poniższym dokumencie oraz LDAP; 16. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	1. Oprogramowanie musi posiadać możliwość podłączenia minimum do baz: DB2, MS SQL Server, MySQL, Oracle, PostgreSQL; 2. Oprogramowanie musi posiadać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 3. Oprogramowanie musi posiadać możliwość integracji z narzędziem do śledzenia błędów oraz zarządzania projektem opisanym w niniejszym dokumencie; 4. Oprogramowanie musi posiadać możliwość instalacji oprogramowania na serwerze pracującym pod kontrolą systemu operacyjnego Linux;

Opis oprogramowania	Narzędzia do śledzenia błędów oraz zarządzania projektem
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 500 użytkowników; 2. Licencja musi zawierać prawo do instalacji na własnym serwerze. 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 24 mc. aktywności subskrypcji.
Cechy oprogramowania	1. Programowanie musi udostępniać podstawowy interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi realizować funkcjonalność narzędzia do śledzenia zadań (issue tracking) 3. Oprogramowanie musi realizować funkcjonalność narzędzia do zarządzania błędami (Bug tracking); 4. Oprogramowanie musi zapewniać możliwość zarządzania wieloma różnymi projektami; 5. Oprogramowanie musi zapewniać wsparcie dla kompleksowego zarządzania projektem i metod typu Agile (Agile Project Management);

	6. Oprogramowanie musi zapewniać możliwość dowolnej konfiguracji przepływu pracy (workflow); 7. Oprogramowanie musi pozwalać integracja z popularnymi platformami programistycznymi jak Eclipse, IntelliJ IDEA, Microsoft Visual Studio, Microsoft Visual Studio Code, JDeveloper, NetBeans, Zend Studio, inne; 8. Oprogramowanie musi zapewniać możliwość zarządzania błędami, właściwościami projektu, zadaniami, osiągnięciami lub innymi zagadnieniami; 9. Oprogramowanie musi zapewniać możliwość połączenia tworzonych zadań i zgłoszeń z kodem źródłowym, dostęp do kodu źródłowego; 10. Oprogramowanie musi zapewniać możliwość dodawania załączników; 11. Oprogramowanie musi zapewniać możliwość tworzenia nowych zadań za pośrednictwem przeglądarki, poczty elektronicznej oraz zintegrowanego środowiska programistycznego (IDE); 12. Oprogramowanie musi zapewniać możliwość szeregowania zadań, nadawania priorytetów; 13. Oprogramowanie musi zapewniać możliwość śledzenia zmian w komponentach i wersjach oprogramowania; 14. Oprogramowanie musi zapewniać możliwość generowania powiadomień członków zespołu projektowego z możliwością ich konfiguracji; 15. Oprogramowanie musi zapewniać możliwość tworzenia ról, poziomów uprawnień, grup użytkowników; 16. Oprogramowanie musi zapewniać możliwość tworzenia użytkowników, przydzielanie ról, poziomów uprawnień dla grup użytkowników; 17. Oprogramowanie musi zapewniać możliwość definiowania uprawnień dostępu z poziomu panelu; 18. Oprogramowanie musi zapewniać możliwość synchronizacji katalogu użytkowników z systemem uwierzytelniania opisanym w poniższym dokumencie oraz LDAP; 19. Oprogramowanie musi zapewniać możliwość rejestracji historii aktywności użytkowników – dostęp do ostatnio otwartych zadań, projektów; 20. Oprogramowanie musi zapewniać możliwość wyszukiwania pełnotekstowego, filtrowania i raportowania; 21. Oprogramowanie musi zapewniać możliwość generowania zestawień i statystyk podsumowujących realizację projektu; 22. Oprogramowanie musi zapewniać możliwość generowania dokumentów w formacie xls, xlsx, xlsx, doc, docx; 23. Oprogramowanie musi zapewniać możliwość wyświetlania podsumowań i raportów dla rozpoczętych projektów – ostanía aktywność, kamienie milowe, logi zmian, mapy projektu, wykresy; 24. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	1. Oprogramowanie musi być dostarczone w najnowszej dostępnej wersji; 2. Oprogramowanie musi zapewniać możliwość podłączenia minimum do baz: MySQL, PostgreSQL, Oracle, SQL Server;

	3. Oprogramowanie musi zapewniać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 4. Oprogramowanie musi zapewniać możliwość integracji z oprogramowaniem wspomagającym tworzenie Bazy wiedzy dostarczonemu w niniejszym postępowaniu 5. możliwość instalacji oprogramowania na serwerze pracującym pod kontrolą systemu operacyjnego Linux; 6. możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git); 7. dostępność aplikacji mobilnej na system Android i iOS.
--	---

Opis oprogramowania	Narzędzie do repozytorium kodu źródłowego
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 100 użytkowników; 2. Licencja musi zawierać prawo do instalacji na własnym serwerze. 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 24 mc. aktywności subskrypcji.
Cechy oprogramowania	1. Oprogramowanie musi posiadać interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi posiadać funkcjonalność narzędzia kontroli wersji kodu źródłowego, 3. Oprogramowanie musi posiadać funkcjonalność narzędzia repozytorium kodu źródłowego, dokumentów, witryn i innych plików; 4. Oprogramowanie musi posiadać możliwość przeglądania kodu źródłowego, dokumentów, witryn i katalogu innych dokumentów; 5. Oprogramowanie musi posiadać możliwość zarządzania prawami dostępu do publikowanych materiałów; 6. Oprogramowanie musi posiadać możliwość zakładania nieograniczonej liczby prywatnych repozytoriów dla każdego z użytkowników; 7. Oprogramowanie musi posiadać możliwość automatycznego generowania plików README na podstawie plików podobnych do plików Markdown; 8. Oprogramowanie musi posiadać funkcjonalność narzędzia do śledzenia problemów (Issue tracking); 9. Oprogramowanie musi posiadać możliwość budowania oprogramowania; 10. Oprogramowanie musi posiadać możliwość śledzenia zmian w komponentach i wersjach oprogramowania; 11. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	1. Oprogramowanie w najnowszej dostępnej wersji; 2. Oprogramowanie musi posiadać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 3. Oprogramowanie musi posiadać dostępność interfejsu REST API; 4. Oprogramowanie musi posiadać oprogramowanie oparte na Git; 5. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem do śledzenia błędów i zarządzania projektem opisanym w niniejszym projekcie, w zakresie pozwalającym na

	śledzenie i edytowanie błędów i problemów, powiązań pomiędzy problemami a kodem źródłowym; 6. Oprogramowanie musi posiadać możliwość instalacji oprogramowania na serwerze pracującym pod kontrolą systemu operacyjnego Linux; 7. Oprogramowanie musi posiadać możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git);
--	---

23. W ramach dostawy części 5 przedmiotu zamówienia Wykonawca dostarczy oprogramowanie o następujących parametrach:

Część 5: Dostawa licencji oprogramowania do monitorowania użytkowników, infrastruktury i obsługi haseł:

Opis oprogramowania	Serwer monitorowania sesji zdalnych
Warunki licencji	1. Licencja na uruchomienie wirtualnego serwera monitorowania sesji zdalnych – wieczysta 2. Licencja na monitorowanie min. 100 sesji zdalnych 3. Licencja na wsparcie producenta na okres 24 mc.
Wsparcie techniczne	1. Zapewnione przez producenta na okres 24 mc.
Cechy oprogramowania	Architektura 1. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu. 2. System musi być zaprojektowany i przygotowany do umieszczenia w DMZ (hardening producenta). 3. System na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem zewnętrznego dostawcy. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia. 4. System musi umożliwiać tryb pracy awaryjnej zapewniający synchronizację danych między dwoma urządzeniami do uprzywilejowanego dostępu zdalnego, tworząc uproszczony proces bezpiecznej wymiany uszkodzonego urządzenia na zapasowe. 5. System musi umożliwiać nawiązywanie sesji przynajmniej w dwóch trybach a. Z wykorzystaniem instalowanego agenta na systemie, do którego będzie nawiązywana sesja, b. Z wykorzystaniem serwerów proxy bez potrzeby instalacji agenta na systemie, do którego będzie nawiązywana sesja. 6. Serwery proxy (nawiązywanie sesji w sposób bezagentowy) muszą być zarządzane w sposób centralny z poziomu oprogramowania do uprzywilejowanego dostępu zdalnego

	(konfiguracja minimalnie w zakresie: nadawania uprawnień dostępowych do serwera proxy dla zewnętrznych dostawców, utworzenie serwera proxy, wyłączenie serwera proxy). 7. Komunikacja między elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego, agentami instalowanymi na urządzeniach końcowych oraz serwerami proxy) musi być szyfrowana (TLS) i odbywać się na jednym porcie 443. 8. System musi posiadać wsparcie dla protokołów SSH, RDP oraz VNC. 9. System musi posiadać możliwość rozbudowy o moduł obsługi sesji do aplikacji WEB (wbudowana przeglądarka WWW). 10. Systemu musi posiadać możliwość uruchomienia sesji aplikacyjnych (uruchomienie wskazanej aplikacji z serwera usług terminalowych lub uruchomienie aplikacji za pomocą dedykowanego agenta) 11. Systemu musi posiadać możliwość tunelowania protokołów TCP na zdefiniowanym porcie między komputerem zewnętrznego dostawcy a zarządzanym systemem. Funkcje operacyjne systemu uprzywilejowanego dostępu zdalnego 12. Logowanie do systemu uprzywilejowanego dostępu zdalnego musi odbywać się poprzez konta lokalne (tworzone na poziomie systemu do uprzywilejowanego dostępu zdalnego) lub konta i grupy importowane z Active Directory. 13. Logowanie dostawców zewnętrznych do systemu uprzywilejowanego dostępu zdalnego musi być zabezpieczone drugim składnikiem (2FA). 14. System musi realizować następujące scenariusze nawiązywania sesji przez zewnętrznego dostawcę: a. za pomocą klienta zainstalowanego na komputerze zewnętrznego dostawcy (gruby klient), b. za pomocą przeglądarki WWW z komputera zewnętrznego dostawcy (bez potrzeby instalacji klienta), c. za pomocą klienta zainstalowanego na urządzeniu mobilnym (minimum wsparcie dla systemu Android). 15. Rozpoczęcie sesji przez zewnętrznego dostawcę musi podlegać kontroli dostępu poprzez: a. Wysyłanie powiadomień o zdarzeniu rozpoczęcia i zakończenia sesji przez zewnętrznego dostawcę do zdefiniowanej listy osób, b. Ograniczenie możliwości nawiązywania sesji przez zewnętrznych dostawców do określonych dni i godzin, oraz do określonych grup zasobów. c. Włączenie procesu wnioskowania przez zewnętrznego dostawcę o dostęp do zasobów i mechanizmu
--	---

	akceptacji lub odrzucenia wniosku przez właściciela zasobu. We wniosku muszą znaleźć się przynajmniej zakres dat kiedy zewnętrzny dostawca będzie nawiązywał sesję oraz pole pozwalające opisać zakres wykonywanych przez niego prac. Wniosek musi być wysyłany w celu akceptacji do zdefiniowanej listy osób. 16. Konsola dostępowa dla zewnętrznego dostawcy musi posiadać co najmniej poniższe funkcje: - widok grup zasobów z możliwością nawiązania sesji do tych zasobów (za pomocą menu kontekstowego lub podwójnego kliknięcia), oraz możliwością wyszukiwania zasobów po ciągach znaków - szczegółowy opis zasobu, do którego możliwe jest nawiązanie sesji, zawierający nazwę hosta / adres IP, status (aktywny/nieaktywny), typ systemu operacyjnego, edytowalną nazwę skróconą. - funkcję wieloosobowego chatu działającą między uczestnikami sesji oraz między zalogowanymi użytkownikami poza sesją. 17. System musi umożliwić wyłączenie synchronizacji schowka i kopiowania plików między komputerem zewnętrznego dostawcy a zarządzanym zasobem. 18. System w trakcie sesji realizowanej przez zewnętrznego dostawcę musi umożliwiać: - Dołączenie do sesji dodatkowych użytkowników posiadających konta w systemie uprzywilejowanego dostępu zdalnego; - Dołączenie dodatkowych użytkowników do sesji nieposiadających konta w systemie uprzywilejowanego dostępu zdalnego przy jednoczesnej możliwości nałożenia dodatkowych restrykcji dla takiej osoby (minimum w zakresie odebrania kontroli myszy i klawiatury); - Przejęcie sesji zewnętrznego dostawcy przez uprawnioną osobę (audytora) i jej zakończenie. Funkcje raportowania 19. System musi posiadać wbudowany i centralnie zarządzany moduł raportowy. 20. System musi generować centralnie konfigurowane i składowane raporty z przeprowadzonych sesji (łącznie z nagraniami sesji). 21. System musi rejestrować sesje graficzne oraz sesje z wierszem poleceń. 22. System musi umożliwiać wybór rozdzielczości rejestrowanych sesji.
--	---

23. W systemie muszą być dostępne raporty dotyczące co najmniej przeprowadzonych sesji i wykorzystania poświadczeń z wbudowanego magazynu haseł.
24. Raporty dotyczące przeprowadzonych sesji muszą podlegać filtrowaniu co najmniej (wymagane wszystkie wymienione) w zakresie daty, nazwy użytkownika (zewnętrznego dostawcy), nazwy / adresu IP zarządzanego zasobu, grupy zarządzanych zasobów.
25. System musi posiadać możliwość uruchomienia filtrowania odbytych sesji po ciągach znaków pisanych z klawiatury w trakcie ich trwania.
26. W szczegółach raportu sesji muszą znajdować się co najmniej informacje na temat:
 - a. daty rozpoczęcia i zakończenia sesji (długość trwania sesji),
 - b. nazwy konta przechowywanego we wbudowanym magazynie haseł za pomocą którego zalogowano się do systemu,
 - c. przesyłanych plików między maszyną zewnętrznego dostawcy a zarządzanym zasobem,
 - d. nagrania z sesji (sesje graficzne oraz okna konsoli),
 - e. transkrypcji chatu,
 - f. wszystkich uczestników sesji (osoby, które dołączały do sesji w trakcie jej trwania),
 - g. listy zdarzeń (log) dotyczący pracy narzędzia uprzywilejowanego dostępu zdalnego,

Konfiguracja i instalacja agentów

27. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi być przygotowany do masowej instalacji.
28. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi posiadać datę ważności, po upływie której niemożliwe będzie jego wykorzystanie.
29. Agent instalowany na zarządzanym zasobie musi być aktualizowany z poziomu systemu uprzywilejowanego dostępu zdalnego.
30. System musi zapewniać możliwość określenia polityk aktualizacji agenta (możliwość definiowania co najmniej liczby jednocześnie aktualizowanych agentów oraz pasma przeznaczonego na aktualizację przez sieć).
31. System musi zapewnić możliwość zdefiniowania akcji zbierania dodatkowych danych na temat zdalnego hosta przez agenta, bez konieczności nawiązywania sesji (przynajmniej w zakresie zużycia CPU, nazwy zalogowanego użytkownika, zajętości dysku).
32. Agenci instalowani na zarządzanych systemach muszą umożliwiać pracę w trybie aktywnego nawiązywania połączenia

z systemem uprzywilejowanego dostępu zdalnego, tj. bez pozostawiania otwartych portów nasłuchujących.

Wbudowany magazyn haseł

33. System musi posiadać wbudowaną funkcjonalność magazynu haseł (przechowywanie haseł, ukrywanie widoczności haseł przed zewnętrznymi dostawcami).
34. System musi umożliwiać dodawanie kont wykorzystywanych do zdalnego logowania co najmniej poprzez:
 - a. wprowadzenie ręczne z poziomu interfejsu konfiguracyjnego narzędzia,
 - b. wyszukanie i import z Active Directory, z możliwością automatycznej zmiany haseł na takich kontach.
 - c. możliwość zintegrowania pobierania poświadczeń z systemu PAM (przynajmniej jednego), poświadczenia muszą być prezentowane w kontekście zasobu, do którego łączy się zewnętrzny dostawca (przy nawiązywaniu sesji musi być możliwość wyboru poświadczeń występujących wyłącznie na danym zasobie).
35. Użycie haseł przez zewnętrznych dostawców musi podlegać kontroli dostępu. Uprawnienia do korzystania z danych poświadczeń (haseł) muszą być przyznawane dla pojedynczego konta dostawcy lub dla grupy kont dostawców.
36. Hasła przechowywane w magazynie haseł muszą być szyfrowane AES256 lub lepszym.

Integracje

37. System musi posiadać otwarte API w zakresie pozwalającym na wykonanie integracji z oprogramowaniem firm trzecich.
38. System musi umożliwiać wykonanie integracji z systemami typu SIEM (poprzez protokół SYSLOG).
39. System musi umożliwiać wykonanie integracji z systemem PAM w zakresie pobierania z niego poświadczeń.

Kontrola dostępu

40. System musi posiadać możliwość zdefiniowania restrykcji sieciowych pozwalających ograniczyć dostęp do interfejsu zarządzającego oprogramowaniem przynajmniej w zakresie zdefiniowania adresów IP hostów lub adresów sieci znajdujących się na białej liście (liście dostępowej) i domyślnej akcji odrzucania innego ruchu skierowanego do interfejsu zarządzającego.
41. System musi umożliwiać edycję poziomu uprawnień użytkowników lub grup użytkowników co najmniej w zakresie:

	a. edycji grup zasobów w zakresie nadawania uprawnień dostępowych do zasobów dla zewnętrznych dostawców oraz uprawnień do edycji tych zasobów (zabronienie możliwości edycji zasobów w systemie uprzywilejowanego dostępu zdalnego), b. edycji i tworzenia nowych poświadczeń w magazynie haseł oraz do przyznawania uprawnień dla zewnętrznych dostawców do możliwości wykorzystania tych poświadczeń, c. generowania i podglądu raportów w tym nagrań z sesji, d. możliwości zapraszania do sesji dodatkowych użytkowników, e. możliwości odebrania lub nadania uprawnień do realizowania sesji z wykorzystaniem instalowanych agentów, serwerów proxy, protokołu RDP lub SSH. f. możliwości definiowania białych lub czarnych list poleceń w sesjach uruchamianych w konsoli.
--	---

Opis oprogramowania	System do samodzielnej obsługi haseł
Warunki licencji	1. Licencja ma umożliwić obsługę min. 500 użytkowników domenowych 2. Licencja ma umożliwić działanie systemu bezterminowo 3. Licencja na wsparcie producenta na okres 24 mc. 4. Licencja ma umożliwić wysłanie min. 2000 SMS
Wsparcie techniczne	1. Zapewnione przez komercyjną firmę, dysponującą inżynierem o umiejętnościach umożliwiających wsparcie techniczne w zakresie problemów z zamawianym rozwiązaniem na okres 24 mc.
Cechy oprogramowania	Kluczowe funkcjonalności: 1. System musi umożliwiać na wdrożenie aplikacji na platformy mobilne iOS. 2. System musi pozwalać na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego. 3. System musi działać w formie aplikacji Internetowej. 4. System musi działać na systemach z rodziny Windows. 5. System musi pozwalać na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore. 6. System musi obsługiwać bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych. 7. System musi działać na pojedynczej bazie danych. 8. System musi posiadać wbudowane skryptu, które pozwalają na: a. backup bazy danych, b. odtworzenie bazy danych, c. zmianę bazy danych.

9. System musi posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
10. System musi używać jednego konta do połączenia z domeną.
11. System musi posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
12. System musi pozwalać na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego.
13. System musi pozwalać na wygenerowanie CSR, do własnego certyfikatu, z poziomu interfejsu graficznego.
14. System musi umożliwiać podłączenie innych aplikacji, w celu autentykacji SSO, poprzez protokół SAML, w tym wszystkie aplikacje będą wyświetlane w interfejsie graficznym aplikacji.
15. System musi umożliwiać na konfigurację uwierzytelniania wieloskładnikowego (MFA) za pomocą dowolnej z 14 obsługiwanych metod uwierzytelniania, w tym YubiKey, uwierzytelniania odcisków palców, RSA SecurID i DUO Security.
16. System musi umożliwiać integrację z usługą 'Have I Been Pwned?' I zablokowanie użycia znanych haseł podczas procesu zmiany hasła lub resetu hasła przez użytkownika.

Funkcjonalności aplikacji:

- a. Aplikacja musi obsługiwać języki: Polski, Angielski.
- b. Aplikacja musi dawać użytkownikom możliwość resetowania hasła, odblokowania konta, aktualizacji danych, zapisywania do grup mailowych i security w środowisku Active Directory. Wszystkie wymienione funkcje powinny być dostępne z poziomu przeglądarki internetowej, a resetowanie hasła i odblokowanie konta z poziomu modułu GINA/Credential Provider Windows
- c. System musi umożliwiać konfigurowanie polityk dla poszczególnych jednostek organizacyjnych OU, a w szczególności:
 - i. Konfigurowanie ustawień dla pytań zabezpieczających i odpowiedzi kontrolnych
 - ii. Konfigurowanie ustawień dla uwierzytelniania za pomocą wiadomości SMS
 - iii. Konfigurowanie ustawień dla uwierzytelniania za pomocą jednorazowej wiadomości e-mail
 - iv. Zablokowanie użytkowników, którzy nie uwierzytelniają się odpowiedziami na pytania kontrolne, kod SMS, jednorazowe hasło wysyłane jako e-mail
 - v. Po udanej autoryzacji następuje automatyczne resetowanie i odblokowywanie kont

	d. Metody uwierzytelniania z punktów x.i - x.xii muszą dawać możliwość ustawienia pojedynczej metody lub powiązania ich ze sobą w celu wprowadzenia uwierzytelniania wieloskładnikowego. e. System musi umożliwiać podłączenie innych aplikacji, w celu autentykacji SSO, poprzez protokół SAML, w tym wszystkie aplikacje będą wyświetlane w interfejsie graficznym aplikacji. f. System musi nie posiadać ograniczenia ilości dodawanych aplikacji, odnosząc się do punktu e. g. System musi umożliwiać notifyfikowanie użytkowników o: i. O fakcie, że hasło wygaśnie za x dni – gdzie istnieje możliwość konfiguracji powiadomień, co cykliczny okres czasu – w tym o niestandardową ilość powiadomień ii. Dokonaniu restartu hasła iii. Dokonania odblokowania konta iv. Dokonania zmiany hasła v. Dokonania rejestracji w programie vi. Dokonania samodzielnej aktualizacji danych h. System musi pozwalać na konfigurację notifyfikacji, w zależności od OU/Grupy i. System musi współpracować z bazą danych MSSQL. j. System musi pozwalać na wysyłanie notifyfikacji za pomocą e-mail'a, jak i SMS'a. k. System musi mieć możliwość wysłania co najmniej 2000 SMS. l. System musi umożliwiać konfigurację widoku edycji danych dla użytkownika w portalu samoobsługi, a w szczególności ma mieć możliwość: i. Modyfikacji ekranu do aktualizacji danych przez użytkowników za pomocą funkcji „przeciągnij i upuść” ii. Dodawania własnych atrybutów m. System musi umożliwiać rejestrowanie pytań i odpowiedzi, a w szczególności i. Wysyłać powiadomienia do użytkowników z prośbą o zdefiniowanie pytań kontrolnych w systemie ii. Wysyłać przypomnienia o rejestracji pytań poprzez wyszukiwanie niezarejestrowanych użytkowników i kojarzenie ich konta ze skryptem logowania, który przypomina o rejestracji przy każdym logowaniu do sieci iii. Rejestrowanie pytań i odpowiedzi dla wielu użytkowników z wykorzystaniem pliku csv n. System musi umożliwiać skonfigurowanie modułu GINA/Credential Provider dla stacji roboczych użytkowników
--	--

	w celu resetowania hasła i odblokowania konta za pomocą ekranu logowania, a w szczególności: i. Pozwalać na instalację modułu GINA/CP bezpośrednio z aplikacji ii. Pozwalać tworzenie harmonogramu instalacji o. System musi umożliwiać dodawanie serwisanta systemu i przypisywanie mu odpowiedniej roli p. System musi umożliwiać tworzenie raportów i posiada wbudowane raporty dotyczące: i. Ogólne raporty w czasie rzeczywistym: 1. Zablokowani użytkownicy 2. Użytkownicy, których hasła wygasły 3. Hasła użytkowników, które wkrótce wygasną ii. Raporty audytowe: 1. Raport z audytu zresetowanych haseł 2. Raport z audytu odblokowanych kont 3. Raport z audytu samodzielnych uaktualnień 4. Raport z audytu zmian hasła iii. Nieudane próby odpowiedzi na pytania zabezpieczające 1. Raporty z rejestracji: 2. Raport o zarejestrowanych użytkownikach 3. Raport o niezarejestrowanych użytkownikach 4. Raport o licencjonowanych użytkownikach 5. Raport o pytaniach i odpowiedziach zabezpieczających q. System musi umożliwiać wyszukiwanie pracowników w katalogu r. System musi umożliwiać automatyczne wysyłanie powiadomień o wygasających hasłach i kontach s. System musi umożliwiać wymuszenie własnych zasad haseł, przy zmianie hasła, w tym ustawiania: i. Minimalnej długości ii. Maksymalnej długości iii. Ilości znaków specjalnych iv. Ilości znaków numerycznych v. Wymuszania, by pierwszym znakiem w hasle była litera vi. Wymuszania, by hasło posiadało duże i małe litery vii. Niezezwalania, by hasło posiadało dwie te same litery z rzędu viii. Niezezwalania, by było używane 5 znaków z loginu ix. Niezezwalania, by było używane 5 znaków z poprzedniego hasła
--	--

	t. Niezezwalania, na użycie określonej liczby kolejnych znaków z nazw użytkowników i starych haseł i. Niezezwalania, na użycie danego znaku (specjalnego, cyfry, litery) określoną ilość razy z rzędu ii. Określanie czy hasło ma się zaczynać od dużej litery, małej litery, cyfry lub znaku specjalnego iii. Niezezwalanie, na zakończenie hasła cyfrą iv. Określenie ilości wykluczonych starych haseł u. System musi pozwalać na synchronizację haseł pomiędzy AD, a: i. Office365 ii. G-Suite iii. IBM AS400 iv. HP UX v. System musi umożliwiać personalizację portalu dla użytkowników w. System musi umożliwiać włączenie workflow (akceptacji) dla: i. Zrestartowania hasła ii. Odblokowania konta iii. Samodzielnej aktualizacji danych w AD x. System musi obsługiwać autoryzację użytkownika końcowego poprzez: i. Pytania zabezpieczające ii. Microsoft Authenticator(TOTP) iii. Google Authenticator iv. Odcisk palca v. YubiKey vi. Notyfikacje push na wcześniej zarejestrowanej aplikacji vii. E-mail viii. SMS ix. Duo Security x. Autentykację RADIUS'ową xi. QR Code xii. SAML xiii. Pytania zabezpieczające z AD y. System musi posiadać aplikację na platformy mobilne, celem weryfikacji użytkownika. z. System musi pozwalać na wdrożenie aplikacji na platformy mobilne iOS. aa. System musi pozwalać na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego. bb. System musi działać w formie aplikacji Internetowej. cc. System musi działać na systemach z rodziny Windows.
--	--

	dd. System musi pozwalać na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore. ee. System musi obsługiwać bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych. ff. System musi działać na pojedynczej bazie danych. gg. System musi posiadać wbudowane skryptu, które pozwalają na: i. backup bazy danych, ii. odtworzenie bazy danych, iii. zmianę bazy danych. hh. System musi posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji. ii. System musi używać jednego konta do połączenia z domeną. jj. System musi posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji. kk. System musi pozwalać na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego. ll. System musi pozwalać na wygenerowanie CSR, do własnego certyfikatu, z poziomu interfejsu graficznego. mm. System musi posiadać integrację z usługą "Have I Been Pwned?", co uniemożliwia korzystanie z naruszonych haseł podczas zmiany lub resetowania hasła przez użytkownika. nn. Administrator musi posiadać możliwość określenia skryptu do rejestracji, widoku tytułu oraz tekstu. oo. System musi posiadać możliwość wykluczenia adresów IP. pp. System musi pozwalać na modyfikację strony logowania do aplikacji, w tym: i. Ma możliwość modyfikacji strony logowania z podstrony administracyjnej ii. Ma możliwość graficznej edycji strony logowania, za pomocą przeciągania odpowiednich elementów. qq. System musi posiadać możliwość zarządzania dostępem na podstawie geolokalizacji.
--	--

Opis oprogramowania	Serwer monitorowania SLA
Warunki licencji	1. Licencja wieczysta na uruchomienie serwera monitorowania SLA powinna umożliwiać podpięcie min. 1000 sensorów
Wsparcie techniczne	1. Zapewnione przez komercyjną firmę, dysponującą inżynierem o umiejętnościach umożliwiających wsparcie techniczne w zakresie problemów z zamawianym rozwiązaniem na okres 24 mc.

Cechy oprogramowania	Kluczowe funkcjonalności oprogramowania do monitorowania: 1. Monitorowanie i ostrzeganie o przestojach lub powolnych serwerach, 2. Monitorowanie stanu systemu różnych urządzeń sprzętowych, 3. Monitorowanie urządzeń sieciowych i rozliczanie przepustowości, 4. Monitorowanie aplikacji, 5. Monitorowanie serwerów wirtualnych, 6. Monitorowanie umowy SLA, 7. Monitorowanie wykorzystania systemu (np. obciążenie procesora, wolna pamięć lub wolne miejsce na dysku), 8. Monitorowanie wydajności bazy danych i wartości tabel, 9. Monitorowanie serwera poczty elektronicznej i przegląd różnych rozwiązań do tworzenia kopii zapasowych, 10. Monitorowanie środowiska fizycznego sieci, 11. Pobieranie informacji za pomocą: a. SNMP b. WMI i Windows Performance Counters c. SSH d. sieciowe protokoły przepływu (jFlow i sFlow) lub podsłuchiwanie ruchu sieciowego (packet sniffing) e. zapytania HTTP f. REST API (wyniki w formacie XML lub JSON) g. PING h. SQL 12. Klasyfikowanie ruchu sieciowego według źródła lub miejsca docelowego, a także treści, 13. Wykrywanie nietypowej, podejrzanej lub złośliwej aktywności na urządzeniach lub użytkownikach, 14. Pomiar parametrów jakości usług (QoS) i Voice over IP (VoIP), 15. Usługi monitorowania w chmurze, 16. Wykrywanie i ocena urządzeń sieciowych, 17. Zbieranie informacji o systemie dla różnych typów sprzętu, 18. Znajdowanie nieoczekiwanych relacji między komponentami sieci w celu wykrywania potencjalnych problemów z bezpieczeństwem i oceny rzeczywistego wykorzystania sieci i sprzętu, 19. Możliwość klastrowania Oprogramowanie do monitorowania posiada: 1. Wysoka wydajność: a. system bazy danych ma przechowywać nieprzetworzone wyniki monitorowania, a także dzienniki, listy Toplists i zgłoszenia, b. możliwość rozdzielenia duże obciążenia na sondy. 2. Dostęp do bazy danych za pośrednictwem interfejsu API. 3. Wysokie standardy bezpieczeństwa: a. zabezpieczone połączenia i serwery internetowe Secure Sockets Layer (SSL) / Transport Layer Security (TLS), b. spersonalizowane zarządzanie prawami użytkowników
-----------------------------	---

	4. Serwer WWW z zabezpieczeniem SSL / TLS z obsługą HTTP i HTTPS dla interfejsu WWW PRTG, który działa jako aplikacja jednostronicowa (SPA), aby uniknąć czasochłonnego ponownego ładowania strony. 5. Serwer przekazujący pocztę e-mail do automatycznego dostarczania wiadomości e-mail. 6. Konfigurowalne, spersonalizowane powiadomienia: a. Różne metody powiadamiania, np. wiadomości e-mail, wiadomości push, wiadomości tekstowe SMS, wiadomości poprzez protokół SYSLOG i pułapki SNMP (Simple Network Management Protocol), żądania HTTP, dzienniki zdarzeń, usługa Amazon Simple Notification Service (SNS), wykonywanie skryptów. b. Wiele sposobów wyzwalania powiadomień, na przykład alerty o stanie, limitach, progach, wielu stanach, eskalacji. c. Stopniowe zależności w celu uniknięcia powodzi alarmowych, potwierdzanie niektórych alarmów w celu uniknięcia dalszych powiadomień o tym alarmie oraz planowanie alertów. 7. Generator raportów do tworzenia raportów na żądanie lub raportów zaplanowanych w HTML, jako plik .pdf, .csv lub .xml. Domyślnie dostępnych ma być kilka szablonów raportów. 8. Silnik graficzny zapewniający przyjazne dla użytkownika wykresy na żywo i wykresy danych historycznych. 9. Moduły analizy sieci do automatycznego wykrywania urządzeń sieciowych i czujników. 10. Funkcjonalność monitorowania kilku sieci w różnych lokalizacjach. 11. Specjalne funkcje dla dostawców usług zarządzanych (MSP) do monitorowania sieci klientów i zwiększania jakości usług. 12. Publikowanie danych za pomocą pulpitów nawigacyjnych w czasie rzeczywistym (mapy prywatne i publiczne), w tym wyniki na żywo i informacje o stanie. Możliwość projektowania tych pulpitów nawigacyjnych z wieloma różnymi obiektami, a także zintegrować obiekty zewnętrzne. 13. Możliwość dostosowania pulpitów nawigacyjnych za pomocą HTML 14. Możliwość tworzenia dedykowanego URL do pulpitu, który może być prywatny lub publiczny 15. Interfejs w wielu językach, takich jak angielski, niemiecki, hiszpański, francuski, portugalski, holenderski, japoński, rosyjski i chiński uproszczony. 16. Możliwość dostosowywania do dodatkowych potrzeb: a. API oprogramowania monitorującego umożliwia tworzenie własnych funkcji, b. tworzenie niestandardowych czujek, powiadomień i szablonów urządzeń zgodnie z określonymi wymaganiami.
--	---

Załącznik nr 2 do SWZ - Projektowane postanowienia umowy.**UMOWA NR**

zawarta w dniu r. w Warszawie¹, zwana dalej „Umową”
pomiędzy:

Skarbem Państwa - Kancelarią Prezesa Rady Ministrów z siedzibą w Warszawie, Aleje
Ujazdowskie 1/3 (00-583 Warszawa) NIP: 5261645000, REGON: 012261725, zwanym dalej
„Zamawiającym”, reprezentowanym przez Michała Pariaszewskiego na podstawie
pełnomocnictwa.

a

..... (dane Wykonawcy) z siedzibą w, przy ul., ,
zwaną/ym dalej „**Wykonawcą**”, reprezentowaną/ym przez, uprawnionego
do jednoosobowej reprezentacji/uprawnionych do łącznej reprezentacji, zgodnie z odpisem z
rejestrów przedsiębiorców KRS/wydrukiem z CEIDG/pełnomocnictwem², którego kopia stanowi
Załącznik nr do Umowy zwaną dalej:

„**Wykonawcą**”,

reprezentowaną przez:

.....

zwanymi łącznie „**Stronami**” lub każda z osobna „**Stroną**”,

zwana dalej: „**Umową**”.

Niniejsza umowa została zawarta w wyniku przeprowadzonego postępowania o udzielenie
zamówienia publicznego w trybie przetargu nieograniczonego na podstawie art. 132 i nast.
ustawy z dnia 11 września 2019 r. *Prawo zamówień publicznych* (Dz. U. z 2019 r., poz. 2019 z
późn. zm., dalej „PZP”), na dostawę licencji oprogramowania niezbędnego do budowy
platformy na potrzeby realizacji projektu „Zintegrowana Platforma Analityczna” (dalej
„Zamówienie”).

Umowa jest finansowana ze środków Unii Europejskiej w ramach projektu pn.
„Zintegrowania Platforma Analityczna” realizowanego w ramach Programu Operacyjnego
Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa nr 2 „E-administracja i otwarty rząd”
Działanie nr 2.2 „Cyfryzacja procesów back-office w administracji rządowej” (dalej „Projekt”).

§1

¹ W przypadku, gdy Umowa będzie zawierana w formie elektronicznej należy usunąć datę i miejsce zawarcia

² Niepotrzebne usunąć

Przedmiot Umowy

1. Przedmiotem Umowy jest dostawa oprogramowania wraz licencjami niezbędnymi do budowy platformy na potrzeby realizacji projektu „Zintegrowana Platforma Analityczna” oraz usługą wsparcia technicznego, zwanego dalej „Oprogramowaniem”, w ramach części Zamówienia.
2. Szczegółowy Opis Przedmiotu Umowy (dalej „SOPZ”) określa załącznik nr 1 do Umowy.

§2

Odbiór przedmiotu Umowy

1. Umowa obowiązuje od dnia zawarcia przez okres 36 m-cy od dnia odbioru Oprogramowania, przy czym Wykonawca zobowiązuje się dostarczyć Oprogramowanie, o którym mowa w § 1 ust. 1, w terminie dni roboczych od dnia jej zawarcia.
2. Zamawiający dokona odbioru przedmiotu Umowy albo odmówi odbioru, jeżeli przedmiot Umowy nie spełni wymagań określonych w Umowie. Czynności odbiorcze powinny zakończyć się w terminie 20 dni roboczych od dnia zawarcia Umowy. Odbiór przedmiotu Umowy zostanie potwierdzony protokołem, którego wzór stanowi załącznik nr 2 do Umowy.

§ 3.

Wynagrodzenie i zasady płatności

1. Za wykonanie Umowy Wykonawcy przysługuje łączne wynagrodzenie w kwocie nie większej niż..... zł netto (słownie),
.....zł brutto (słownie.....) w tym podatek VAT w kwocie.....zł, w tym:
 - 1) Część 1 w kwocie zł netto (słownie),
.....zł brutto (słownie.....) w tym podatek VAT w kwocie.....zł,
 - 2) Część 2 w kwocie zł netto (słownie),
.....zł brutto (słownie.....) w tym podatek VAT w kwocie.....zł,
 - 3) Część 3 w kwocie zł netto (słownie),
.....zł brutto (słownie.....) w tym podatek VAT w kwocie.....zł,
 - 4) Część 4 w kwocie zł netto (słownie),
.....zł brutto (słownie.....) w tym podatek VAT w kwocie.....zł,
 - 5) Część 5 w kwocie zł netto (słownie),
.....zł brutto (słownie.....) w tym podatek VAT w kwocie.....zł,*
- *zostanie dostosowane do oferty złożonej przez wykonawcę.
2. Wynagrodzenie określone w ust. 1 obejmuje wszystkie koszty, jakie powstaną w związku z realizacją Umowy. W przypadku jeśli z dostarczeniem Oprogramowania, o którym mowa w ust. 1, związana jest usługa odpłatnej gwarancji producenta Oprogramowania, wynagrodzenie z tytułu realizacji Umowy, pokrywa koszt tej usługi w okresie do zakończenia gwarancji na ustalonym w Umowie poziomie.
3. Wynagrodzenie, o którym mowa w ust. 1, będzie płatne przelewem bankowym na rachunek Wykonawcy wskazany na fakturze VAT w terminie 21 dni od daty

- otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.
4. Podstawą zapłaty faktury VAT, o której mowa w ust. 3, będzie protokół odbioru, podpisany przez Strony bez zastrzeżeń. Zamawiający nie dopuszcza jednostronnych protokołów odbioru wystawionych przez Wykonawcę.
 5. Wykonawca doręczy Zamawiającemu fakturę na adres Zamawiającego: ul. Królewska 27, 00-060 Warszawa, lub w formie elektronicznej na adres mailowy: efaktury@kprm.gov.pl. Jako nabywcę należy wskazać Kancelarię Prezesa Rady Ministrów, adres: Al. Ujazdowskie 1/3, 00-583 Warszawa, NIP: 526-16-45-000.
 6. Fakturę na wskazany w ust. 5 adres e-mail należy przestać w dniu roboczym do godziny 16:15. Jeżeli faktura wpłynie po godzinie 16:15, datą jej dostarczenia będzie następujący dzień roboczy.
 7. Przez prawidłowo wystawioną fakturę strony rozumieją fakturę wystawioną zgodnie z obowiązującymi przepisami, postanowieniami umowy oraz pozytywnie zweryfikowanym rachunkiem bankowym w wykazie podmiotów, o których mowa w art. 96b ustawy o podatku od towarów i usług.
 8. Wykonawca zobowiązany jest do złożenia oświadczenia podatkowego stanowiącego załącznik nr 4 do umowy w dniu podpisania umowy.

§ 4.

Oświadczenia stron

1. Wykonawca oświadcza, że jest uprawniony do wykonania Umowy, w szczególności sprzedaży licencji Oprogramowania, o którym mowa w § 1 ust. 1.
2. Wykonawca za działania lub zaniechania osób trzecich, którymi posługuje się przy realizacji Umowy, ponosi odpowiedzialność jak za działania lub zaniechania własne.
3. Wykonawca oświadcza, że realizacja Umowy nie naruszy praw osób trzecich, w szczególności autorskich praw majątkowych oraz praw licencyjnych. W przypadku naruszenia takich praw, Wykonawca ponosi odpowiedzialność względem osób trzecich i Zamawiającego oraz zobowiązuje się zwolnić Zamawiającego z odpowiedzialności wobec osób trzecich.
4. Jeżeli Zamawiający nie będzie mógł korzystać z Oprogramowania, Wykonawca na swój koszt uzyska niezwłocznie dla Zamawiającego prawa do kontynuowania korzystania z Oprogramowania.
5. Strony wyznaczają przedstawicieli upoważnionych do współpracy w realizacji Umowy, w tym do dokonywania czynności odbioru oraz podpisywania protokołu odbioru, w osobach:
 - 1) ze strony Zamawiającego:, e-mail, tel.
 - 2) ze strony Wykonawcy:, e-mail, tel.

Zmiana tych osób nie stanowi zmiany Umowy i nie wymaga aneksu, jednak należy o niej niezwłocznie powiadomić drugą Stronę.

§5

Obowiązki Wykonawcy

1. Wykonawca zobowiązuje się wykonywać Umowę z zachowaniem staranności i profesjonalizmu uwzględniających zawodowy charakter prowadzonej przez niego działalność zgodnie z SOPZ oraz Ofertą Wykonawcy.
2. Wykonawca zapewnia, że korzystanie z Oprogramowania podczas realizacji i na cele Umowy nie będzie naruszać praw osób trzecich, w tym w szczególności majątkowych praw autorskich i nie będzie wymagało żadnych opłat na rzecz takich osób.
3. Wykonawca oświadcza, że posiada odpowiedni potencjał techniczny, kadrowy i ekonomiczny oraz posiada wymaganą przez Zamawiającego autoryzację producentów Oprogramowania niezbędną do realizacji przedmiotu Umowy.
4. W celu uniknięcia wątpliwości przyjmuje się, że jeżeli Strony nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji Umowy jako obowiązku Zamawiającego, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca.

§6

Treść licencji

1. Wykonawca, w ramach wynagrodzenia, o którym mowa w § 3 ust. 1, zobowiązuje się do zapewnienia Zamawiającemu niewyłącznej licencji do Oprogramowania, zapewniającej Zamawiającemu prawo do korzystania z Oprogramowania w zakresie wystarczającym do korzystania z niego w sposób określony w SOPZ oraz ofercie Wykonawcy, w tym w szczególności do:
 - 1) wykorzystania w pełnej funkcjonalności określonej w SOPZ,
 - 2) wprowadzania i zapisywania w pamięci komputerów, odtwarzania, utrwalania, przekazywania, przechowywania, wyświetlania i stosowania, instalacji, uruchamiania oraz eksploatacji Oprogramowania,
 - 3) instalacji, uruchamiania oraz eksploatacji Oprogramowania.
2. W ramach udzielonych przez Wykonawcę Zamawiającemu licencji, o których mowa w ust. 1, Zamawiający będzie miał prawo do umożliwienia korzystania w swoim imieniu z Oprogramowania podmiotom publicznym w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r., poz. 346 z późn. zm.) wykonujących badania w ramach platformy ZPA, w tym w szczególności partnerom projektu ZPA.
3. W ramach wynagrodzenia, o którym mowa w § 3 ust. 1, Wykonawca zapewnia Zamawiającemu możliwość instalacji poprawek oraz aktualizacji Oprogramowania udostępnionych przez producentów tego Oprogramowania.
4. W ramach wynagrodzenia, o którym mowa w § 3 ust. 1, Zamawiający ma prawo do korzystania ze zaktualizowanego Oprogramowania jak również z Oprogramowania po zainstalowaniu poprawek na warunkach i polach eksploatacji wskazanych w ust. 1.
5. Wykonawca zobowiązuje się, że w przypadku, gdy podmiot udzielający licencji z wypowie Zamawiającemu licencję do Oprogramowania lub z jakichkolwiek względów utraci zdolność zapewnienia Zamawiającemu możliwości korzystania z tego Oprogramowania w okresie obowiązywania Umowy, Wykonawca w ramach otrzymanego z tytułu Umowy wynagrodzenia dostarczy i oprogramowanie równoważne, posiadające co najmniej analogiczne cechy i funkcjonalność w stosunku do oprogramowania pierwotnego.

§ 7

Obowiązki informacyjne i kontrola

1. Ilekroć w Umowie pojawi się pojęcie:
 - 1) Instytucji Kontrolującej – oznacza to Instytucję Pośredniczącą, ministra właściwego do spraw rozwoju regionalnego, Komisję Europejską, Europejski Trybunał Obrachunkowy, instytucję audytową w rozumieniu art. 2 pkt 8 ustawy z dnia 11 lipca 2014 r. *o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020* (Dz. U. z 2018 r. poz. 1431 z późn. zm.), a także inne podmioty upoważnione do dokonywania kontroli na podstawie odrębnych przepisów;
 - 2) Instytucji Pośredniczącej – oznacza to Centrum Projektów Polska Cyfrowa z siedzibą w Warszawie, będące stroną umowy z Zamawiającym o dofinansowanie Projektu
2. Wykonawca zobowiązuje się do udzielania, na żądanie Zamawiającego lub Instytucji Pośredniczącej, informacji związanych z realizacją Umowy, w szczególności informacji dotyczących postępów prac, przyczyn opóźnień lub przyczyn nienależytego wykonywania Umowy. W ramach tego obowiązku Wykonawca przedstawi Zamawiającemu lub Instytucji Pośredniczącej wszelkie dane i dokumenty związane z realizacją Umowy, a także zapewni udzielenie wyjaśnień przez członków personelu Wykonawcy.
3. Wykonawca zobowiązuje się poinformować Zamawiającego o pojawieniu się jakichkolwiek okoliczności zagrażających należytemu lub terminowemu wykonaniu Umowy, niezwłocznie po ich rozpoznaniu.
4. Wykonawca zobowiązuje się do poinformowania Zamawiającego i Instytucji Pośredniczącej, w formie pisemnej pod rygorem nieważności, o:
 - 1) złożeniu do sądu wniosku o ogłoszenie upadłości Wykonawcy oraz każdej zmianie w tym zakresie;
 - 2) otwarciu likwidacji oraz każdej zmianie w tym zakresie;
 - 3) toczącym się wobec Wykonawcy jakimkolwiek postępowaniu egzekucyjnym, karnym skarbowym lub o zajęciu składników majątku Wykonawcy oraz o każdej zmianie w tym zakresie.
5. Strony potwierdzają, że ilekroć Umowa przewiduje uprawnienie Zamawiającego do żądania od Wykonawcy udzielenia informacji, uprawnienie to przysługuje także Instytucji Kontrolującej. Instytucja Kontrolująca może ponadto żądać udzielenia jej informacji, do której udzielenia Zamawiającemu Wykonawca jest zobowiązany bez uprzedniego żądania.
6. Wykonawca zobowiązuje się do poddania kontrolom w zakresie sposobu, jakości i terminowości realizacji Umowy, prowadzonym przez Instytucję Kontrolującą – za pośrednictwem jej personelu lub z wykorzystaniem osób trzecich. Wykonawca zobowiązuje się do niezwłocznego:
 - 1) zaprezentowania i udostępnienia Instytucji Kontrolującej rezultatów prowadzonych prac w ramach realizacji Umowy;
 - 2) przedstawienia Instytucji Kontrolującej wszelkich informacji i dokumentów związanych z realizacją Umowy, w szczególności rachunków i faktur, umów z podwykonawcami, protokołów, oświadczeń i raportów;
 - 3) udzielenia Instytucji Kontrolującej niezbędnych wyjaśnień.
7. Instytucja Pośrednicząca jest uprawniona do uczestniczenia we wszelkich procedurach odbiorowych. W tym celu Instytucja Pośrednicząca uzyska dostęp do niezbędnych dokumentów i informacji oraz będzie uprawniona do żądania wyjaśnień.

8. Wszelkie ustanowione w Umowie zobowiązania Stron do nieujawniania informacji poufnych nie dotyczą Instytucji Kontrolującej. Jest ona uprawniona do dostępu do wszelkich informacji poufnych należących do Zamawiającego lub Wykonawcy, związanych z realizacją Umowy.
9. Wykonawca zobowiązany jest, na wezwanie Zamawiającego lub Instytucji Pośredniczącej, wziąć udział w wywiadach, ankietach oraz badaniach ewaluacyjnych.

§8

Podwykonawstwo

1. Wykonawca wykona przedmiot Umowy przy udziale następujących podwykonawców:
.....- w zakresie
2. Wykonawca zobowiązany jest do poinformowania Zamawiającego w formie pisemnej lub elektronicznej o każdej zmianie danych dotyczących podwykonawców, jak również o ewentualnych nowych podwykonawcach, którym zamierza powierzyć prace w ramach realizacji Umowy.
3. Informacja o zmianie danych dotyczących podwykonawców powinna zostać przekazana Zamawiającemu w terminie 3 dni roboczych od momentu powzięcia przez Wykonawcę informacji o takiej zmianie.
4. Informacja o zamiarze powierzenia prac nowemu podwykonawcy powinna zostać przekazana Zamawiającemu nie później niż na 3 dni robocze przed planowanym powierzeniem mu realizacji prac.
5. Zmiana podwykonawcy wymaga pisemnej zgody Zamawiającego, nie stanowi jednak zmiany Umowy wymagającej zawarcia aneksu.
6. Jeżeli Wykonawca dokonuje zmiany podwykonawcy, na zasoby którego powoływał się w toku postępowania poprzedzającego zawarcie Umowy, to jest:
..... zobowiązany jest do wykazania Zamawiającemu, że nowy podwykonawca spełnia warunki udziału w postępowaniu poprzedzającym zawarcie umowy. Zamawiający jest uprawniony do odmowy współdziałania z podwykonawcą, co do którego Wykonawca nie wykazał spełnienia warunków lub kryteriów kwalifikacji, do czasu wykazania przez Wykonawcę ich spełnienia, a opóźnienie w wykonaniu Umowy, powstałe wskutek braku współdziałania z takim podwykonawcą, stanowi zwłokę Wykonawcy.
7. Jeżeli Wykonawca rezygnuje z posługiwania się podwykonawcą, na zasoby którego powoływał się w toku postępowania poprzedzającego zawarcie Umowy, to jest:
..... zobowiązany jest do wykazania Zamawiającemu, że Wykonawca samodzielnie spełnia warunki udziału w postępowaniu poprzedzającym zawarcie umowy w stopniu nie mniejszym, niż podwykonawca, z którego Wykonawca rezygnuje. Zamawiający jest uprawniony do odmowy współdziałania z Wykonawcą, który nie wykazał samodzielnego spełnienia warunków, do czasu wykazania przez Wykonawcę ich spełnienia lub wskazania innego podwykonawcy i wykazania spełnienia przez niego tych warunków lub kryteriów, a opóźnienie w wykonaniu Umowy, powstałe wskutek braku współdziałania z Wykonawcą, stanowi zwłokę Wykonawcy.
8. Jeżeli powierzenie podwykonawcy wykonania części przedmiotu Umowy następuje w trakcie jego realizacji, Wykonawca na żądanie Zamawiającego, w celu wykazania, że wobec podwykonawcy nie zachodzą podstawy do wykluczenia, przedkłada dotyczące podwykonawcy oświadczenia lub dokumenty na potwierdzenie braku istnienia

podstaw do wykluczenia wskazane w SIWZ. Jeżeli Zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą podstawy wykluczenia, Wykonawca obowiązany jest zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia podwykonawcy.

9. Wykonawca jest odpowiedzialny za zapłatę wynagrodzenia należnego podwykonawcom, oraz zmiany wysokości wynagrodzenia należnego Wykonawcy w przypadkach, o których mowa w § 13 ust. 9
10. Korzystając w ramach wykonywania niniejszej Umowy ze świadczeń podwykonawców, Wykonawca zobowiązany jest nałożyć na takiego podwykonawcę obowiązek przestrzegania wszelkich zasad, reguł i zobowiązań określonych w Umowie, w zakresie, w jakim odnoszą się one będą do zakresu prac danego podwykonawcy.
11. Powierzenie wykonania części Umowy podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie Umowy. Wykonawca w pełni i wyłącznie odpowiada za działania lub zaniechania podwykonawców jak za działania własne. Wykonawca pozostaje gwarantem wykonywania i przestrzegania przez podwykonawców wszelkich zasad, reguł i zobowiązań określonych w Umowie.
12. Postanowienia Umowy dotyczące Wykonawcy stosuje się odpowiednio do podwykonawcy, chyba że Umowa stanowi inaczej.

§ 9

Gwarancja oraz usługa wsparcia technicznego

1. Wykonawca oświadcza, że Oprogramowanie posiada właściwości określone w Umowie oraz, że w ramach wynagrodzenia, o którym mowa w § 3 ust. 1, udziela Zamawiającemu gwarancji na warunkach określonych w Umowie.
2. Gwarancja obowiązuje przez 12 miesięcy od daty podpisania protokołu odbioru dotyczącego wykonania wszystkich zobowiązań określonych w Załączniku nr 1 do Umowy, z wyłączeniem wykonania usług wsparcia technicznego.
3. Wykonawca jest zobowiązany do usunięcia usterek Oprogramowania, które ujawnią się w terminie 12 miesięcy od dnia podpisania protokołu odbioru, o którym mowa w ust. 2.
4. Wykonawca przekaze Zamawiającemu bezpośredni kontakt (numer telefonu oraz adres email) do wsparcia technicznego producenta dostarczonego Oprogramowania lub zapewni dostęp do wsparcia technicznego przez portal producenta dostarczonego Oprogramowania, dzięki któremu Zamawiający będzie w stanie skorzystać ze wsparcia technicznego.
5. Zgłoszenia przyjmowane będą telefonicznie pod nr tel. lub mailowo na adres lub przez portal producenta dostarczonego Oprogramowania, w godzinach od 9:00 do 17:00, w dni robocze.
6. Czas reakcji Wykonawcy na zgłoszenie Usterki wynosi do 24 godzin roboczych od momentu zgłoszenia Usterki. Poprzez sformułowanie „Usterka” rozumie się niedostępność jakiegokolwiek funkcjonalności dostarczonego Oprogramowania.
7. Czas naprawy Usterki wynosi do 10 dni roboczych od momentu zgłoszenia Usterki. Wyjątkiem są potwierdzone błędy producenta Oprogramowania, gdzie czas naprawy może być dłuższy niż w zdaniu poprzedzającym i zostanie uzgodniony przez Strony.
8. Okres obowiązywania gwarancji będzie automatycznie wydłużany o czas naprawy. Okres gwarancji poprawionego elementu biegnie od początku.

9. Jeżeli Wykonawca stwierdzi, iż przyczyna Usterki leży poza wykonanym przedmiotem Umowy, w szczególności w środowisku informatycznym, w jakim jest zainstalowany, Wykonawca jest zobowiązany:
 - 1) wskazać przyczynę nieprawidłowego działania poprzez wskazanie elementu, który ją powoduje, a jeżeli to możliwe także podmiotu odpowiedzialnego za usunięcie takiej nieprawidłowości działania;
 - 2) w razie zgłoszenia takiej potrzeby przez Zamawiającego – do wsparcia osoby trzeciej usuwającej przyczynę zgłoszenia, w tym udzielenia takiej osobie wszelkich informacji o wykonanym przedmiocie Umowy do przywrócenia pełnej funkcjonalności.
10. Od dnia następującego po ostatnim dniu obowiązywania gwarancji, o której mowa w ust. 1, przez 24 miesiące, Wykonawca zobowiązuje się do zapewnienia obsługi wsparcia technicznego producenta Oprogramowania na zasadach określonych w ust. 4-9.
11. Postanowienia niniejszego paragrafu nie wyłączają uprawnień Zamawiającego z tytułu rękojmi za wady na zasadach określonych w Kodeksie cywilnym.

§ 10

Bezpieczeństwo Informacji

1. Wykonawca zobowiązuje się, że wszelkie informacje podlegające ochronie u Zamawiającego, co do których powziął wiadomość w związku z wykonaniem bądź podpisaniem Umowy, które nie są ujęte w rejestrach publicznych ani nie są powszechnie znane, lub w odniesieniu do których fakt ich publicznej znajomości nie jest następstwem naruszenia zasad poufności lub przepisów prawa, objęte są klauzulą poufności w czasie trwania Umowy, jak również po jej ustaniu, w zakresie nienaruszającym przepisów ustawy *o dostępie do informacji publicznej* oraz ustawy o udostępnianiu informacji *o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko*.
2. Wykonawca zobowiązuje się do nieograniczonego w czasie zachowania w tajemnicy wszelkich informacji związanych z wykonywaniem zadań na rzecz Zamawiającego oraz odpowiada w tym zakresie za pracowników i pracowników podwykonawców, którzy w jego imieniu wykonują zadania na rzecz Zamawiającego.
3. Wykonawca zobligowany jest do niezwłocznego przekazania Zamawiającemu podpisanych przez osoby zaangażowane w realizację Umowy *Oświadczeń podmiotu zewnętrznego o zachowaniu poufności*. Wzór *Oświadczenia podmiotu zewnętrznego o zachowaniu poufności* stanowi Załącznik nr 5 Umowy.
4. Wykonawca udostępnia informacje związane z wykonywaniem zadań na rzecz Zamawiającego, niezbędne do realizacji Umowy, wyłącznie tym spośród pracowników Wykonawcy i podwykonawców, którym są one niezbędne do wykonywania powierzonych zadań. Zakres udostępnianych poszczególnym osobom informacji uzależniony jest od zakresu powierzonych zadań.
5. Obowiązek zachowania poufności nie dotyczy informacji żądanych przez uprawnione organy, w zakresie w jakim te organy są uprawnione do ich żądania, zgodnie z obowiązującymi przepisami prawa. W takim przypadku Wykonawca zobowiązuje się poinformować osobę sprawującą nadzór nad realizacją Umowy o żądaniu takiego organu, przed ujawnieniem informacji.

6. Wykonawca jest zobowiązany do przedstawienia *Listy osób, które będą wykonywały prace na rzecz KPRM*, której wzór stanowi Załącznik nr 7 do Umowy. Listę należy dostarczyć osobie sprawującej nadzór nad realizacją Umowy w terminie co najmniej 10 dni roboczych przed planowanym rozpoczęciem realizacji Umowy.
7. Udostępnianie, ujawnianie, przekazywanie, powielanie oraz kopiowanie przez Wykonawcę dokumentów, zawierających informacje związane z realizacją Umowy, z wyjątkiem przypadków, w jakich jest to konieczne w celu jej realizacji, wymaga zgody Dyrektora Generalnego KPRM.
8. Ujawnienie, przekazanie, wykorzystanie, zbycie przez Wykonawcę informacji, pozyskanych w wyniku realizacji Umowy oraz uzyskanie referencji, wymaga pisemnej zgody Zamawiającego. Nie dotyczy to informacji, które znajdowały się w nieograniczonym posiadaniu Wykonawcy przed ich otrzymaniem od Zamawiającego i są powszechnie znane.
9. Powielanie oraz kopiowanie przez Wykonawcę dokumentów, zawierających dane techniczne związane z systemami i sieciami teleinformatycznymi Zamawiającego, pozyskanych w związku z wykonywaniem zadań na rzecz Zamawiającego w ramach realizacji Umowy, wymaga uzyskania zgody Dyrektora Biura Ochrony KPRM.
10. Wykonawca jest zobowiązany, w uzgodnieniu z osobą sprawującą nadzór nad realizacją Umowy po stronie Zamawiającego, do szyfrowania ogólnodostępnymi mechanizmami kryptograficznymi (np. GPG) korespondencji elektronicznej zawierającej informacje mogące mieć istotny wpływ na bezpieczeństwo lub poufność informacji Zamawiającego.
11. Po wykonaniu Umowy lub na każde wezwanie Zamawiającego, Wykonawca zobowiązuje się do niezwłocznego zwrócenia wszelkich informacji (uzyskanych i wytworzonych w trakcie realizacji Umowy, utrwalonych zarówno w postaci tradycyjnej, jak i elektronicznej) oraz ich kopii, a także trwałego usunięcia informacji przetwarzanych w postaci elektronicznej, w szczególności zawierających dane osobowe. Wykonawca może nie dokonać zniszczenia jedynie tych informacji, które zgodnie z obowiązującymi przepisami prawa muszą pozostać w jego posiadaniu. Wykonawca zobowiązany jest do niezwłocznego przekazania osobie sprawującej nadzór nad realizacją Umowy po stronie Zamawiającego, protokołu z ww. czynności.
12. Zamawiający zastrzega sobie prawo do uczestnictwa w czynnościach usuwania informacji, określonych w ust. 11, a Wykonawca jest zobowiązany do poinformowania osoby sprawującej nadzór nad realizacją Umowy o zamiarze usunięcia przedmiotowych informacji na co najmniej 7 dni przed planowaną datą wykonania przedmiotowej czynności.
13. Wykonawca zobowiązuje się umożliwić Zamawiającemu przeprowadzenie audytu/kontroli w zakresie spełnienia zapisów bezpieczeństwa oraz audytu bezpieczeństwa wdrażanego rozwiązania.
14. Na potrzeby postanowień umowy dotyczących bezpieczeństwa informacji pod pojęciem pracownika rozumie się osoby wykonujące pracę na podstawie stosunku pracy oraz realizujące zadania dla podmiotu zewnętrznego na innej podstawie prawnej.

§11

Kary umowne, zasady odpowiedzialności

1. Wykonawca odpowiada za szkodę wyrządzoną Zamawiającemu, w tym również za szkodę wyrządzoną przez podwykonawców lub osoby, którymi Wykonawca posłużył się przy wykonywaniu Umowy.
2. W przypadku zwłoki w dostawie Oprogramowania, w stosunku do terminu określonego w § 2 ust. 1, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,2% wynagrodzenia brutto określonego w § 3 ust. 1, za każdy rozpoczęty dzień zwłoki.
3. W przypadku niedotrzymania warunków usług wsparcia producenta, Wykonawca zapłaci karę umowną w wysokości 0,05 % wynagrodzenia brutto, określonego w § 3 ust. 1, za każdy rozpoczęty dzień zwłoki w stosunku do terminów określonych w § 9.
4. W przypadku odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy, Zamawiający naliczy Wykonawcy karę umowną w wysokości:
 - a) 10% kwoty całkowitego wynagrodzenia brutto określonego w § 3 ust. 1, w przypadku odstąpienia od Umowy w całości;
 - b) 5% kwoty całkowitego wynagrodzenia brutto określonego w § 3 ust. 1, w przypadku odstąpienia od Umowy w części.
5. Zamawiający ma prawo naliczania Wykonawcy kar umownych w wysokości 500,00 zł za każde stwierdzone naruszenie obowiązku polegającego na:
 - a) przestrzeganiu określonych w § 7 obowiązków informacyjnych i dotyczących kontroli;
 - b) zachowaniu zasad bezpieczeństwa informacji, określonych w § 10
6. W przypadku braku zapłaty lub nieterminowej zapłaty wynagrodzenia należnego podwykonawcom, w tym w przypadku braku zapłaty lub nieterminowej zapłaty wynagrodzenia należnego podwykonawcom z tytułu zmiany wysokości wynagrodzenia o których mowa w § 13 ust. 9, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia brutto określonego w § 3 ust. 1.
7. Wykonawca zapłaci kary umowne w terminie 14 dni od daty otrzymania wystosowanego przez Zamawiającego wezwania do zapłaty. Po upływie terminu wskazanego zd. pierwszym, Zamawiający potrąci naliczone kary z wynagrodzenia należnego Wykonawcy bądź dokona zaspokojenia roszczeń z zabezpieczenia należytego wykonania Umowy, według wyboru Zamawiającego, na co Wykonawca wyraża zgodę, z zastrzeżeniem art 15 r1 ust. 1 i 2 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem Covid-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020 r. poz. 374 z późn. zm.).
8. Potrącenie, o którym mowa w ust. 12, jest skuteczne bez składania dodatkowych oświadczeń.
9. Strony zgodnie ustalają, że kary umowne nałożone na Wykonawcę w związku z realizacją Umowy nie mogą przekroczyć wartości 80% Wynagrodzenia brutto należnego Wykonawcy.
10. Zapłata kar umownych z tytułu niewykonania lub nienależytego wykonywania Umowy nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych uregulowanych w Kodeksie Cywilnym.

§ 12

Odstąpienie od Umowy

1. Zamawiający może odstąpić od Umowy bez wyznaczania dodatkowego terminu w przypadku gdy zwłoka w wykonaniu Umowy w stosunku do któregośkolwiek z terminów wskazanych w § 2 pkt 1 lit. a lub b wynosi więcej niż 7 dni.
2. Zamawiający może odstąpić od Umowy w przypadku, gdy:
 - 1) zaistniała istotna zmiana okoliczności powodująca, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy – w tym przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Przedmiotu Umowy;
 - 2) stwierdził zaistnienie, po stronie Wykonawcy, okoliczności uniemożliwiające wykonanie lub należyte wykonanie Przedmiotu Umowy, w szczególności Wykonawca zaprzestał prowadzenia działalności, wszczęte zostało wobec niego postępowanie likwidacyjne, upadłościowe, bądź postępowanie naprawcze z tej przyczyny;
 - 3) Wykonawca nienależyście wykonuje Przedmiot Umowy, po uprzednim pisemnym wezwaniu Wykonawcy do należytego wykonania Przedmiotu Umowy oraz upływie wyznaczonego stosownego terminu, nie krótszego niż 14 Dni Roboczych.
3. Odstąpienie od Umowy powinno nastąpić na piśmie pod rygorem nieważności i zawierać uzasadnienie.
4. Odstąpienie od Umowy nie narusza określonego w § 11 obowiązku zachowania bezpieczeństwa informacji.

§13

Zmiany Umowy

1. Wszelkie zmiany Umowy wymagają dla swej ważności aneksu zawartego w formie pisemnej albo elektronicznej (kwalifikowany podpis elektroniczny).
2. Umowa może zostać zmieniona w sytuacji gdy:
 - 1) zaistnieją okoliczności związane z wystąpieniem wirusa SARS-CoV-2, które wpływają lub mogą wpłynąć na należyte wykonanie Umowy;
 - 2) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy;
 - 3) wynikną rozbieżności lub niejasności w Umowie, których nie można usunąć w inny sposób, a zmiana Umowy będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej postanowień przez Strony;
 - 4) zaistnieje konieczność wprowadzenia zmiany terminu realizacji Przedmiotu Umowy;
 - 5) zaistnieje działanie siły wyższej rozumianej jako nadzwyczajne okoliczności niezależne od Stron, których nie można było przewidzieć, jak m.in.: wojna, stany wyjątkowe, strajki generalne, blokady, embargo, działania sił przyrody o charakterze klęsk żywiołowych jak huragany, powodzie, trzęsienia ziemi, pożary, epidemie, pandemie itp., uniemożliwiającej realizację w części lub w całości Przedmiotu Umowy;
 - 6) wystąpią uzasadnione zmiany w zakresie sposobu realizacji, w tym zmiana miejsca lub terminu realizacji Przedmiotu Umowy;
 - 7) nastąpi konieczność zmiany warunków i terminów płatności.
3. Strony mają prawo do przedłużenia terminu zakończenia wykonywania Przedmiotu Umowy o okres trwania przyczyn, z powodu których nie było możliwe wykonanie dostawy, w następujących sytuacjach:
 - 1) jeżeli przyczyny, z powodu których nie było możliwe wykonanie dostawy są następstwem okoliczności, za które odpowiedzialność ponosi Zamawiający,

- 2) wystąpią opóźnienia w dokonaniu określonych czynności lub ich zaniechanie przez właściwe organy administracji państwowej, które nie są następstwem okoliczności, za które Wykonawca ponosi odpowiedzialność,
 - 3) gdy wystąpią opóźnienia w wydawaniu decyzji, zezwoleń, uzgodnień, itp., do wydania których właściwe organy są zobowiązane na mocy przepisów prawa, jeżeli opóźnienie przekroczy okres, przewidziany w przepisach prawa, w którym ww. decyzje powinny zostać wydane oraz nie są następstwem okoliczności, za które Wykonawca ponosi odpowiedzialność,
 - 4) wystąpienia zdarzeń natury siły wyższej uniemożliwiającej wykonanie Przedmiotu Umowy z godnie z jej postanowieniami.
4. Strony są uprawnione do zmiany Umowy w zakresie materiałów, parametrów technicznych, technologii, sposobu i zakresu wykonania Przedmiotu Umowy, bez zmiany wysokości wynagrodzenia należnego Wykonawcy, w następujących sytuacjach:
- 1) konieczności zrealizowania jakiegokolwiek części Przedmiotu Umowy, przy zastosowaniu odmiennych rozwiązań technicznych lub technologicznych, niż wskazane w opisie przedmiotu zamówienia, a wynikających ze stwierdzonych wad opisu przedmiotu zamówienia, zmiany stanu prawnego w oparciu, o który je przygotowano, gdyby zastosowanie przewidzianych rozwiązań groziło niewykonaniem lub nienależytym wykonaniem Przedmiotu Umowy,
 - 2) konieczności zrealizowania Przedmiotu Umowy przy zastosowaniu innych rozwiązań technicznych lub materiałowych ze względu na zmiany obowiązującego prawa,
 - 3) wystąpienia siły wyższej uniemożliwiającej wykonanie Przedmiotu Umowy zgodnie z jej postanowieniami.
 - 4) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili podpisania Umowy, nie powodujących zmiany Przedmiotu Umowy;
 - 5) w zakresie terminu realizacji Umowy, gdy producent wprowadza nowe wersje (charakteryzujące się wyższymi parametrami) posiadanego oprogramowania, co ma wpływ na realizację umowy lub zmieniają się warunki udzielenia licencji przez producenta.
5. Zamawiający dopuszcza zmianę postanowień Umowy w stosunku do treści Oferty w sytuacji, gdy nie była możliwa do przewidzenia na etapie zawarcia Umowy, a ponadto jej dokonanie podyktowane jest zmianą stanu prawnego w zakresie mającym wpływ na realizację Umowy, tj. w szczególności:
- 1) stawki podatku od towarów i usług;
 - 2) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (t.j. Dz.U. z 2018 r. poz. 2177);
 - 3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne;
 - 4) – zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U. poz. 2215 oraz z 2019 r. poz. 1074 i 1572);
- jeżeli zmiany te będą miały wpływ na koszty wykonania Przedmiotu Umowy przez Wykonawcę, każda ze Stron Umowy, w terminie 30 (trzydziestu) dni kalendarzowych od dnia wejścia w życie przepisów dokonujących tych zmian, może zwrócić się do drugiej

Strony o przeprowadzenie negocjacji w sprawie odpowiedniej zmiany wysokości wynagrodzenia.

6. W razie wątpliwości, przyjmuje się, że nie stanowią zmiany Umowy następujące zmiany:
 - 1) danych związanych z obsługą administracyjno-organizacyjną Umowy,
 - 2) danych teleadresowych,
 - 3) danych rejestrowych,
 - 4) będące następstwem sukcesji uniwersalnej po jednej ze stron Umowy,
7. Warunkiem dokonania zmiany Umowy jest złożenie wniosku przez Stronę inicjującą zmianę, zawierającego w szczególności opis propozycji zmian, ich uzasadnienie, a w przypadku jeśli wniosek pochodzi od Wykonawcy i wskazuje na potrzebę zmiany wysokości wynagrodzenia, także kalkulację uzasadniającą tę zmianę.
8. Wykonawca, którego wynagrodzenie zostało zmienione zgodnie z ust. 1-8, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom dotyczącym zobowiązania podwykonawcy

§ 14

Zabezpieczenie należytego wykonania Umowy

1. Wykonawca wniósł zabezpieczenie należytego wykonania Umowy, zgodnie z art. 450 ust. 1 pkt Pzp, w formie, w wysokości zł (słownie złotych:), co stanowi 5 % wynagrodzenia całkowitego brutto za wykonanie przedmiotu Umowy („Zabezpieczenie”). Dokument potwierdzający zabezpieczenie należytego wykonania Umowy stanowi Załącznik nr do Umowy.
2. Wykonawca jest zobowiązany do niezwłocznego informowania Zamawiającego o faktycznych lub prawnych okolicznościach, które mają lub mogą mieć wpływ na moc wiążącą Zabezpieczenia należytego wykonania Umowy oraz na możliwość i zakres wykonywania przez Zamawiającego praw wynikających z Zabezpieczenia.
3. Wniesione Zabezpieczenie należytego wykonania Umowy zabezpiecza roszczenia z tytułu niewykonania lub nienależytego wykonania Umowy, w tym usunięcia wad, w szczególności roszczenia Zamawiającego wobec Wykonawcy o zapłatę kar umownych.
4. W przypadku wystąpienia przez Wykonawcę z żądaniem zmiany sposobu zabezpieczenia należytego wykonania Umowy dotychczasowe zabezpieczenie zostanie wydane lub zwrócone Wykonawcy w terminie 14 dni od ustanowienia oraz dostarczenia Zamawiającemu nowego zabezpieczenia w formie zaakceptowanej uprzednio na piśmie przez Zamawiającego.
5. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone Wykonawcy pod warunkiem należytego wykonania Umowy.
6. Jeżeli w terminie 30 dni przed wygaśnięciem obowiązującego Zabezpieczenia należytego wykonania Umowy wniesionego w innej formie niż pieniężna, Wykonawca w przypadku konieczności jego przedłużenia, nie przedłuży lub nie wniesie nowego Zabezpieczenia należytego wykonania Umowy, to Zamawiający zmieni formę zabezpieczenia na zabezpieczenie w pieniądzu poprzez wypłatę kwoty z dotychczasowego zabezpieczenia. Wypłata, o której mowa w zdaniu poprzednim, następuje nie później niż w ostatnim dniu ważności dotychczasowego zabezpieczenia. Zmiana formy zabezpieczenia następuje z zachowaniem ciągłości oraz wysokości zabezpieczenia.
7. W przypadku zabezpieczenia należytego wykonania Umowy o charakterze niepieniężnym, w tym w szczególności, gdy będzie nim gwarancja bankowa lub ubezpieczeniowa, powinno mieć ono charakter nieodwołalny, bezwarunkowy, płatny na pierwsze żądanie.

- Zamawiający wymaga, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie Zamówienia, gwarancja bankowa lub ubezpieczeniowa obejmowała swoją treścią zobowiązanie solidarne wszystkich Wykonawców wspólnie ubiegających się o udzielenie Zamówienia (zobowiązanych z tytułu gwarancji).
8. Sądem właściwym dla rozstrzygania sporów na gruncie gwarancji winien być sąd polski właściwy miejscowo dla siedziby Zamawiającego. Gwarancja powinna być sporządzona w języku polskim, natomiast w przypadku gdy językiem gwarancji jest język obcy wówczas taka gwarancja winna być przedłożona wraz z tłumaczeniem przysięgłym. Jeśli gwarancja poza językiem polskim sporządzona będzie również w innym języku, w razie rozbieżności między wersjami językowymi decydująca będzie wersja językowa polska. Gwarancja bankowa albo ubezpieczeniowa będzie sporządzona i interpretowana zgodnie z prawem obowiązującym w Polsce.
 9. Zabezpieczenie należytego wykonania Umowy wnoszone w pieniądzu Wykonawca wpłaci przelewem na rachunek bankowy Zamawiającego. Jeżeli Zabezpieczenie należytego wykonania Umowy wniesiono w pieniądzu, Zamawiający przechowuje je na oprocentowanym rachunku bankowym. Zamawiający zwraca Zabezpieczenie należytego wykonania Umowy wniesione w pieniądzu wraz z odsetkami, wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.
 10. Jeżeli na skutek jakichkolwiek okoliczności, w szczególności ogłoszenia upadłości gwaranta lub innych zdarzeń zależnych lub niezależnych od Stron, Zamawiający utraci w trakcie realizacji Umowy Zabezpieczenie należytego wykonania Umowy, Wykonawca niezwłocznie, lecz nie później niż w terminie 14 dni od takiego zdarzenia, ustanowi nowe Zabezpieczenie należytego wykonania Umowy w wysokości nie niższej niż wynikająca z Umowy. W razie braku ustanowienia przez Wykonawcę Zabezpieczenia należytego wykonania Umowy zgodnie z postanowieniami Umowy Zamawiający może, aż do ustanowienia Zabezpieczenia należytego wykonania Umowy, wstrzymać wszelkie płatności na rzecz Wykonawcy. Wstrzymanie płatności nie zwalnia Wykonawcy z jakichkolwiek obowiązków Wykonawcy określonych w Umowie.

§ 15

Ochrona danych osobowych

1. Zamawiający oświadcza, że będzie przetwarzał przekazane mu przez Wykonawcę dane osobowe osób skierowanych przez Wykonawcę do realizacji przedmiotu Umowy, jeśli zajdzie taka czynność.
2. Wykonawca oświadcza, że przekazane dane osobowe, o których mowa w ust. 1, zebrał i przetwarza zgodnie z obowiązującymi w tym zakresie regulacjami prawnymi i jest uprawniony do ich przekazania Zamawiającemu oraz uczynił zadość wszelkim obowiązkom związanym z ich przekazaniem, a w szczególności poinformował osoby, których dane przekazuje, o fakcie i celu ich przekazania.
3. W razie wystąpienia przez osoby, których dane osobowe zostały przekazane przez Wykonawcę, z jakimikolwiek roszczeniami do Zamawiającego wynikającymi z naruszenia przez Wykonawcę obowiązku, o którym mowa w ust. 2, lub w razie wszczęcia jakiegokolwiek postępowania publicznoprawnego z tym związanego, Wykonawca:
 - a) ponosić będzie odpowiedzialność z tytułu ewentualnych naruszeń praw osób, których dane osobowe zostały przekazane przez Wykonawcę Zamawiającemu w

- ramach realizacji Umowy lub z tytułu związanych z tym naruszeń prawa powszechnie obowiązującego w zakresie danych osobowych;
- b) udzieli Zamawiającemu niezbędnej pomocy do wyjaśnienia zaistniałej sytuacji, w szczególności złoży niezbędne wyjaśnienia i dokumenty;
 - c) po uzgodnieniu z Zamawiającym, przystąpi na własny koszt do wszczętych postępowań po stronie Zamawiającego;
 - d) zwolni Zamawiającego z kosztów jego udziału w tych postępowaniach;
 - e) zwolni Zamawiającego od obowiązku świadczeń z tytułu uwzględnionych lub nałożonych przez właściwe sądy lub organy roszczeń, kar i innych obciążeń w związku z naruszeniami praw osób, których dane osobowe zostały przekazane przez Wykonawcę Zamawiającemu w ramach realizacji Umowy lub związanych z tym naruszeń prawa powszechnie obowiązującego w zakresie danych osobowych.

§16

Klauzula salwatoryjna

1. W przypadku stwierdzenia, że którekolwiek z postanowień Umowy jest z mocy prawa nieważne lub bezskuteczne, okoliczność ta nie będzie miała wpływu na ważność, skuteczność lub możliwość wyegzekwowania pozostałych postanowień, chyba że z okoliczności wynikać będzie w sposób oczywisty, że bez postanowień nieważnych lub bezskutecznych, Umowa nie zostałaby zawarta.
2. W sytuacji, o której mowa w ust. 1, Strony zobowiązują się zawrzeć aneks do Umowy, w którym sformułują postanowienia zastępcze, których cel gospodarczy i ekonomiczny będzie równoważny lub maksymalnie zbliżony do celu postanowień nieważnych lub bezskutecznych.
3. W przypadku nieosiągnięcia porozumienia do treści postanowień zastępczych zastosowanie będą miały przepisy kodeksu cywilnego.

§ 17

Postanowienia końcowe

1. W sprawach nieuregulowanych Umową zastosowanie mają przepisy prawa polskiego, w szczególności przepisy ustawy prawo zamówień publicznych, Kodeksu cywilnego i ustawy o prawie autorskim i prawach pokrewnych.
2. Ilekroć w Umowie jest mowa o „dniach roboczych” Strony rozumieją przez to dni od poniedziałku do piątku z wyłączeniem dni uznanych ustawowo za wolne od pracy. Dla uniknięcia wątpliwości Strony wskazują, że terminy wskazane w Umowie należy liczyć w dniach roboczych tylko w przypadku takiego wyraźnego wskazania w Umowie.
3. Zmiany postanowień Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Przeniesienie uprawnień, obowiązków i wierzytelności z Umowy wymaga zgody drugiej Strony, z zastrzeżeniem przypadku określonego § 6 ust. 2.
5. Pisma przesłane na adresy Stron określone w komparycji Umowy uważa się za skutecznie doręczone, chyba że Strony poinformują się pismem poleconym o zmianie adresu.
6. Za dni robocze Strony przyjmują dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
7. Wykonawca nie może przenieść wierzytelności wynikających z Umowy na rzecz osób trzecich bez pisemnej zgody Zamawiającego.
8. Korespondencja przesłana pocztą elektroniczną na wskazane w Umowie adresy e-mail uważana jest za skutecznie doręczoną w chwili, w której przesyłana wiadomość zostanie

- umieszczona na serwerze obsługującym konto pocztowe jej adresata, i tenże adresat będzie mógł w toku zwykłych czynności zapoznać się z jej treścią.
9. Spory wynikłe w związku lub na podstawie umowy i nie rozstrzygnięte polubownie będą rozstrzygane przez sąd właściwy miejscowo dla Zamawiającego.
10. Integralną część Umowy stanowią Załączniki:
- 1) Załącznik Nr 1 – Szczegółowy opis przedmiotu Zamówienia,
 - 2) Załącznik Nr 2 – Wzór protokołu zdawczo-odbiorczego,
 - 3) Załącznik Nr 3 – Oferta Wykonawcy,
 - 4) Załącznik nr 4 – Oświadczenie podatkowe.
 - 5) Załącznik nr 5 - Wzór Oświadczenia podmiotu zewnętrznego o zachowaniu poufności
 - 6) Załącznik nr 6 Dowód wniesienia zabezpieczenia
 - 7) Załącznik nr 7 do Zasad bezpieczeństwa przy współpracy z podmiotami zewnętrznymi, stanowiących załącznik nr 1 do karty procesu B2.2, wersji nr 3.0 z dnia 7 lutego 2019
11. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, z których jeden otrzymuje Zamawiający, a jeden Wykonawca³ / wchodzi w życie z dniem podpisania przez ostatnią ze Stron⁴.

ZAMAWIAJĄCY

.....

WYKONAWCA

.....

³ W przypadku podpisywania Umowy w formie papierowej

⁴ W przypadku podpisywania Umowy w formie elektronicznej

Załącznik nr 2 do Istotnych postanowień umowy

PROTOKÓŁ ZDAWCZO-ODBIORCZY

Miejsce i data dokonania odbioru:

Ze strony Wykonawcy:
(imię i nazwisko osoby upoważnionej) (nazwa Wykonawcy)

Ze strony Zamawiającego:
(imię i nazwisko osoby upoważnionej) (nazwa Wykonawcy)

Przedmiotem odbioru w ramach Umowy nr z dnia
jest **dostawa rzecz Zamawiającego licencji oprogramowania:**

- a) Część 1: Dostawa oprogramowania wraz z licencjami na systemy operacyjne:
 - I. Systemu operacyjnego typu *desktop* (instalowanych na stacjach roboczych) w ilości 50 szt.;
 - II. Licencje dla usług terminalowych w ilości 90 szt.;
 - III. Licencje do usług serwerowych w ilości 150 szt.
- b) Część 2: Dostawa oprogramowania wraz z licencjami UTM:
 - I. Oprogramowanie UTM w ilości 1 szt.;
 - II. Oprogramowanie do składowania i analizy logów systemu UTM w ilości 1 szt.
- c) Część 3: Dostawa oprogramowania wraz z licencjami kluczy szyfrujących:
 - I. Oprogramowanie do zarządzania kluczami szyfrującymi w ilości 2 szt.;
 - II. Oprogramowanie do realizacji operacji pseudonimizacji w ilości 2 szt.
- d) Część 4: Dostawa oprogramowania wraz z licencjami na narzędzia programistyczne:
 - I. Oprogramowanie wspomagające tworzenie Bazy Wiedzy w ilości 1 szt.;
 - II. Oprogramowanie do śledzenia błędów oraz zarządzania projektem w ilości 1 szt.;
 - III. Oprogramowanie do repozytorium kodu źródłowego w ilości 1 szt.
- e) Część 5: Dostawa licencji oprogramowania do monitorowania użytkowników, infrastruktury i obsługi haseł:
 - I. Serwer monitorowania sesji zdalnych i wsparcia zdalnego dla użytkowników w ilości 1 szt.;
 - II. System do samodzielnej obsługi haseł w ilości 1 szt.;
 - III. Serwer monitorowania SLA w ilości 1 szt.

Potwierdzenie kompletności odbieranego przedmiotu umowy:

Tak* (potwierdzam odebranie bez zastrzeżeń)

Tak* (potwierdzam odebranie – zastrzeżenia.....)

Nie* –

Końcowy wynik odbioru:

Pozytywny*

Pozytywny* – zastrzeżenia.....

Negatywny* –

* niepotrzebne skreślić

Podpisy:

.....

(Ze strony Zamawiającego)

.....

(Ze strony Wykonawcy)

Załącznik nr 4 do Istotnych postanowień umowy

Oświadczenie podatkowe

Firma:

Adres:

Ulica: nr domu:, nr mieszkania:

kod pocztowy: Gmina:

Powiat: Województwo:

Identyfikator podatkowy NIP

Urząd Skarbowy:

.....

Podpis

Załącznik nr 5 do Istotnych postanowień umowy

OŚWIADCZENIE PODMIOTU ZEWNĘTRZNEGO O ZACHOWANIU POUFNOŚCI

I. Dane osoby składającej oświadczenie	
1.	Nazwisko
2.	Imię
3.	PESEL
II. Dane Podmiotu	
1.	Nazwa Podmiotu
2.	Adres Podmiotu
III. Treść oświadczenia	
W czasie wykonywania zadań na rzecz Kancelarii Prezesa Rady Ministrów, a także po ich zakończeniu zobowiązuję się do zachowania w tajemnicy wszelkich informacji uzyskanych podczas ich wykonywania. Ewentualne ujawnienie, przekazanie, wykorzystanie, zbycie informacji wymaga pisemnej zgody Kancelarii Prezesa Rady Ministrów albo osoby przez niego upoważnionej.	
IV. Data i podpis osoby składającej oświadczenie	
Data:.....	Podpis:
V. Imię, nazwisko, stanowisko, data i podpis osoby przyjmującej oświadczenie	
Imię i nazwisko:	
Stanowisko:	
Data:.....	Podpis:
Informacje i dane do kontaktów w sprawie danych osobowych Administratorem danych osobowych jest Kancelaria Prezesa Rady Ministrów, Aleje Ujazdowskie 1/3, 00-583, Warszawa, e-mail: ad@kprm.gov.pl . Dane kontaktowe do Inspektora Ochrony Danych: Inspektor Ochrony Danych, Minister Cyfryzacji Aleje Ujazdowskie 1/3, 00-583, Warszawa, e-mail: IOD@mc.gov.pl .	
Informacje dotyczące przetwarzanych danych osobowych Pani/Pana dane osobowe są przetwarzane w celu realizacji umowy nr oraz realizacji innych obowiązków wynikających z przepisów prawa, w tym obowiązku archiwizacji. Podstawą prawną przetwarzania danych osobowych jest zawarcie lub wykonanie umowy, prawnie uzasadnione interesy realizowane przez administratora, a także wypełnienie obowiązku prawnego spoczywającego na administratorze danych osobowych. Dane osobowe będą przetwarzane do czasu istnienia podstawy ich przetwarzania - w przypadku niezbędności danych osobowych do wykonania umowy przez czas jej wykonywania, w przypadku obowiązku prawnego spoczywającego na administratorze danych osobowych do czasu istnienia tego obowiązku. Podanie danych osobowych jest wymogiem wynikającym z umowy, a konsekwencją ich niepodania będzie brak możliwości realizacji umowy.	

Odbiorcy danych osobowych

Dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej. Dane osobowe są przekazywane do podmiotów przetwarzających dane w imieniu administratora danych osobowych, posiadających uprawnienia do ich przetwarzania.

Prawa osoby, której dane dotyczą

Przysługuje Pani/Panu prawo do żądania od administratora danych osobowych:

dostępu do swoich danych osobowych, ich sprostowania, ograniczenia ich przetwarzania.

Żądanie realizacji wyżej wymienionych praw proszę przesłać w formie pisemnej do administratora danych osobowych (adres podany na wstępie, z dopiskiem "Ochrona danych osobowych").

Przysługuje Pani/Panu prawo do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.

Informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu

Pani/Pana dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 7 do Istotnych postanowień umowy

Lista osób wykonujących prace na rzecz KPRM

Dotyczy umowy nr

związanej z realizacją prac

Dane podmiotu zewnętrznego

nazwa firmy:

adres:

REGON:

Lista osób/pracowników podmiotu zewnętrznego wykonujących prace na rzecz KPRM				
Lp.	Imię i nazwisko	Imię ojca	PESEL/numer dowodu albo innego dokumentu tożsamości	Uwagi
1.				
2.				
3.				
4.				
5.				

Imię i nazwisko, nr telefonu do osoby odpowiedzialnej za realizację umowy

(pracownik KPRM/COAR)*

Imię i nazwisko, pieczęć przełożonego osoby odpowiedzialnej za realizację umowy

* Niepotrzebne skreśli

Załącznik nr 3 do SWZ - Formularz oferty.

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa

Nazwa i adres Wykonawcy:

.....

tel.

e-mail

NIP REGON

Nr KRS lub innego rejestru Wykonawcy (jeżeli dotyczy)

Nazwa rejestru i adres strony internetowej bezpłatnej i ogólnodostępnej bazy danych, z
 której zamawiający może samodzielnie pobrać odpis z odpowiedniego rejestru wykonawcy:

.....

Osoba upoważniona do kontaktu:

Imię i nazwisko.....

telefon:.....

e-mail:

Przystępując do prowadzonego przez Kancelarię Prezesa Rady Ministrów postępowania o
 udzielenie zamówienia, którego przedmiotem jest „**Zakup licencji oprogramowania
 niezbędnego do budowy platformy ZPA**” nr PN-22/2021, zobowiązuję się do zrealizowania
 zamówienia zgodnie ze wszystkimi warunkami zawartymi w SWZ oraz w załącznikach.

1. **OŚWIADCZAMY**, że zadeklarowane ceny zawierają wszystkie koszty składające się
 na należyte wykonanie przedmiotu umowy, zobowiązuje się do zrealizowania
 zamówienia zgodnie z wymogami i warunkami określonymi w Specyfikacji Warunków
 Zamówienia i jej załącznikach:

ZREALIZUJĘ(EMY) przedmiotowe zamówienie zgodnie z wymaganiami określonymi w
 SIWZ łącznie za:

całkowitą cenę netto PLN

(słownie: złotych)

plus należny podatek VAT PLN (jeśli dotyczy)

(słownie: złotych)

co stanowi całkowitą cenę brutto PLN

(słownie: złotych)

W tym:

a) **część 1 ZREALIZUJĘ(EMY)** zgodnie z wymaganiami określonymi w SIWZ za:

całkowitą cenę netto PLN

(słownie: złotych)

plus należny podatek VAT PLN (jeśli dotyczy)

(słownie: złotych)

co stanowi całkowitą cenę brutto PLN

(słownie: złotych)

Wyliczoną na podstawie poniżej kalkulacji;

Lp.	Przedmiot zamówienia	Ilość	Cena jedn. netto	Wartość netto w PLN	Wartość podatku VAT w PLN	Wartość brutto w PLN
a.	b.	c.	d.	e.	f.	g.
1.	Oprogramowanie Systemu operacyjnego typu <i>desktop</i> (instalowanych na stacjach roboczych) w pakiecie	50	zł	zł	zł	zł
2.	Licencje dla usług terminalowych w pakiecie	90	zł	zł	zł	zł
3.	Licencje do usług serwerowych w pakiecie	150	zł	zł	zł	zł
4.	Razem :			zł	zł	zł

b) **część 2 ZREALIZUJĘ(EMY)** zgodnie z wymaganiami określonymi w SIWZ za:

całkowitą cenę netto PLN

(słownie: złotych)

plus należny podatek VAT PLN (jeśli dotyczy)

(słownie: złotych)

co stanowi całkowitą cenę brutto PLN

(słownie: złotych)

Wyliczoną na podstawie poniżej kalkulacji;

Lp.	Przedmiot zamówienia	Ilość	Cena jedn. netto	Wartość netto w PLN	Wartość podatku VAT w PLN	Wartość brutto w PLN
a.	b.	c.	d.	e.	f.	g.
1.	Oprogramowanie UTM	1	zł	zł	zł	zł
2.	Oprogramowanie do składowania i analizy logów systemu UTM	1	zł	zł	zł	zł

3.	Razem :	zł	zł	zł
----	---------	---------	---------	---------

c) **część 3** ZREALIZUJĘ(EMY) zgodnie z wymaganiami określonymi w SIWZ za:

całkowitą cenę netto PLN

(słownie: złotych)

plus należny podatek VATPLN (jeśli dotyczy)

(słownie: złotych)

co stanowi całkowitą cenę brutto PLN

(słownie: złotych)

Wyliczoną na podstawie poniżej kalkulacji;

Lp.	Przedmiot zamówienia	Ilość	Cena jedn. netto	Wartość netto w PLN	Wartość podatku VAT w PLN	Wartość brutto w PLN
a.	b.	c.	d.	e.	f.	g.
1.	Oprogramowanie do zarządzania kluczami szyfrującymi	2	zł	zł	zł	zł
2.	Oprogramowanie do realizacji operacji pseudonimizacji	2	zł	zł	zł	zł
3.	Razem :			zł	zł	zł

d) **część 4** ZREALIZUJĘ(EMY) zgodnie z wymaganiami określonymi w SIWZ za:

całkowitą cenę netto PLN

(słownie: złotych)

plus należny podatek VATPLN (jeśli dotyczy)

(słownie: złotych)

co stanowi całkowitą cenę brutto PLN

(słownie: złotych)

Wyliczoną na podstawie poniżej kalkulacji;

Lp.	Przedmiot zamówienia	Ilość	Cena jedn. netto	Wartość netto w PLN	Wartość podatku VAT w PLN	Wartość brutto w PLN
a.	b.	c.	d.	e.	f.	g.
1.	Oprogramowanie wspomagające tworzenie Bazy Wiedzy	1	zł	zł	zł	zł

2.	Oprogramowanie do śledzenia błędów oraz zarządzania projektem	1	zł	zł	zł	zł
3.	Oprogramowanie do repozytorium kodu źródłowego	1	zł	zł	zł	zł
4.	Razem :		zł	zł	zł	zł

e) **część 5 ZREALIZUJĘ(EMY)** zgodnie z wymaganiami określonymi w SIWZ za:

całkowitą cenę netto PLN

(słownie: złotych)

plus należny podatek VAT PLN (jeśli dotyczy)

(słownie: złotych)

co stanowi całkowitą cenę brutto PLN

(słownie: złotych)

Wyliczoną na podstawie poniżej kalkulacji;

Lp.	Przedmiot zamówienia	Ilość	Cena jedn. netto	Wartość netto w PLN	Wartość podatku VAT w PLN	Wartość brutto w PLN
a.	b.	c.	d.	e.	f.	g.
1.	Serwer monitorowania sesji zdalnych i wsparcia zdalnego dla użytkowników	1	zł	zł	zł	zł
2.	System do samodzielnej obsługi haseł	1	zł	zł	zł	zł
3.	Serwer monitorowania SLA	1	zł	zł	zł	zł
4.	Razem :		zł	zł	zł	zł

2. **Dostarczymy** przedmiot zamówienia:

- w części 1** w ciągu dni (maks. 8 dni) od dnia zawarcia umowy;
- w części 2** w ciągu dni (maks. 8 dni) od dnia zawarcia umowy;
- w części 3** w ciągu dni (maks. 8 dni) od dnia zawarcia umowy;
- w części 4** w ciągu dni (maks. 8 dni) od dnia zawarcia umowy;
- w części 5** w ciągu dni (maks. 8 dni) od dnia zawarcia umowy.

3. **Oświadczamy**, że zamówienie zrealizujemy w terminie **36 miesięcy** od dnia zawarcia umowy.

4. **Oświadczamy**, że posiadamy uprawnienia do sprzedaży zaoferowanych produktów, tj. autoryzację producenta do sprzedaży licencji producenta klientom sektora publicznego nr....., wystawione przez:
5. Oświadczamy, że wykazując spełnienie warunków udziału w postępowaniu:
- ☐ nie polegamy na potencjale udostępnionym przez podmiot udostępniający zasoby
 - ☐ polegamy na potencjale udostępnionym przez podmiot udostępniający zasoby. **W związku z powyższym wraz z ofertą składamy zobowiązanie podmiotu udostępniającego zasoby do oddania do dyspozycji niezbędnych zasobów lub inny podmiotowy środek dowodowy.**
6. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i nie wnosimy do niej zastrzeżeń.
7. Jesteśmy związani niniejszą ofertą przez okres wskazany w SWZ.
8. Akceptujemy Projektowane postanowienia umowy (stanowiące załącznik nr 2 do SWZ) i zobowiązujemy się, w przypadku wybrania naszej oferty, do zawarcia umowy o treści określonej w Projektowanych postanowieniach umowy w miejscu i terminie wyznaczonym przez Zamawiającego.
9. Oświadczamy, że informacje i dokumenty, zawarte w pliku (*wypełnić, jeśli dotyczy*), tj. następujące elementy oferty:, stanowią tajemnicę przedsiębiorstwa* w rozumieniu art. 11 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji i zastrzegamy, że nie mogą być udostępnione. Elementy oferty, o których mowa powyżej, zostały złożone w osobnym pliku i oznaczone „Załącznik stanowiący tajemnicę przedsiębiorstwa” a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP).
10. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[†]
11. Akceptujemy postanowienia: Regulaminu korzystania z systemu miniPortal i instrukcji użytkownika systemu miniPortal-ePUAP[‡]

* w przypadku dokonania takiego zastrzeżenia, należy wykazać w odniesieniu do każdej z zastrzeżonych informacji:

- że ma ona charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub inny posiadający wartość gospodarczą,
- która jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie jest powszechnie znana osobom zwykle zajmującym się tym rodzajem informacji albo nie jest łatwo dostępna dla takich osób,
- uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

[†] W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (prosimy o usunięcie treści oświadczenia np. przez jego wykreślenie).

[‡] Z zapisami regulaminu i instrukcji można zapoznać się w BIP-ie zamawiającego w zakładce Informacja dla wykonawców dotycząca postępowań przeprowadzanych przy użyciu środków komunikacji elektronicznej lub pod adresem <https://miniportal.uzp.gov.pl/WarunkiUslugi.aspx>, https://www.uzp.gov.pl/__data/assets/pdf_file/0030/37596/Instrukcja-Uzytkownika-Systemu-miniPortal-ePUAP.pdf

12. Numer rachunku bankowego, na który Zamawiający winien zwrócić wadium wniesione w pieniądzu (w przypadku, jeśli jest on inny niż nr rachunku, z którego wniesione zostało wadium):

13. Oświadczenie składane przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy):

Oświadczamy, że część zamówienia, co do której zamawiający wymagał wykazania się doświadczeniem opisanym w warunku udziału w postępowaniu, zostanie wykonana przez ten z podmiotów wspólnie ubiegających się o zamówienie, którego doświadczenie zostało wykazane na potwierdzenie spełnienia tego warunku udziału w postępowaniu.

Podział zadań w ramach wykonawców występujących wspólnie przedstawia poniższa tabela:

Zadanie	Podmiot realizujący zadanie

14. Do Formularza oferty dołączam następujące załączniki:

1. Oświadczenie w formie JEDZ Wykonawcy;
2. Oświadczenie w formie JEDZ Wykonawcy składającego wspólną ofertę (jeżeli dotyczy);
3. Oświadczenie o udostępnieniu potencjału przez podmiot zewnętrzny (jeżeli dotyczy);
4. Oświadczenie w formie JEDZ Podmiotu udostępniającego potencjał (jeżeli dotyczy);
5. Pełnomocnictwo do reprezentowania wykonawcy (jeżeli dotyczy);
6. Pełnomocnictwo do reprezentowania wykonawców wspólnie ubiegających się o zamówienie (jeżeli dotyczy);
7. Przedmiotowe środki dowodowe (jeżeli dotyczy);
8. Dowód wniesienia wadium (jeżeli dotyczy);
9. Uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa (jeżeli dotyczy);
10.
11.

**kwalfikowany podpis elektroniczny osoby (osób)
upoważnionej do reprezentowania Wykonawcy**

Załącznik nr 4 do SWZ - Oświadczenie o udostępnieniu potencjału.**Zobowiązanie innego podmiotu do oddania
do dyspozycji wykonawcy niezbędnych zasobów
(składane wraz z ofertą – jeżeli dotyczy)**

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego przez Kancelarię Prezesa Rady Ministrów na „**Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA**”, post nr - PN-22/2021

DANE PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY:

Nazwa /Firma:

.....

Adres:

telefon:

e-mail:

Będąc upoważnionym do reprezentowania wskazanego podmiotu, niniejszym oświadczam, że oddaję do dyspozycji Wykonawcy:

Nazwa /Firma Wykonawcy:

.....

Adres:

określone poniżej zasoby, przez okres korzystania z nich przy wykonaniu powołanego zamówienia i oświadczam, że stosunek łączący mnie z Wykonawcą gwarantuje rzeczywisty dostęp Wykonawcy do tych zasobów:

1. Określenie zakresu zasobów dostępnych Wykonawcy od podmiotu udostępniającego zasoby:

.....

.....

2. Sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia:

.....

.....

***kwalifikowany podpis elektroniczny
osoby (osób) upoważnionej do
reprezentowania podmiotu
udostępniającego zasoby***

Załącznik nr 5 do SWZ - Oświadczenie o aktualności danych zawartych w JEDZ.

Oświadczenie o aktualności danych zawartych w oświadczeniu JEDZ (składane na wezwanie Zamawiającego)

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego przez Kancelarię Prezesa Rady Ministrów na „**Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA**”, post nr - PN-22/2021

Będąc upoważnionym do reprezentacji Wykonawcy:

Nazwa/firma Wykonawcy

Adres,

niniejszym oświadczam, że pozostają aktualne informacje zawarte w oświadczeniu JEDZ złożonym w powołanym postępowaniu, w zakresie podstaw wykluczenia z postępowania wskazanych przez Zamawiającego, o których mowa w:

1. art. 108 ust. 1 pkt 3 ustawy pzp
2. art. 108 ust. 1 pkt 4 ustawy pzp, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego
3. art. 108 ust. 1 pkt 5 ustawy dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji
4. art. 108 ust. 1 pkt 6 ustawy pzp

***kwalifikowany podpis elektroniczny
osoby (osób) upoważnionej do
reprezentowania Wykonawcy***

Załącznik nr 6 do SWZ - Oświadczenie o braku przynależności do grupy kapitałowej.

Kancelaria Prezesa Rady
Ministrów

Al. Ujazdowskie 1/3

00-583 Warszawa

Oświadczenie

(składane na wezwanie Zamawiającego)

o przynależności lub braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę bądź ofertę częściową w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego na „**Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA**”, post nr - PN-22/2021

Niniejszym oświadczam/oświadczamy w imieniu:

....., że:

nazwa Wykonawcy, adres

- ☐ **nie należą** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę bądź ofertę częściową w niniejszym postępowaniu,
- ☐ **należą** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), do której należy następujący wykonawca/cy, którzy złożyli odrębną ofertę bądź ofertę częściową w tym postępowaniu:

.....

.....

.....

W związku z powyższym do oświadczenia załączam dokumenty lub informacje potwierdzające przygotowanie oferty, oferty częściowej w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

*kwalfikowany podpis elektroniczny
osoby (osób) upoważnionej do
reprezentowania Wykonawcy*

Załącznik nr 7 do SWZ – Wykaz zrealizowanych dostaw.**Wykaz zrealizowanych dostaw**

Przystępując do prowadzonego przez Kancelarię Prezesa Rady Ministrów postępowania o udzielenie zamówienia na „**Zakup licencji oprogramowania niezbędnego do budowy platformy ZPA**”, dla części **1, 2, 3, 4, 5** (niepotrzebne skreślić) post nr - PN-22/2021, składam Wykaz zrealizowanych dostaw:

Lp.	Podmiot, na którego rzecz wykonane zostało zamówienie	Wykonawca	Okres realizacji***)		Przedmiot zamówienia (usług), <u>pozwalający na stwierdzenie</u> , czy został spełniony postawiony warunek, określony w rozdziale VII. 1.2.3 SWZ	Wartość brutto zł ***)
			Początek (dd-mm-rrrr)	Zakończenie (dd-mm-rrrr)		
					1. Przedmiot zamówienia	
					2. Zakres zadań wchodzących w zakres zrealizowanego zamówienia związanych z przedmiotowym zamówieniem:	
					3. Rodzaj doświadczenia: WŁASNE*)/ INNYCH PODMIOTÓW*), **).	
					1. Przedmiot zamówienia	
					2 Zakres zadań wchodzących w zakres zrealizowanego zamówienia związanych z przedmiotowym zamówieniem:	
					3. Rodzaj doświadczenia: WŁASNE*)/ INNYCH PODMIOTÓW*), **).	
					1. Przedmiot zamówienia	
					2 Zakres zadań wchodzących w zakres zrealizowanego zamówienia związanych z przedmiotowym zamówieniem:	
					3. Rodzaj doświadczenia: WŁASNE*)/ INNYCH PODMIOTÓW*), **).	

Uwaga: Zamawiający wymaga, aby Wykonawca załączył wykaz wraz z dowodami potwierdzającymi należyte wykonanie dostaw.

*) niepotrzebne skreślić;

**) w przypadku wskazania doświadczenia innych podmiotów, Wykonawca winien udowodnić, iż będzie dysponował tymi zasobami, w szczególności przedstawiając zobowiązanie tych podmiotów do jego udostępnienia;

**) zgodnie z warunkiem postawionym w SWZ.

***kwalfikowany podpis elektroniczny osoby (osób)
upoważnionej do reprezentowania Wykonawcy***

Załącznik nr 9 do SWZ - Oświadczenie o spełnieniu warunków udziału w postępowaniu i braku podstaw do wykluczenia z postępowania, w formie JEDZ.