UMOWA nr .....

zawarta w dniu ..... roku pomiędzy:

Skarbem Państwa - Kasą Rolniczego Ubezpieczenia Społecznego, z siedzibą: 00-608 Warszawa, Al. Niepodległości 190, NIP 526-00-13-054, REGON 012513262 reprezentowaną przez:

.....Biura Informatyki i Telekomunikacji,

na podstawie pełnomocnictwa Prezesa Kasy Rolniczego Ubezpieczenia Społecznego nr .....

z dnia .....

zwanym w treści Umowy „Zamawiającym",

a

.....wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod nr KRS, NIP:, REGON

reprezentowaną przez:

.....

zwanym w treści Umowy „Wykonawcą".

Zamawiający i Wykonawca zwani łącznie w treści Umowy „Stronami".

W wyniku przeprowadzenia uproszczonego postępowania do którego na podstawie art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129) nie stosuje się przepisów niniejszej ustawy, zawarto umowę następującej treści:

§ 1

Przedmiot Umowy

1. Przedmiotem zamówienia jest „Zakup usługi dostępu do oprogramowania w modelu Software-as-a-Service (SaaS) wspierającego obszar analizy ryzyka w ramach Kontroli Zarządczej, Bezpieczeństwa Informacji oraz Ochrony Danych Osobowych".
2. Szczegółowy opis i zakres przedmiotu zamówienia stanowi Załącznik nr 2 do niniejszej Umowy.
3. Wykonawca udostępni w ciągu 5 dni od podpisania niniejszej Umowy login i hasła dostępu do oprogramowania będącego przedmiotem niniejszej Umowy.

§ 2

Wynagrodzenie

1. Wynagrodzenie całkowite Wykonawcy za realizację usług nie przekroczy kwoty ..... zł netto (słownie złotych: .....zł 00/100) plus podatek VAT w wysokości 23%, co stanowi kwotę ..... zł brutto (słownie złotych..... zł 00/100).

2. Podstawą do zapłaty faktury VAT będzie oryginał Protokołu odbioru prac podpisany bez zastrzeżeń przez upoważnionych przedstawicieli Stron. Wzór Protokołu stanowi Załącznik nr 1 do Umowy.
3. Zapłata wynagrodzenia za wykonanie przedmiotu umowy nastąpi przelewem na rachunek bankowy Wykonawcy, wskazany w fakturze VAT, w terminie 14 dni od daty dostarczenia do siedziby Zamawiającego poprawnie wystawionego oryginału faktury VAT wraz z oryginałem Protokołu odbioru prac podpisanym bez zastrzeżeń przez upoważnionych przedstawicieli Stron.
4. Za dzień płatności przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego należną Wykonawcy kwotą.
5. Zamawiający nie wyraża zgody na cesję wierzytelności wynikających z umowy.
6. Wykonawca zobowiązany jest zamieścić na fakturze adnotację „mechanizm podzielonej płatności", jeżeli dokumentuje ona czynność podlegającą temu mechanizmowi.

(dotyczy przypadku gdy Wykonawca będzie korzystał z przesyłania faktur VAT za pośrednictwem poczty elektronicznej)

7. Zamawiający oświadcza, że zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. z 2021 r. poz. 685), wyraża zgodę na wystawienie przez Wykonawcę faktury VAT, korekt faktury VAT oraz ich duplikatów w formie elektronicznej (w formacie PDF) i przesyłanie ich za pośrednictwem poczty elektronicznej na adres: bf@krus.gov.pl. Wykonawca oświadcza, że adresem z którego będą wysyłane faktury VAT, korekty faktury VAT oraz ich duplikaty, jest następujący adres: .....

§ 3

Okres obowiązywania Umowy

Wykonawca będzie świadczył usługę dostępu do oprogramowania przez okres 12 miesięcy kalendarzowych, od daty zawarcia Umowy, z uwzględnieniem zapisu § 1 ust. 3 niniejszej Umowy.

§ 4

Zasady poufności

1. Wszelkie informacje oraz dokumenty uzyskane przez Wykonawcę w związku z realizacją przedmiotu Umowy, jak również wykonanego przedmiotu Umowy stanowią informacje poufne. Bez uprzedniej pisemnej zgody Zamawiającego, Wykonawca nie może przekazywać, publikować, ujawniać ani udzielać osobom trzecim ww. informacji oraz dokumentów, ani też wykorzystywać tychże informacji i dokumentów w interesie własnym lub osób trzecich.
2. Strony zobowiązują się do zachowania w ścisłej tajemnicy wszelkich informacji uzyskanych w związku z wykonaniem niniejszej Umowy, w szczególności w czasie obowiązywania niniejszej Umowy oraz przez czas nieograniczony po jej wygaśnięciu lub rozwiązaniu.
3. Strony zobowiązują się nie kopiować, nie powielać, ani w jakikolwiek sposób nie rozpowszechniać jakichkolwiek informacji dotyczących drugiej Strony, jej interesów, finansów lub działań, włącznie

z wszelkimi informacjami technicznymi, finansowymi i tajemnicą przedsiębiorstwa, niezależnie od źródeł tych informacji, chyba, że taka informacja jest już powszechnie znana bez naruszania postanowień Umowy lub musi być ujawniona uprawnionemu organowi lub osobom działającym w ramach obowiązującego prawa.

4. W przypadku powierzenia przez Wykonawcę innym podmiotom wykonania wszystkich lub niektórych czynności związanych z realizacją przedmiotu Umowy, Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez te podmioty.
5. Wykonawca zobowiązuje się zwrócić Zamawiającemu i trwale usunąć wszelkie materiały otrzymane od niego w związku z realizacją Umowy po jej zakończeniu.
6. Wykonawca oświadcza, że jest podmiotem prowadzącym działalność gospodarczą, niepowiązanym kapitałowo, organizacyjnie ani na podstawie odrębnych umów z firmami świadczącymi usługi telekomunikacyjne na terenie Polski i Unii Europejskiej.

§ 5

Kary umowne

1. Wykonawca zapłaci Zamawiającemu karę w wysokości 0,5% całkowitej wartości brutto Umowy, określonej w § 2 ust. 1 za każdy dzień opóźnienia w wykonaniu przedmiotu Umowy.
2. W przypadku odstąpienia od realizacji Umowy wskutek okoliczności zależnych od Wykonawcy, Wykonawca zapłaci Zamawiającemu karę w wysokości 10% całkowitej wartości brutto Umowy, określonej w § 2 ust. 1.
3. Za naruszenie obowiązku zachowania poufności, o których mowa w § 4, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 50% całkowitej wartości brutto Umowy wymienionej w § 2 ust. 1, za każdorazowe naruszenie zachowania poufności.
4. Zamawiający zastrzega sobie prawo do dochodzenia na zasadach ogólnych odszkodowania ponad wysokość kar umownych.

§ 6

Postanowienia końcowe

1. W sprawach nieuregulowanych w Umowie mają zastosowanie odpowiednie przepisy Kodeksu cywilnego oraz inne przepisy mające związek z realizacją umowy.
2. Wszelkie ewentualne spory mogące wynikać przy realizacji niniejszej umowy będą podlegały rozstrzygnięciu przez sąd właściwy miejscowo dla siedziby Zamawiającego.
3. Wszelkie zmiany i uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Wykaz załączników:

Załącznik nr 1 – Protokół odbioru;

Załącznik nr 2 - Szczegółowy opis i zakres przedmiotu zamówienia.

ZAMAWIAJĄCY: **WYKONAWCA:**

Załącznik nr 1

do Umowy nr .....

z dn. .....

Warszawa, dn. .....

Protokół odbioru

W dniu ..... w ramach realizacji umowy nr ..... z dn. .....2020 r., w siedzibie Centrali KRUS w Warszawie Al. Niepodległości 190, dokonano odbioru wykonania prac: .....
.....

Niniejszy Protokół odbioru jest podstawą do zapłaty faktury za wykonaną usługę.

Prace zostały przyjęte/nieprzyjęte* - uwagi:
.....
.....
.....
.....

ZAMAWIAJĄCY WYKONAWCA

Załącznik nr 2

do Umowy nr .....

z dn. .....

Szczegółowy opis i zakres przedmiotu zamówienia

I. Przedmiot zamówienia

1. Zakup usługi dostępu do oprogramowania w modelu Software-as-a-Service (SaaS) wspierającego obszar analizy ryzyka w ramach Kontroli Zarządczej, Bezpieczeństwa Informacji oraz Ochrony Danych Osobowych.
2. Przeprowadzenie instruktażu stanowiskowego dla użytkowników.
3. Zapewnienie wsparcia technicznego.

II. Założenia podstawowe

1. Liczba użytkowników systemu – 5 szt.
2. Cała niezbędna infrastruktura i oprogramowanie niezbędne do świadczenia usługi dostarcza Zamawiający.
3. Usługa dostępu w języku polskim.
4. Dostawca usługi powinien posiadać certyfikat ISO 27001 oraz ISO 22301.

III. Zakres metodyczny

W ramach podstawowych funkcjonalności dostarczona usługa musi wspierać zarządzanie ryzykiem:

- bezpieczeństwa informacji i ciągłości działania,
- operacyjnym,
- strategicznym,
- ochrony danych osobowych,
- kontroli zarządczej.

Usługa ma umożliwić realizacje procesu:

1. szacowania ryzyka,
2. postępowania z ryzykiem,
3. akceptowanie ryzyka,
4. monitorowanie ryzyka,
5. informowania o ryzyku,
6. zgłaszania incydentów,
7. oceny efektywności stosowanych zabezpieczeń,
8. prowadzenia rejestru czynności przetwarzania,
9. prowadzenia kategorii przetwarzania,
10. raportowania.

IV. Zakres funkcjonalny

Wymagania funkcjonalne dla oprogramowania w modelu Software-as-a-Service (SaaS):

1. Interfejs użytkownika rozwiązania powinien być w całości oparty o protokół http, wiec po stronie standardowych użytkowników wymagana będzie jedynie przeglądarka internetowa.
2. Rozwiązanie powinno umożliwiać definiowanie powiadomień e-mail nt. oczekujących zadań, akcji jakie należy podjąć, upływających terminów (powiadomienie powinno być wysłane do określonych użytkowników).
3. Panel administracyjny pozwalający samodzielnie parametryzować poszczególne funkcjonalności, takie jak: dodawanie/edycja pól, dodawanie/edycja raportów, parametryzacja słowników aplikacji, parametryzacja workflow, parametryzacja interfejsów do pobierania danych.
4. Rozwiązanie musi umożliwiać zarządzanie uprawnieniami w oparciu o role wynikające z procesu zarządzania ryzykiem.
5. Rozwiązanie powinno umożliwiać definiowanie poszczególnych etapów procesu zarządzania ryzykiem oraz ich parametrów (np.: różnych rodzajów skutków ryzyka: operacyjnych, wizerunkowych, zgodności) czasu ich wykonywania, powiązań miedzy nimi, ról potencjalnych uczestników).
6. Rozwiązanie powinno zapewnić możliwość zdefiniowania ścieżki akceptacji pozwalającej na procesowanie (akceptacja/brak akceptacji).
7. Rozwiązanie powinno zapewnić mechanizmy monitorowania i powiadomień (z możliwością wyboru przez użytkownika ustawień co do cyklu powiadomień), np.: powiadomienia o przedłużającym się zadaniu.
8. Rozwiązanie powinno umożliwiać dodawanie komentarzy osób biorących udział w jego obsłudze w formularzu dotyczącym tego ryzyka.
9. Rozwiązanie powinno umożliwiać przechowywanie dodatkowej dokumentacji elektronicznej dotyczącej ryzyka w formie plików np.: MS Excel, MS Word, Adobe Acrobat PDF, CSV, JPG, HTML.
10. Rozwiązanie powinno umożliwiać przepisywanie skutków ryzyka do różnych jednostek organizacyjnych.
11. Rozwiązanie powinno posiadać możliwość tworzenia słowników, bibliotek.
12. Powinna być możliwość powiązania ryzyk ze zdarzeniami operacyjnymi zarejesrtowanymi w rozwiązaniu.
13. Rozwiązanie powinno umożliwić dowolne definiowanie formularzy samooceny ryzyka dla poszczególnych grup użytkowników lub obszarów działalności.
14. Rozwiązanie powinno umożliwić generowanie raportów dostosowanych do potrzeb poszczególnych grup użytkowników (poziom operacyjny, poziom kierowniczy), np.: zestawienie miesięczne liczby ryzyk, raporty statusu planów postepowania z ryzykiem, ryzyka

w danym obszarze organizacji, dotyczące danego procesu, aktywa. Powinna istnieć możliwość eksportu takich raportów w formatach doc/docx, xls, pdf.

15. Rozwiązanie powinno umożliwiać wysyłanie powiadomienia o gotowym do pobrania raporcie oczekującym w aplikacji lub wysłania tak wygenerowanego pliku na wskazany (jeden lub kilka) adres e-mail.
16. Rozwiązanie powinno zapewnić możliwość prowadzenia analiz ryzyka bezpieczeństwa informacji w zakresie procesów (jako część SZBI zgodnie z ISO 27001), indywidulanych produktów IT, infrastruktury IT.
17. Rozwiązanie powinno umożliwiać przeprowadzenie analizy BIA zgodnej z wymogami normy ISO 22301.
18. Rozwiązanie powinno umożliwiać realizację analiz DPIA wymaganych Rozporządzeniem RODO i Ustawą o ochronie danych osobowych.
19. Rozwiązanie powinno umożliwić porównanie stanu i poziomu ryzyk w czasie (np.: archiwizacja ryzyk zamkniętych w danym roku, archiwizacja stanu na dany dzień).
20. Rozwiązanie powinno zapewniać możliwość zdefiniowania różnych sposobów postępowania z ryzykiem.
21. Kiedy poziom jest nieakceptowalny, proce analizy ryzyka powinien zapewniać możliwość opracowania planu postępowania z ryzykiem, obejmującego działania mitygujące z automatycznym lub ręcznym szacowaniem wpływu na poziom ryzyka.
22. Rozwiązanie powinno zapewniać możliwość monitorowania planu postępowania z ryzykiem.
23. Model analizy ryzyka powinien pozwalać na ocenę ryzyka z perspektywy atrybutów bezpieczeństwa informacji: poufność, integralność, dostępność i musi gwarantować rozliczalność.
24. Rozwiązanie powinno umożliwiać gromadzenie informacji na temat wdrożonych mechanizmów kontrolnych, ich powiązania z poszczególnymi wymaganiami standardów i przepisów (np.: ISO 27001, ISO 22301, RODO).
25. Rozwiązanie powinno umożliwić generowanie raportu, deklaracji zgodności z wymaganiami standardów i przepisów na podstawie informacji o wdrożonych mechanizmach kontrolnych.
26. Rozwiązanie musi umożliwiać monitorowania i raportowanie skuteczności zabezpieczeń.

Dodatkowe wymagania:

1. Docelowo system musi dawać możliwość rozszerzenia liczby użytkowników. Program musi umożliwiać indywidualne nadawanie uprawnień użytkownikom do każdego z modułów.
2. Zapewnienie dostępności systemu w trybie 24/7.
3. Konieczne jest wsparcie techniczne oprogramowania dostawcy systemu.
4. Udostepnienie dokumentacji dostarczonego oprogramowania w modelu Software-as-a-Service (SaaS).

5. Zapewnienie aktualizacji oprogramowania dostarczonego oprogramowania w modelu Software-as-a-Service (SaaS).
6. Wykonywanie kopii zapasowej niezbędnej do zachowania ciągłości świadczonej usługi.
7. Kryteriów SLA dla świadczonej usługi:
    a. błąd krytyczny - rozumiany jako niedostępność kluczowych funkcji oprogramowania musi być usunięty w ciągu : 3 dni roboczych,
    b. błąd wysoki - rozumiany jako niedostępność innych funkcji oprogramowania musi być usunięty w ciągu: 7 dni roboczych.
8. Gwarantowane parametry świadczonej usługi:
    a. Dostępność usługi – 99,8% w trybie rocznym,
    b. Maksymalna długość przerwy konserwacyjnej – 8h w miesiącu.

V. Zakres wdrożenia

1. W ramach wdrożenia Wykonawca powinien:

1.1 Uruchomić i udostępnić Zamawiającemu usługę od dnia.....

1.2 Utrzymać usługę w ciągu roku od protokolarnego jej odebrania.

1.3 Zapewnić wsparcie techniczne usługi w ciągu roku od protokolarnego jej odbioru.

1.4 Przeszkolić wszystkich użytkowników z obsługi oprogramowania i dostępnych funkcji.

1.5 Przenieś do oprogramowania metodykę analizy ryzyka w zakresie ISO 27001 stosowaną w KRUS.

1.6 Dostarczyć w wersji elektronicznej:

- dokumentację użytkownika – podręcznik użytkownika,
- dokumentację administratora – podręcznik administratora.