Specyfikacja Warunków Zamówienia

Dostawa i wdrożenie oprogramowania klasy XDR dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie

Nr zamówienia: DZiK-DZP.2921.41.2024

Wspólny Słownik Zamówień CPV: 48000000-8

Postępowanie będzie prowadzone w trybie podstawowym o jakim stanowi art. 275 pkt 1) ustawy Pzp. Zgodnie z art. 61 ust. 1 oraz art. 63 ust. 2 ustawy Pzp komunikacja w niniejszym postępowaniu odbywa się **wyłącznie przy użyciu środków komunikacji elektronicznej.**

Załączniki:

1. Formularz ofertowy - Załącznik nr 1 do SWZ
2. Oświadczenie Wykonawcy - Załącznik nr 2 do SWZ
3. Oświadczenie Wykonawcy o przynależności/ bądź braku przynależności do grupy kapitałowej – załącznik nr 3 do SWZ
4. Projektowane postanowienia umowy - Załącznik nr 4 do SWZ

Rozdział 1

Nazwa, adres i dane kontaktowe Zamawiającego, tryb udzielenia zamówienia publicznego, informacje o procedurze, adres strony prowadzonego postępowania oraz miejsce publikacji ogłoszenia o zamówieniu i pozostałych dokumentów zamówienia

1. Dane kontaktowe Zamawiającego:

UNIWERSYTET ROLNICZY im. Hugona Kołłątaja w Krakowie

z siedzibą pod adresem: 31-120 Kraków, al. Adama Mickiewicza 21

NIP: 675-000-21-18, REGON: 000001815

tel. +48 12 662-42-22

http: www.urk.edu.pl

e-mail: paulina.zurek@urk.edu.pl

strona internetowa prowadzonego postępowania:

https://platformazakupowa.pl/pn/urk/proceedings

2. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w **trybie podstawowym** na podstwie **art. 275 pkt 1) ustawy Pzp**, którego wartość nie przekracza kwoty, o której mowa w art. 3 ust. 1 pkt 1) ustawy Pzp.
3. Zamawiający informuje, iż wszelkie zmiany/wyjaśniania/modyfikacje, bądź dodatkowe informacje/zawiadomienia, a także inne dokumenty zamówienia bezpośrednio związane z niniejszym postępowaniem udostępniane będą w Profilu Nabywcy Zamawiającego pod adresem: https://platformazakupowa.pl/pn/urk/proceedings

Rozdział 2

1. Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania klasy XDR (Extended Endpoint Detection and Response). Zaawansowanego oprogramowania ochrony stacji roboczych, serwerów i urządzeń mobilnych które zapewnia m.in.:

   1) funkcjonalność ochrony antywirusowej

   2) aktywną ochronę stacji końcowych przed działaniem złośliwego oprogramowania i innych zaawansowanych cyberzagrożeń

   3) możliwość gromadzenia informacji o zdarzeniach oraz rozbudowane funkcje reakcji na incydenty

   4) detekcji zagrożeń, identyfikacji działań cyberprzestępców oraz zdarzeń z kategorii APT (Advanced Persistent Threats)

5) aktywnej reakcji i odpowiedzi na wykryte zdarzenie oraz incydenty
6) realizacji działań proaktywnych w tym aktywnego wyszukiwania intruzów

w infrastrukturze informatycznej.

2. Zamawiający nie dokonuje podziału zamówienia na części. Tym samym zamawiający nie dopuszcza składanie ofert częściowych, o których mowa w art. 7 pkt 15 ustawy Pzp. Brak podziału nie ogranicza konkurencji na rynku ani nie utrudnia dostępności do zamówienia. Zamawiający chce zakupić jedno kompletne oprogramowanie wraz z wdrożeniem. Podział zamówienia na części wiązałby się ze zwiększeniem kosztów dla Zamawiającego, trudnościami technicznymi oraz koordynacją działań różnych Wykonawców realizujących poszczególne elementy zamówienia. Taki podział mógłby zagrozić właściwemu wykonaniu zamówienia.

Szczegółowy opis przedmiotu zamówienia

EDR (Endpoint Detection and Response) umożliwia monitorowanie stacji końcowych pod kątem podejrzanego zachowania i rejestrować każdą aktywność czy zdarzenie. System następnie koreluje te informacje w celu wykrycia występowania zaawansowanych zagrożeń, gdzie następnie uruchamia zautomatyzowane działania mające na celu zatrzymanie zagrożenia.

XDR (Extended Endpoint Detection and Response) to rozwinięcie systemu EDR. Podczas gdy EDR zbiera i koreluje dane z stacji końcowych, XDR rozszerza ten zakres poza stacje końcowe, zapewniając wykrywanie i analizę informacji także w sieciach, serwerach, chmurze, SIEM i wielu innych.

APT (Advanced Persistent Threats) - w ataku APT aktor wykorzystuje najbardziej wyrafinowane taktyki i technologie w celu penetracji sieci o wysokim profilu. Celem ataków APT jest pozostanie w ukryciu i eksploracja sieci, pozostając niewykrytym przez tygodnie, miesiące, a nawet lata.

AMSI (Antimalware Scan Interface) - to wbudowany w system Windows mechanizm do zaawansowanej ochrony przed złośliwym oprogramowaniem, używany między innymi do sprawdzania złośliwych skryptów.

Agent – to wszystkie aplikacje dostarczanego oprogramowania które muszą być zainstalowane na stacji końcowej.

Stacja robocza – komputery stacjonarne oraz laptopy

Stacja końcowa - dowolne urządzenie (stacja robocza / serwer / urządzenie mobilne) z dowolnym systemem operacyjnym wymienionym w Wymaganiach Ogólne (WO60) na którym jest zainstalowany agent oferowanego oprogramowania.

Systemy Microsoft Windows - rodzina systemów operacyjnych aktualnie wspieranych i stworzonych przez firmę Microsoft. Rodzina systemów operacyjnych działająca na serwerach oraz na stacjach roboczych.

MacOS - rodzina systemów operacyjnych aktualnie wspieranych i stworzonych przez firmę Apple Inc. Rodzina systemów operacyjnych działająca na stacjach roboczych.

Urządzenie mobilne - telefony komórkowe, smartfony, tablety wyposażone w system operacyjny iOS lub Android.

Konsola centralnego zarządzania – serwer lub serwery na których odbywa się zarządzanie wszystkimi agentami zainstalowanymi na stacjach końcowych.

Etapy realizacji zamówienia

Etap I – „Dostawa oprogramowania”

Etap II – „Wdrożenie oprogramowania”

Etap III – „Dokumentacja powykonawcza i szkolenia”

Wymagania dla dostarczonego oprogramowania – Etap I - „Dostawa Oprogramowania”

Wymagania ogólne	
WO1	Należy dostarczyć 3000 licencji na urządzenia wykorzystywane przez Zamawiającego. Rozwiązanie musi zapewnić możliwość używania oprogramowania na co najmniej: 2770 stacjach roboczych, 200 serwerach, 30 urządzeniach mobilnych.
WO2	Udzielone licencje zezwalać będą na swobodne przenoszenie oprogramowania pomiędzy tego samego typu stacjami końcowymi (pomiędzy stacjami roboczymi, pomiędzy serwerami oraz pomiędzy urządzeniami mobilnymi).
WO3	Udzielone licencje będą licencjami terminowymi obowiązującymi przez 3 lata, od daty podpisania protokołu odbioru etapu II, ale nie wcześniej niż od 20 czerwca 2024 r.

WO4	Licencja powinna umożliwiać działanie zakupionego oprogramowania na czas wdrożenia (tj. od dnia podpisania umowy do podpisania protokołu odbioru etapu II), aby Zamawiający nie pozostał bez ochrony stacji końcowych przy użyciu obecnie posiadanego oprogramowania lub oprogramowania zaoferowanego przez Wykonawcę. Czas ten nie wlicza się w czas ważności licencji określony w punkcie WO3.
WO5	Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Zamawiającemu nie może być zaoferowane oprogramowanie, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
WO6	Oferowane oprogramowanie w dniu składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub ze sprzedaży.
WO7	Oferowane oprogramowanie musi umożliwiać zarządzanie stacjami końcowymi za pomocą mechanizmu konsoli centralnego zarządzania.
WO8	Wszystkie moduły oferowanego rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich elementów oraz prawidłowego funkcjonowania.
WO9	Oprogramowanie musi pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych w Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania.
WO10	Zamawiający wymaga aby Wykonawca dostarczył najnowsze wersje oprogramowania i umożliwił jego aktualizacje w każdym momencie użytkowania objętym zakupioną licencją. Możliwość aktualizacji dotyczy zarówno konsoli centralnego zarządzania jak i agentów zainstalowanych na stacjach końcowych, oraz każdego innego składowego elementu nabywanego oprogramowania umożliwiającego jego poprawne funkcjonowanie.

WO11	Wykonawca dostarczy Zamawiającemu wszelkie dane niezbędne do prawidłowego uruchomienia i korzystania z Oprogramowania (np. klucze licencyjne, instalatory). W szczególności dokumentację przedwdrożeniową zawierającą pełną informację o wymaganiach sprzętowych oraz sieciowych niezbędnych do prawidłowego działania oferowanego oprogramowania. Jeśli zajdzie taka konieczność Zamawiający będzie mógł zwracać się o nieodpłatne udzielenie takich informacji przez cały okres ważności licencji na dostarczane oprogramowanie.
WO12	Zamawiający oczekuje, że konsola centralnego zarządzania oprogramowaniem na stacjach końcowych zostanie zainstalowana na serwerach Zamawiającego lub jeżeli nie ma takiej możliwości będą to serwery producenta dostarczanego oprogramowania. Serwery muszą fizycznie znajdować się na terenie Unii Europejskiej. Przerwanie dostępu do konsoli centralnego zarządzania nie powoduje przerwania ochrony stacji końcowych.
WO13	W przypadku konsoli centralnego zarządzania zainstalowanej w na serwerach producenta, miesięczna dostępność konsoli centralnego zarządzania musi wynosić nie mniej niż 99,5%.
WO14	W przypadku instalacji na serwerach Zamawiającego rozwiązanie musi dawać możliwość instalacji zarówno na serwerze fizycznym jak i w postaci maszyny wirtualnej. Rozwiązanie musi wspierać co najmniej następujące środowiska wirtualizacji Microsoft Hyper-V, Vmware.
WO15	Zamawiający wymaga aby komunikacja agenta zainstalowanego na stacjach końcowych z serwerami producenta oraz z konsolą centralnego zarządzania odbywała się szyfrowanym protokołem, a wszystkie dane zebrane były przechowywane i przetwarzane na obszarze Unii Europejskiej.
WO16	Oferowane rozwiązanie musiało być poddane ewaluacji przez MITRE ENGENUITY, ATT&CK Evaluations i musiało być oceniane przynajmniej w dwóch z trzech ewaluacji: • Turla (2023 r.) • Wizard Spider + Sandworm (2022 r.) • Carbanak+FIN7 (2021 r.)

WO17	Oferowane rozwiązanie musiało brać udział w teście skuteczności ewaluacji MITRE ENGENUITY, ATT&CK w ewaluacji Turla (2023) i uzyskać mniej niż 25 % braku wykryć (none detections) oraz brak udziału (Not applicable) w scenariusz Carbon i Snake (co oznacza relatywnie niską wykrywalność etapów ataku „substeps") W scenariuszu Carbon istnieje 76 etapów ataku (substeps), w scenariuszu Snake istnieje 67 etapów ataku, łącznie 143 etapy ataku (substeps). M – liczba procent nie wykrytych etapów ataku Le – maksymalna liczba wszystkich etapów ataku (substeps) Lb – suma etapów ataku (substeps) 'None' i 'Not applicable' badanej oferty M = Lb / Le * 100%
WO18	Producent oferowanego systemu posiada certyfikat ISO 27001 lub SOC 2 type 2.
WO19	Dostarczone oprogramowanie musi posiadać interfejs w języku polskim lub angielskim.
WO20	Dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczonego za pomocą aktualnie zalecanego protokołu SSL/TLS (HTTPS).
WO21	Konsola centralnego zarządzania musi być wspierana przez następujące przeglądarki: Microsoft Edge, Mozilla Firefox, Google Chrome, w wersji aktualnej na dzień podpisania umowy.
WO22	Dostarczone oprogramowanie musi posiadać dwustopniowa autoryzację podczas logowania do konsoli centralnego zarządzania (dotyczy co najmniej konsoli centralnego zarządzania znajdującej się w na serwerach producenta).
WO23	Dostarczone oprogramowanie musi posiadać możliwość zakładania lokalnych kont użytkowników oraz definiowania ról i zestawów uprawnień dla tych użytkowników.
WO24	Dostarczone oprogramowanie musi posiadać możliwość tworzenia grup stacji końcowych.

WO25	Rozwiązanie ma możliwość definiowania różnych profili ustawień dla stacji końcowych z poziomu konsoli centralnego zarządzania. Profile te mogą być przypisane do pojedynczych stacji końcowych lub do grup.
WO26	Dostarczone oprogramowanie musi posiadać możliwość konfiguracji i monitorowania wszystkich modułów dostarczonego rozwiązania zainstalowanych na stacjach końcowych, ich aktualizację oraz zlecanie im zadań z poziomu konsoli centralnego zarządzania.
WO27	Konsola centralnego zarządzania musi umożliwiać wgląd w szczegóły zgłaszającego się hosta, w których zawarte są co najmniej informacje dotyczące: • kto jest zalogowany na stacji roboczej • systemu operacyjnego • wersji systemu operacyjnego • stanu zaszyfrowania dysków systemowych • adresów IP • wersji zainstalowanego oferowanego przez Wykonawcę produktu • wersji programu i bazy wirusów • ostatniej aktualizacji • stanu ochrony • aktualnych ustawień programu • przypisanej polityki (konfiguracji) • wyników skanowania skanera na żądanie • akcji związanych z wykrytymi zagrożeniami i skanowaniami
WO28	Konsola centralnego zarządzania musi umożliwiać filtrowania po różnych parametrach stacji końcowej z zainstalowanym agentem. Filtry muszą uwzględniać co najmniej: • system operacyjny • adres IP • nazwę stacji końcowej • które stacje końcowe były online w ciągu ostatnich 24 godzin, 7 lub 30 dni
WO29	Konsola centralnego zarządzania ma możliwość definiowania wykluczeń m.in. w zakresie:

	• ochrony antywirusowej w czasie rzeczywistym • skanowania na żądanie • ochrony behawioralnej
WO30	Konsola centralnego zarządzania umożliwia wysyłanie minimum następujących zadań do agenta zainstalowanego na stacji końcowej: • skanowanie komputera • izolacji komputera, usunięcia komputera z izolacji • zebrania logów z klienta • zaszyfrowania dysków systemowych • odinstalowania agenta
WO31	Dostarczone rozwiązanie posiada funkcjonalność generowania raportów, w tym w formie graficznej z poziomu konsoli centralnego zarządzania. Raporty mogą być generowane ręcznie lub automatycznie (według ustalonego harmonogramu)
WO32	Dostarczone rozwiązanie pozwala na eksport raportów w postaci plików PDF.
WO33	Dostarczone rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące stacji końcowej, na której wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
WO34	Dostarczone rozwiązanie pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie, tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
WO35	Raporty z wykrytych infekcji zawierają minimum: • informacje na temat źródła ataku • pliki jakie zostały zaatakowane przez wirusa • adresy sieciowe do jakich niebezpieczny proces próbował się połączyć • informacje na temat wyleczenia lub usunięcia wirusa • mapowanie wykrytych metod ataku na matrycę MITRE ATT&CK
WO36	Dostarczone rozwiązanie pozwala na automatyczne powiadamianie o pojawiających się zagrożeniach wraz z określeniem czy stacja końcowa jest odpowiednio zabezpieczona.

WO37	Dostarczone rozwiązanie pozwala na zarządzanie powiadomieniami.
WO38	Dostarczone rozwiązanie posiada możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. Co najmniej dla stacji końcowych z systemami Microsoft Windows wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
WO39	Dostarczone rozwiązanie pozwala na powiadomienia w przypadku, gdy podsystemy bezpieczeństwa agenta nie będą funkcjonowały poprawnie.
WO40	Dostarczone rozwiązanie pozwala na wysyłanie powiadomień poprzez e-mail.
WO41	Dostarczone rozwiązanie posiada "Dashboard" (konsolę) prezentujący incydenty w czasie rzeczywistym oraz ma możliwość definiowanie własnych "Dashboardów" z wykorzystaniem predefiniowanych "Widgetów" (kontrolek).
WO42	Dostarczone rozwiązanie posiada interaktywny interfejs użytkownika, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe.
WO43	Dostarczone rozwiązanie posiada podgląd wykrytych zagrożeń umożliwiający odfiltrowania ich według: • daty • kategorii • typu zagrożenia • działań naprawczych • poziomu ryzyka
WO44	Interfejs użytkownika tworzy widok incydentu zawierający kluczowe informacje, takie jak: • przyczyna źródłowa • lista urządzeń na których zarejestrowano podejrzane zdarzenia • zakres ataku (powiązane maszyny i konta użytkowników) • data i czas wystąpienia podejrzanych zdarzeń • listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie • wykonanie wiersza poleceń używane do uruchomienia procesu

	• opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane • sumę kontrolną plików, które zostały uznane za podejrzane • poszczególne fazy ataku zaprezentowane na osi czasu • komunikacja sieciowa nawiązana w trakcie trwania ataku • poziom ryzyka, określający istotność danej detekcji • typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu) • zdarzenia które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK) • zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal)
WO45	Dostarczone rozwiązanie posiada mechanizm pozwalający na wyszukiwanie i ”polowanie” na zagrożenia sieciowe. Mechanizm ten posiada różne znaczniki, z których można budować zapytania.
WO46	Dostarczone rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: • PID nowego procesu • ścieżkę • nazwę procesu docelowego • nazwa pliku • typ zdarzenia • nazwę systemu • typ systemu • adres IP źródłowy • adres IP zdalny • port lokalny

	• port zdalny • adres URL • wartość klucza rejestru
WO47	Dostarczone rozwiązanie umożliwia przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem zapytań.
WO48	Dostarczone rozwiązanie zapewnia predefiniowane zapytania dotyczące artefaktów kryminalistycznych (np. hash, domena, nieprzetworzone zdarzenia, klucze rejestru). Reguły tworzenia zapytań muszą być opisane w dokumentacji systemu.
WO49	Dostarczone rozwiązanie posiada możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem oraz możliwość wyświetlenia zablokowanych hashy plików.
WO50	Dostarczone rozwiązanie na bazie zebranych danych w czasie rzeczywistym generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji końcowych.
WO51	Dostarczone rozwiązanie koreluje alerty, incydenty, zdarzenia wykryte w ramach wykrytego ataku, mapuje na matrycę taktyk, technik i procedur w ramach frameworku (metodyki) MITRE ATT&CK.
WO52	Dostarczone rozwiązanie automatyczne koreluje powiązane alerty wykryte na różnych stacjach końcowych w celu przyspieszenia i ułatwienia klasyfikacji oraz analizy incydentu. Wygenerowany skonsolidowany incydent prezentuje graficzną oś czasu, na której umieszczone będą kluczowe zdarzenia i podejrzenia, uruchamiane procesy, rozprzestrzenianie się ataku na kolejne stacje, wraz z możliwością interaktywnego śledzenia szczegółów tych zdarzeń.
WO53	Dostarczone rozwiązanie pokazuje kompletny widok drzewa ataku dla każdego złośliwego i niezłośliwego procesu zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. Automatycznie dostarcza informacji o urządzeniach i kontach użytkowników,

	które zostały dotknięte lub brały udział w przebiegu ataku. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów.
WO54	Dostarczone rozwiązanie pozwala na dodawanie komentarzy do incydentów, w celu łatwiejszego ich procesowania i przekazywania pomiędzy analitykami. System pozwala na przypisywanie zdarzeń/incydentów operatorom systemu.
WO55	Dostarczone rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędnej.
WO56	Dostarczone rozwiązanie posiada wbudowane reguły, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Istnieje możliwość utworzenia własnych reguł.
WO57	Dostarczone rozwiązanie posiada możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. Kryteria wykluczeń są konfigurowane w oparciu o przynajmniej: • nazwę procesu • ścieżkę procesu • hash pliku
WO58	Dostarczone rozwiązanie posiada możliwość eksportu logów audytowych poprzez Syslog po SSL/TLS w formacie CEF.
WO59	Dostarczone rozwiązanie posiada interfejs API do integracji z popularnymi narzędziami do orkiestracji i automatyzacji.
WO60	Na dzień podpisania umowy oprogramowanie musi wspierać ochronę stacji końcowych z poniższymi systemami operacyjnymi : Microsoft Windows 7, Microsoft Windows 10, Microsoft Windows 11, MacOS Sonoma 14.x, MacOS Ventura 13.x, MacOS Monterey 12x, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Ubuntu (20.04, 22.04), Debian (10-12), RHEL (8-9), CentOS (7-9), Amazon Linux (2, 2023), SUSE (15), Android (10-14), iOS 15, iOS 16.
WO61	Dostarczone rozwiązanie musi umożliwiać instalację agenta zarówno na fizycznych maszynach jak i w środowisku wirtualnym.

WO62	Dostarczone rozwiązanie musi wspierać następujące metody instalacji agenta na stacjach końcowych: • instalacja z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory • ręcznej instalacji
WO63	Dostarczone rozwiązanie zapewnia nieprzerwane działanie agenta i ochronę stacji końcowej od momentu startu systemu operacyjnego aż do momentu zamknięcia systemu operacyjnego.
WO64	Dostarczone rozwiązanie zapewnia aktualizację agenta zainstalowanego na stacji końcowej do nowej wersji, następuje ona w sposób automatyczny, niewidoczny dla użytkownika końcowego. Wszystkie aktualizacje definicji wirusów lub bazy sygnatur nie wymagają restartu systemu operacyjnego.
WO65	Dostarczone rozwiązanie zapewnia możliwość ręcznej aktualizacji agenta lub definicji wirusów.
WO66	Dostarczone rozwiązanie musi umożliwić zabezpieczenia agenta przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
WO67	Dostarczone rozwiązanie zapewnia komunikację agenta zainstalowanego na stacjach końcowych z konsolą centralnego zarządzania z interwałem nie dłuższym niż 10 min.
WO68	Dostarczone rozwiązanie zapewnia ochronę stacji końcowych w trybie offline.
WO69	Dostarczone rozwiązanie zapewnia po stronie stacji końcowej mechanizm buforowania danych w przypadku braku połączenia z konsolą centralnego zarządzania (np. praca w trybie offline). Dane zebrane na stacji końcowej są przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
WO70	Stacje końcowe nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie.

WO71	Agent zainstalowany na stacjach końcowych posiada możliwość zarejestrowania się w Windows Security Centre jako pełnoprawne rozwiązanie antywirusowe.

Wymagania dotyczące ochrony (co najmniej stacji roboczych i serwerów z systemami Microsoft Windows)	
WS1	Dostarczone rozwiązanie posiada mechanizm ochrony w czasie rzeczywistym opartym na bazie definicji wirusów dla stacji końcowych z systemami Microsoft Windows, MacOS, Linux.
WS2	Dostarczone rozwiązanie posiada mechanizm Antymalware dla stacji końcowych z systemami Microsoft Windows, MacOS, Linux.
WS3	Dostarczone rozwiązanie umożliwia skanowanie plików niewykonywalnych (dokumentów, ogólnych formatów plików) w systemach Microsoft Windows, MacOS, Linux.
WS4	Dostarczone rozwiązanie posiada funkcjonalność ochrony UEFI.
WS5	Dostarczone rozwiązanie posiada mechanizm wykrywania i przeciwdziałania nowym i nieznanym zagrożeniom, bazujący na: • modelu uczenia maszynowego (ang. Machine Learning - ML) • analizie behawioralnej, która wykrywa wzorce zachowań atakującego • algorytmach wykrywania anomalii oraz profilowania komputera i jego użytkownika • wykrywaniu anomalii w ruchu sieciowym • technologii chmurowej • technologii heurystycznej
WS6	Dostarczone rozwiązanie posiada następujące funkcjonalności w zakresie ochrony przed ransomware: • wykrywanie ataków ransomware, w szczególności tych których celem jest uszkodzenie Master Boot Record (MBR) niezależnie od tego, czy zostały uruchomione lokalnie, czy ze zdalnego punktu końcowego

	• w przypadku wykrycia ataku przerwanie próby szyfrowania plików na dysku oraz dodanie procesu odpowiedzialnego za szyfrowanie do listy procesów, których nie będzie można ponownie uruchomić na innych stacjach końcowych
WS7	Dostarczone rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) w celu odbierania i analizowania zdekodowanych skryptów.
WS8	Dostarczone rozwiązanie posiada mechanizm ochrony przed zagrożeniami uruchamianymi z dysków zmapowanych, pamięci przenośnych, przed zagrożeniami płynącymi z plików odebranych przez klienta poczty elektronicznej, zagrożeń pobranych przez przeglądarkę internetową oraz wynikających z innych połączeń sieciowych.
WS9	Dostarczone rozwiązanie zapewnia ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w podejrzany sposób poprzez analizę złożonych łańcuchów przyczynowo skutkowych i wykrywanie taktyk, technik i procedur stosowanych przez cyberprzestępców.
WS10	Dostarczone rozwiązanie jest w stanie wykryć fazę "ruchu bocznego" ataku - ang. Lateral Movement (np. ataki Pass-the-hash, zdalne tworzenie zaplanowanego zadania itp.).
WS11	Dostarczone rozwiązanie wykrywa i zapobiega atakom bezplikowym, działającym tylko w pamięci operacyjnej.
WS12	Dostarczone rozwiązanie zapewnia ochronę przed wykorzystywaniem exploitów w pamięci Windows (np. exploity 0-day), w tym: Mandatory ASLR, DEP.
WS13	Dostarczone rozwiązanie zapewnia ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploitacji: Kernel Privilege Escalation, ROP.
WS14	Dostarczone rozwiązanie posiada mechanizmy prewencji, które będą blokowały wykonanie złośliwej aktywności w trybie przed wykonaniem (ang. pre-execution), a także przerwanie złośliwej aktywności w trakcie wykonania (ang. on-execution). W ramach działania silników prewencyjnych systemu jest dostępna opcja

	automatycznego przeniesienia do kwarantanny plików uznanych za niebezpieczne.
WS15	Dostarczone rozwiązanie ma możliwość odizolowania stacji końcowej od sieci, jednocześnie zapewniając ciągłość analizy przeprowadzanej na tej stacji końcowej dla operatora systemu. Dostarczone rozwiązanie ma możliwość cofnięcia izolacji sieciowej maszyny z konsoli centralnego zarządzania.
WS16	Dostarczone rozwiązanie ma możliwość zestawienia sesji Remote Shell do wybranych stacji, udostępniając operatorowi linię poleceń systemu operacyjnego (np. PowerShell dla systemu Windows). Dostarczone rozwiązanie przechowuje pełny log z wykorzystania funkcji Remote Shell, w którym zachowane będą wszystkie komendy wydawane podczas nawiązanej sesji ze stacją końcową.
WS17	Dostarczone rozwiązanie pozwala na wykonanie akcji naprawczych na stacji końcowej. Dostarczone rozwiązanie dostarcza automatycznie zestaw działań naprawczych, jakie należy wykonać w przypadku danego typu wykrytego zagrożenia.
WS18	Dostarczone rozwiązanie w ramach odpowiedzi na incydent umożliwia: • reakcje (remediację) ze wskazaniem kroków, które mogą być podjęte automatycznie • uruchomienie skryptu na stacji końcowej • nawiązanie interaktywnego połączenia do linii poleceń na stacji końcowej • wyłączenie procesu na stacji końcowej • izolację sieciową stacji końcowej • usunięcie pliku na stacji końcowej • przeniesienie pliku na stacji końcowej do kwarantanny
WS19	Dostarczone rozwiązanie posiada funkcjonalność analizatora w środowisku sandbox.
WS20	Dostarczone rozwiązanie umożliwia: • skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików

	• skanowanie całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie” • skanowanie podmontowanych dysków sieciowych • skanowanie urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. Skanowanie to może odbywać się w sposób automatyczny bez wiedzy użytkownika
WS21	Dostarczone rozwiązanie umożliwia umieszczenia na liście wykluczeń ze skanowania wybranych katalogów lub plików na podstawie: • rozszerzenia • sumy kontrolnej • lokalizacji pliku
WS22	Dostarczone rozwiązanie posiada następujące funkcjonalności w zakresie kontroli urządzeń zewnętrznych: • mechanizm kontroli urządzeń zewnętrznych (urządzania USB, pamięci masowe, napędy CD/DVD, modemy, porty LPT/COM, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth) • możliwość tworzenie reguł dla podłączanych urządzeń w oparciu o numer seryjny • możliwość blokady zapisywania plików na zewnętrznych dyskach USB, urządzenia takie są wówczas dostępne w trybie tylko do odczytu • możliwość zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej
WS23	Dostarczone rozwiązanie posiada funkcjonalność zapory sieciowe lub możliwość wykorzystania natywnych narzędzi wbudowanych w system.
WS24	Dostarczone rozwiązanie posiada funkcjonalność pełnego szyfrowania dysku lub możliwość wykorzystania natywnego szyfrowania wbudowanego w systemy Microsoft Windows i MacOS.
WS25	Dostarczone rozwiązanie zbiera całą telemetrię aktywnie w czasie zbliżonym do rzeczywistego (bez wymaganej interakcji użytkownika dla wszystkich typów danych).

WS26	Telemetria ze stacji końcowych objętych ochroną jest przechowywana centralnie, aby móc korelować zdarzenia między różnymi stacjami.
WS27	Wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywa się na serwerze, a nie na monitorowanej stacji końcowej.
WS28	Dostarczone rozwiązanie zapewnia ochronę na podstawie zachowań opisywanych przez dane telemetryczne zbierane ze stacji końcowych.
WS29	Dostarczone rozwiązanie dokonuje analizy danych telemetrycznych ze stacji końcowych bez jakiegokolwiek filtrowania tych danych po stronie stacji końcowej.
WS30	Dostarczone rozwiązanie nie ogranicza liczby zdarzeń danego typu (np. limitowana liczba zapytań DNS w określonym przedziale czasowym, itp.).

WS31	Telemetria zbierana ze stacji końcowych uwzględnia minimalnie takie elementy jak:
	• połączenia sieciowe do/ze stacji, w tym takie szczegóły jak:
	  ○ adresy
	  ○ porty
	  ○ stan połączenia
	  ○ ilość danych otrzymanych/wysłanych
	  ○ czas utworzenia połączenia
	• działania na plikach, operacje:
	  ○ utworzenia
	  ○ zmiany nazwy
	  ○ usunięcia pliku
	  ○ zapisywanie
	  ○ przesunięcie
	  ○ modyfikacja
	  ○ wraz z informacją o tym, jaki proces wykonywał dane działanie oraz jaki użytkownik jest zalogowany w systemie podczas tej operacji
	• operacje w rejestrze
	  ○ skasowanie wartości

	○ ustawienie wartości ○ utworzenie klucza ○ kasowanie klucza ○ zmiana nazwy klucza • utworzenie nowego procesu i zakończenie procesu
WS32	Dostarczone rozwiązanie musi być dostarczone z funkcją umożliwiającą przetwarzanie i przechowywanie danych telemetrycznych z następujących systemów: • stacje końcowe • zdarzenia/logi (ang. events) z Active Directory i Azure Entra ID (Azure Active Directory) lub ochrania aplikacje Microsoft Office 365 i Google Workspace. Jeśli funkcjonalność wymaga dodatkowych licencji, licencje powinny zostać dostarczone wraz z oferowanym oprogramowaniem.
WS33	System przechowuje szczegółowe dane telemetryczne z wszystkich zabezpieczonych agentem stacji końcowych przez co najmniej 30 dni.
WS34	System przechowuje informacje o alarmach minimum przez okres 180 dni.
WS35	System przechowuje informacje o incydentach minimum przez okres 180 dni.

Wymagania dla dostarczonego oprogramowania – Etap II – „Wdrożenie oprogramowania”

Wymagania dotyczące wdrożenia	
WW1	Zamawiający wymaga aby Wykonawca przydzielił do wdrożenia zaoferowanego rozwiązania co najmniej 2 osoby posiadające aktualny certyfikat (dotyczący znajomości i obsługi) wystawiony przez producenta wdrażanego oprogramowania oraz osoby przydzielone posiadały minimum 2 lata doświadczenia we wdrażaniu oferowanego rozwiązania.
WW2	Zakres wdrożenia musi obejmować wszystkie elementy oferowanego systemu.
WW3	Zamawiający dopuszcza wdrożenie i konfigurację oferowanego systemu w formie zdalnej.
WW4	Konfiguracja oferowanego systemu zostanie wykonana przez Wykonawcę w uzgodnieniu z Zamawiającym.

WW5	Prace będą wykonywane przy asyście i obecności oddelegowanego pracownika Zamawiającego.
WW6	Instalacja lub uruchomienie konsoli centralnego zarządzania w zależności od rozwiązania oferowanego przez Wykonawcę.
WW7	Dodanie min. 2 głównych administratorów, min. 2 użytkowników systemu do konsoli centralnego zarządzania.
WW8	Przygotowanie min. 2 zestawów uprawnień dla różnych grup użytkowników systemu w konsoli centralnego zarządzania.
WW9	Przygotowanie profili konfiguracyjnych w zależności od typu stacji końcowej z ustawieniami dla agentów.
WW10	Przygotowanie instalatorów z agentem do wdrożenia na stacjach końcowych.
WW11	Zamawiający wdroży/zainstaluje na stacjach końcowych agentów we własnym zakresie.
WW12	Konfiguracja powiadomień i integracja z systemem pocztowym Zamawiającego.
WW13	Przygotowanie przykładowych raportów w konsoli centralnego zarządzania.
WW14	Wykonanie testów poprawności działania całego systemu w szczególności sprawdzenie czy oferowany system poprawnie reaguje na zagrożenia.

Wymagania dla dostarczonego oprogramowania – Etap III – „Dokumentacja powykonawcza i Szkolenia”

Zamawiający wymaga od Wykonawcy dostarczenia dokumentacji powykonawczej. Dokumenty powinny być dostarczone w formie elektronicznej.

Wymagania dotyczące dokumentacji powykonawczej	
DP1	Opis wdrożonego systemu wraz z szczegółowym opisem jego poszczególnych modułów oraz schematami funkcjonalnymi.
DP2	Opis instalacji i konfiguracji systemu, w tym zmiennych środowiskowych.
DP3	Konfigurację systemu.

DP4	Zestawienie adresacji, protokołów i portów IP oraz danych dostępowych utworzonych użytkowników.
DP5	Konfiguracja profili stacji końcowych.
DP6	Opis procedur utrzymaniowych i administracyjnych w szczególności aktualizacji poszczególnych modułów systemu.
DP7	Opis procedury wykonywania kopii zapasowej oraz archiwizacji systemu.
DP8	Opis procedur awaryjnych oraz „disaster recovery”.
DP9	Dokumentacja musi zostać przygotowana w języku polskim.

Wymagania dotyczące warsztatów organizowanych przez Wykonawcę	
SW1	Wykonawca zobowiązany jest przeprowadzić warsztaty dla maksymalnie 15 osób wskazanych przez Zamawiającego.
SW2	Zamawiający zastrzega sobie prawo do możliwości utrwalenia wszelkich materiałów szkoleniowych oraz przebiegu warsztatów w postaci materiału wideo do późniejszego wielokrotnego odtwarzania przez Zamawiającego i tylko na użytek wewnętrzny Zamawiającego.
SW3	Warsztaty będą omawiały wszystkie komponenty dostarczonego oprogramowania.
SW4	Językiem warsztatów musi być język polski.
SW5	Wykonawca zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej w języku polskim.
SW6	Czas warsztatów: nie mniej niż 3 dni (czas całego warsztatu nie mniej niż 18 godzin warsztaty w godzinach pracy Zamawiającego od 8:00 do 16:00). Jeżeli Wykonawca uważa, ze jest potrzebny dłuższy okres na przekazanie omawianego zakresu materiału, Zamawiający dopuszcza dłuższy czas warsztatów.
SW7	Warsztaty odbędą się w kilku grupach (grupa 4-6 osób). O przypisaniu użytkownika do grupy oraz ilości użytkowników w poszczególnych grupach decyduje Zamawiający.

	Zakres warsztatów będzie ustalany z Zamawiającym, który moduł szkolenia powinien być bardziej lub mniej rozwinięty w zależności do której grupy jest kierowany.
SW8	Warsztaty mogą odbyć się w formie zdalnej.
SW9	Wykonawca przygotuje na potrzeby przeprowadzenia warsztatów wszelkie niezbędne zaplecze techniczne tj. środowiska informatyczne dla poszczególnych uczestników, wirtualną salę laboratoryjną, oprogramowanie, licencje. Każdy uczestnik warsztatów będzie miał przydzielone własne środowisko informatyczne.
SW10	Osoba prowadząca warsztaty powinna posiadać aktualny certyfikat (dotyczący znajomości i obsługi) wystawiony przez producenta wdrażanego oprogramowania oraz minimum 2 lata doświadczenia we wdrażaniu oferowanego rozwiązania.
SW11	Po zakończeniu warsztatów Wykonawca przekaże uczestnikom certyfikaty uczestnictwa.
SW12	Wykonawca przeprowadzi instruktaż omawiający wszystkie elementy składowe dostarczanego rozwiązania, który będzie dotyczył konfiguracji oraz administracji dla pracowników Zamawiającego. Zakres warsztatów zostanie ustalony z Wykonawcą po wyborze najlepszego rozwiązania. Zakres powinien odnosić się bezpośrednio do przedmiotowego wdrożenia i obejmować co najmniej: • omówienie wszystkich komponentów systemu • wdrożenie systemu • utrzymanie systemu • zarządzanie oferowanym systemem • konfiguracja powiadomień i raportów • obsługa konsoli centralnego zarządzania • tworzenie dostępu do konsoli centralnego zarządzania • zarządzanie uprawnieniami • tworzenie pakietów instalacyjnych agentów • wdrożenie ręczne oraz zdalne agentów • profile / polityki bezpieczeństwa agentów

	• omówienie opcji występujących w politykach, zwróceniem uwagi na najważniejsze ustawienia pod kątem stacji końcowych • zarządzanie grupami chronionych urządzeń końcowych • przypisywanie reguł do grup lub urządzeń końcowych • zarządzanie agentami chronionych urządzeń końcowych • rozwiązywanie problemów z agentem • rozwiązywanie podstawowych problemów przy administracji • tworzenie reguł bezpieczeństwa i wyjątków od nich • ochronę przed malware • ochronę przed exploit • obsługę wykrytych incydentów • podstawowe i zaawansowane odpowiedzi na ataki • konfiguracja zapory sieciowej • obsługa i zarzadzanie szyfrowaniem stacji roboczych i serwerów • obsługa systemu XDR • Threat Hunting • sposób wykorzystywania zebranych danych • jak tworzyć zapytania na potrzeby wyszukiwania kluczowych elementów zdarzeń • głęboka analiza incydentów z uwzględnieniem artefaktów (np. IP, Hash) • wykrywanie zagrożenia APT • wykonywanie analizy po włamaniowej • zagadnienia związane ze zbieraniem danych z zewnętrznych źródeł • zagadnienia związane z eksportem danych do zewnętrznych źródeł • wykorzystywanie interfejsu API

Wymagania dotyczące certyfikowanych szkoleń producenta oferowanego oprogramowania

SC1	Wykonawca zobowiązany jest do dostarczenia voucherów na certyfikowane szkolenia autoryzowane przez producenta oferowanego oprogramowania dla maksymalnie 5 osób. Dostarczone vouchery nie będą wystawione imiennie. Dostarczone vouchery będą miały co najmniej rok ważność na ich wykorzystanie lub będą pozwalały na bezpłatne przedłużenie ich ważności.
SC2	Certyfikowane szkolenia producenta będą omawiały wszystkie komponenty dostarczonego oprogramowania.
SC3	Językiem szkolenia musi być język polski.
SC4	Wykonawca szkolenia zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej.
SC5	Czas szkolenia: minimum 4 dni (minimum po 6 godzin dziennie). Jeżeli Wykonawca uważa, że jest potrzebny dłuższy okres na przekazanie omawianego zakresu materiału, Zamawiający dopuszcza dłuższy czas szkolenia.
SC6	Certyfikowane szkolenia producenta mogą odbyć się w formie zdalnej.
SC7	Wykonawca szkolenia przygotuje na potrzeby przeprowadzenia szkolenia wszelkie niezbędne zaplecze techniczne tj. środowiska informatyczne dla poszczególnych uczestników, wirtualną salę laboratoryjną, oprogramowanie, licencje. Każdy uczestnik szkolenia będzie miał przydzielone własne środowisko informatyczne.
SC8	Po zakończeniu certyfikowanego szkolenia producenta uczestnikom zostaną przekazane certyfikaty uczestnictwa.

Etap I – „Dostawa Oprogramowania”

1. Wykonawca w terminie do 7 dni kalendarzowych od dnia podpisania Umowy zapewni Zamawiającemu możliwość pobierania zamówionego oprogramowania i kluczy licencyjnych za pośrednictwem witryny producenta - strony internetowej wskazanej przez Wykonawcę.
2. Możliwość pobierania wersji instalacyjnych Oprogramowania producenta, o których mowa w pkt 1 będzie zapewniona w trybie 24 godziny na dobę, 7 dni w tygodniu.

Etap II – „Wdrożenie oprogramowania”

1. Wykonawca w terminie do 30 dni kalendarzowych od dnia podpisania Umowy wdroży wszystkie elementy oferowanego oprogramowania.

2. Zamawiający w terminie 5 dni roboczych od dostarczenia przez Wykonawcę przygotowanego instalatora z agentem, zainstaluje go na co najmniej 100 stacjach końcowych.
3. Podstawą podpisania protokołu odbioru Etapu II będzie uruchomienie konsoli centralnego zarządzania i podpięcie do niej co najmniej 100 stacji końcowych.

Etap III – „Dokumentacja powykonawcza i Szkolenia"

1. Wykonawca dostarczy dokumentację powykonawczą, przeprowadzi warsztaty oraz dostarczy vouchery na certyfikowane szkolenia producenta oferowanego oprogramowania nie później niż do 30 dni kalendarzowych od podpisania protokołu odbioru Etapu II.
2. Dokumentacja przekazana Zamawiającemu podlega weryfikacji w ciągu 5 dni roboczych, w przypadku wykrycia przez Zamawiającego błędów lub jeżeli dokumentacja będzie niepełna Wykonawca jest zobowiązany do poprawienia dokumentacji.
3. Wykonawca przekaże Zamawiającemu kompletną/poprawioną dokumentację przed podpisaniem protokołu odbioru końcowego.
4. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy będzie podpisany protokół odbioru końcowego.

Wykonawca udzieli Zamawiającemu gwarancji na oprogramowanie, której okres wynosi 36 miesięcy.

Termin gwarancji, będzie liczony od daty podpisania protokołu odbioru Etapu II.

Wykonawca w ramach bezpłatnej udzielonej gwarancji świadczyć usługi, które będą obejmować:

1) zapewnienie świadczenia obsługi zgłoszeń serwisowych we wszystkie dni tygodnia w formie elektronicznej - poprzez internetowy serwis asysty technicznej lub dedykowaną skrzynkę mailową,
2) elektroniczny dostęp do informacji na temat posiadanego oprogramowania,
3) publikowanie i udostepnianie aktualizacji dokumentacji do oprogramowania w postaci elektronicznej przez internetowy serwis, takich jak np.: techniczna dokumentacja, internetowa baza wiedzy lub forum internetowe producenta oprogramowania,
4) wsparcie zespołu certyfikowanych inżynierów,
5) pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu,
6) doradztwo w zakresie konfiguracji,
7) pomoc w zakładaniu zgłoszeń serwisowych u producenta.

Usługi wskazane świadczone będą w języku polskim w godzinach pracy Zamawiającego tj. pn-pt 8:00-16:00.

Asysta techniczna w szczególności powinna obejmować pomoc w rozwiązywaniu problemów związanych z bieżącym administrowaniem, konfiguracją i utrzymaniem systemu.

Zamawiający zastrzega sobie prawo do weryfikacji: na prośbę Zamawiającego, Wykonawca musi wskazać w którym miejscu dana funkcjonalność umieszczona w OPZ występuje w oferowanych oprogramowaniu.

Rozdział 3

Termin realizacji zamówienia

Wykonawca dostarczy i wdroży oprogramowanie, dokumentację powykonawczą i vouchery na certyfikowane szkolenie producenta oferowanego oprogramowania, a także przeprowadzi warsztaty, w terminie do 60 dni kalendarzowych licząc od daty zawarcia Umowy, z tym że:

Etap I – do 7 dni kalendarzowych od daty zawarcia umowy,

Etap II - do 30 dni kalendarzowych od daty zawarcia umowy,

Etap III – do 30 dni kalendarzowych od podpisania protokołu odbioru Etapu II.

Rozdział 4

Warunki udziału w postępowaniu i podstawy wykluczenia

Warunki udziału w postępowaniu

1. O udzielenie zamówienia publicznego mogą ubiegać się wszyscy Wykonawcy, którzy spełniają warunki udziału niniejszym postępowaniu – zgodnie z art. 112 ust. 2 ustawy Pzp, dotyczące:
    1) Zdolności do występowania w obrocie gospodarczym – Zamawiający nie stawia warunku.
    2) Uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie stawia warunku.
    3) Sytuacji ekonomicznej lub finansowej – Zamawiający nie stawia warunku.
    4) Zdolności technicznej lub zawodowej – Zamawiający nie stawia warunku.
2. Wykonawca może w celu potwierdzenie spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub

ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. W tym celu wykonawca musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji.

3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te zrealizują roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
4. Zamawiający oceni, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.
5. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa 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.
6. Wykonawca nie może, po upływie terminu składania w postępowaniu ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

Podstawy wykluczenia z postępowania

1. O udzielenie zamówienia publicznego mogą ubiegać się wszyscy Wykonawcy, którzy nie podlegają wykluczeniu z niniejszego postępowania, na podstawie przesłanek określonych odpowiednio w:
   1) Art. 108 ust. 1 ustawy Pzp,
   2) Art. 109 ust. 1 pkt 4) ustawy Pzp,

3) Art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę.

2. Z postępowania o udzielenie zamówienia wyklucza się wykonawcę:
   1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego, w art. 46 - 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r., poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),
      d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
      e) o charakterze terrorystycznym, o którym mowa w art. 115 §20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
      f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9ust.2 ustawy z dnia 15 czerwca 2012r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz.U. poz.769),
      g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa wart.286Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
      h) o którym mowa w art. 9 ust. 1 i 3 lub art.10 ustawy z dnia 15 czerwca 2012r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki współce jawnej lub partnerskiej albo komplementariusza współce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo,
o którym mowa w pkt 1;
3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
6) jeżeli, w przypadkach, o których mowa w art. 85 ust.1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane winny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

3. Z postępowania o udzielenie zamówienia zamawiający wykluczy również wykonawcę, w stosunku do którego okoliczność wskazana w art. 109 ust. 1 pkt 4) ustawy Pzp:
4) 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 winnej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.

4. Mocą art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022, poz. 835), z postępowania o udzielenie zamówienia Zamawiający wykluczy:
   1) Wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 specustawy sankcyjnej.
   2) Wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 specustawy sankcyjnej.
   3) Wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 specustawy sankcyjnej".
5. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1), 2) i 5) jeżeli udowodni Zamawiającemu, że spełnił łącznie przesłanki określone w art. 110 ust. 2 ustawy Pzp.
6. Wykluczenie Wykonawcy nastąpi zgodnie z art. 111 ustawy Pzp.
7. Wykluczenie Wykonawcy, o którym mowa w art. 7 ust. 1. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie

bezpieczeństwa narodowego, nastąpi na okres trwania okoliczności określonych w art. 7 ust. 1. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

8. Osoba lub podmiot podlegające wykluczeniu na podstawie art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, które w okresie tego wykluczenia ubiegają się o udzielenie zamówienia publicznego lub biorą udział w postępowaniu o udzielenie zamówienia publicznego, podlegają karze pieniężnej, nakładanej przez Prezesa Urzędu Zamówień Publicznych, w drodze decyzji, w wysokości do 20 000 000 zł.
9. W celu potwierdzenia barku istnienia okoliczności, o których mowa w pkt 3 niniejszego rozdziału, Zamawiający żąda złożenia oświadczenia, którego wzór stanowi Załącznik nr 2 do SWZ.

Rozdział 5

Wykaz dokumentów składanych przez wszystkich Wykonawców ubiegających się o udzielenie zamówienia

Zamawiający żąda od wszystkich Wykonawców złożenia następujących dokumentów, stanowiących Ofertę:

1. Formularz ofertowy (Załącznik nr 1 do SWZ).
2. Oświadczenie Wykonawcy (Załącznik nr 2 do SWZ). W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie, o którym mowa powyżej, zobowiązany jest złożyć każdy z Wykonawców osobno.
3. Wadium
4. Dokument potwierdzający umocowanie do reprezentowania – Pełnomocnictwo (jeżeli dotyczy).

   Zgodnie z Rozporządzeniem 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, pełnomocnictwo przekazuje się elektronicznie. Pełnomocnictwo do złożenia oferty opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, w przypadku postępowań lub konkursów o wartości mniejszej niż progi unijne.

W sytuacji, gdy pełnomocnictwo zostało sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się skan tego dokumentu opatrzony kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem papierowym.

Należy pamiętać, że poświadczenia zgodności skanu pełnomocnictwa z dokumentem w postaci papierowej dokonuje mocodawca.

Dopuszcza się również przedłożenie pełnomocnictwa poświadczonego za zgodność z oryginałem przez notariusza.

Rozdział 6

Informacja o podmiotowych i przedmiotowych środkach dowodowych

Podmiotowe środki dowodowe

1. Podmiotowe środki dowodowe wymagane od Wykonawcy obejmują:
   1) **oświadczenie Wykonawcy w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp**, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz. U. z 2024 r. poz. 594), z innym Wykonawcą, który złożył odrębną ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej – zgodnie z **Załącznikiem nr 3 do SWZ;**
   2) **odpis lub informacja z Krajowego Rejestru Sądowego [KRS] lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej [CEiDG], 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;
2. Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, **nie krótszym niż 5 dni od dnia wezwania,** podmiotowych środków dowodowych, aktualnych na dzień złożenia podmiotowych środków dowodowych.
3. Jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, Zamawiający może w każdym czasie wezwać Wykonawcę lub Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.

4. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej zamiast dokumentu, o którym mowa w pkt 1 ppk 2) (tj. odpis lub informacja z Krajowego Rejestru Sądowego [KRS] lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej [CEiDG], w zakresie art. 109 ust. 1 pkt 4) ustawy Pzp) składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji, ani 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. Dokument (dokumenty), o którym mowa w niniejszym punkcie, powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.
5. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie wydaje się dokumentu, o którym mowa w pkt 4, zastępuje się go 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, złożony pod przysięgą, lub jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Dokument (dokumenty), o którym mowa w niniejszym punkcie, powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.
6. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:
    1) może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp dane umożliwiające dostęp do tych środków;
    2) podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp.
7. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

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

Przedmiotowe środki dowodowe

Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych w przedmiotowym postępowaniu.

Rozdział 7

Podwykonawstwo oraz Wykonawcy wspólnie ubiegający się o zamówienie

Podwykonawcy

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.
4. W przypadku powierzenia części zamówienia podwykonawcy/podwykonawcom, Wykonawca zobowiązany jest do wskazania w oświadczeniu, o którym mowa w Rozdziale 5 pkt 2 SWZ – czy wobec podwykonawcy/ podwykonawców zachodzą podstawy wykluczenia, o których mowa w art. 108 ust. 1, art. 109 ust. 1 pkt 4) ustawy Pzp oraz w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę.

Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (Spółki cywilne/Konsorcja)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku

Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo powinno być załączone do oferty.

2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie, o którym mowa w Rozdziale 5 pkt 2 SWZ składa każdy z Wykonawców. Oświadczenie to potwierdza brak podstaw wykluczenia.
3. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

Rozdział 8

Komunikacja między Zamawiającym, a Wykonawcami

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów oraz oświadczeń między Zamawiającym, a Wykonawcą odbywa się przy użyciu środków komunikacji elektronicznej. Przez środki komunikacji elektronicznej rozumie się środki komunikacji elektronicznej zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
2. Ofertę, oświadczenia, o których mowa w art. 125 ust. 1 ustawy Pzp, podmiotowe środki dowodowe, przedmiotowe środki dowodowe, pełnomocnictwa sporządza się w postaci elektronicznej, w ogólnie dostępnych formatach danych. Zamawiający rekomenduje wykorzystanie formatów .pdf, .doc, docx, .xls, .jpg ze szczególnym wskazaniem na .pdf.
3. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem strony internetowej: platformazakupowa.pl, pod adresem https://platformazakupowa.pl/pn/urk/proceedings
4. W celu skrócenia czasu udzielania odpowiedzi na pytania, Zamawiający zaleca, aby komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były w formie elektronicznej za pośrednictwem strony internetowej: platformazakupowa.pl i formularza „Wyślij wiadomość do Zamawiającego”. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień, informacji przyjmuje się datę ich przesłania za pośrednictwem strony internetowej: platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do Zamawiającego”, po którym pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.

5. Zamawiający będzie przekazywał Wykonawcom informacje za pośrednictwem strony internetowej: platformazakupowa.pl. Informację dotyczące odpowiedzi na pytania, zmiany SWZ, zmiany terminu składania i otwarcia ofert itp. Zamawiający będzie zamieszczał na platformie w sekcji „Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami, adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem strony internetowej platformazakupowa.pl do konkretnego Wykonawcy.
6. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na stronie internetowej platformazakupowa.pl przesłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
7. Zamawiający, zgodnie z Rozporządzeniem 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), określa niezbędne wymagania sprzętowo-aplikacyjne umożliwiające prace na stronie internetowej: platformazakupowa.pl tj.:
   1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   2) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   3) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
   4) włączona obsługa JavaScript,
   5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   6) Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
   7) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
8. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   1) akceptuje warunki korzystania ze strony internetowej: platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący;

2) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod adresem https://drive. google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view.

9. Zamawiający informuje, że instrukcje korzystania ze strony internetowej: platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
10. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego").
    Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu, ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.
11. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
12. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed terminem składania ofert.
13. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w pkt 12, przedłuża termin składania ofert o czas niezbędny do należytego przygotowania i złożenia oferty. W przypadku, gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie określonym w pkt 12, Zamawiający nie ma obowiązku udzielenia wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
14. Przedłużenie terminu składania ofert, o których mowa w pkt 12, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
15. Zamawiający wyznacza osobę do bezpośredniego kontaktowania się z Wykonawcami: **mgr inż. Paulina Żurek**, tel. **+48 12 662 42 22**, e-mail: **paulina.zurek@urk.edu.pl** (godziny kontaktu w sprawie postępowania: od poniedziałku do piątku w godz. 7:00-15:00).
    Zamawiający zwraca uwagę, że w sprawach związanych z niniejszym postępowaniem, wszelkie wnioski/pytania/pisma itp. należy składać za pośrednictwem Platformy Zakupowej.

Rozdział 9

Wadium

1. Zamawiający wymaga wniesienia wadium w wysokości 9 000,00 zł
2. Wadium należy wnieść przed upływem terminu składania ofert i utrzymywać nieprzerwanie do dnia upływu terminu związania ofertą, z wyjątkiem przypadków, o których mowa w art. 98 ust. 1 pkt 2 i 3 oraz ust. 2 ustawy Pzp.
3. Wadium może być wnoszone według wyboru Wykonawcy w jednej lub kilku następujących formach:
    1) pieniądzu,
    2) gwarancjach bankowych,
    3) gwarancjach ubezpieczeniowych,
    4) poręczeniach udzielonych przez podmioty, o których mowa w art. 6b ust. 5 pkt. 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tekst jedn.: Dz. U. z 2020 r. poz. 299).
4. Wadium wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy Zamawiającego w ALIOR BANK S.A nr rachunku: 86 2490 0005 0000 4530 1756 3779 z dopiskiem: wadium na zabezpieczenie oferty w postępowaniu na **„Dostawa i wdrożenie oprogramowania klasy XDR dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie”.** Za termin wniesienia wadium w formie pieniężnej zostanie przyjęty termin uznania rachunku Zamawiającego. Wadium wniesione w pieniądzu Zamawiający przechowuje na rachunku bankowym.
5. Jeżeli wadium jest wnoszone w formie gwarancji lub poręczenia, o którym mowa w art. 97 ust. 7 pkt 2-4 ustawy Pzp, Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia w postaci elektronicznej.
6. Wadium wnoszone w formie poręczeń lub gwarancji musi spełniać co najmniej poniższe wymagania:
    1) musi obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez Wykonawcę określone w ustawie Pzp, bez potwierdzania tych okoliczności;
    2) z jej treści powinno jednoznacznej wynikać zobowiązanie gwaranta do zapłaty całej kwoty wadium;
    3) powinno być nieodwołalne i bezwarunkowe oraz płatne na pierwsze żądanie;

4) termin obowiązywania poręczenia lub gwarancji nie może być krótszy niż termin związania ofertą (z zastrzeżeniem iż pierwszym dniem związania ofertą jest dzień składania ofert);
5) w treści poręczenia lub gwarancji powinna znaleźć się nazwa oraz numer przedmiotowego postępowania;
6) beneficjentem poręczenia lub gwarancji jest: Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie;
7) w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia(art. 58 PZP), Zamawiający wymaga aby poręczenie lub gwarancja obejmowała swą treścią (tj. zobowiązanych z tytułu poręczenia lub gwarancji) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia lub aby z jej treści wynikało, że zabezpiecza ofertę Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum);
8) musi zostać złożone w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym przez wystawcę poręczenia lub gwarancji.

5. W przypadku wniesienia wadium w formie:
   1) pieniężnej - zaleca się, by dowód dokonania przelewu został dołączony do oferty;
   2) poręczeń lub gwarancji-wymaga się, by oryginał dokumentu został złożony wraz z ofertą.
6. Oferta wykonawcy, który nie wniesie wadium lub wniesie w sposób nieprawidłowy lub nie utrzyma wadium nieprzerwanie do upływu terminu związania ofertą zostanie odrzucona.
7. Zamawiający zwraca wadium na zasadach uregulowanych w art. 98 ust. 1 - 5 ustawy Pzp.

Rozdział 10

Termin związania ofertą

1. Wykonawca będzie związany ofertą przez okres **30 dni** tj. **do dnia 03.07.2024 r.**
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w pkt 1, 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 30 dni. Przedłużenie terminu związania ofertą wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

Rozdział 11

Sposób przygotowania ofert

1. Wykonawca może złożyć tylko jedną ofertę.
2. Treść oferty musi odpowiadać treści SWZ.
3. Ofertę składa się na Formularzu ofertowym - zgodnie z Załącznikiem nr 1 do SWZ. Wraz z ofertą Wykonawca zobowiązany jest złożyć dokumenty i oświadczania, o których mowa w Rozdziale 5 niniejszej SWZ.
4. Oferta, oświadczenia i dokumenty, o których mowa w pkt 3, składane elektronicznie, muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny Wykonawca może złożyć bezpośrednio na dokumencie, który następnie przesyła do systemu (**opcja rekomendowana** przez **platformazakupowa.pl**) oraz dodatkowo dla całego pakietu dokumentów w kroku 2 **Formularza składania oferty lub wniosku** (po kliknięciu w przycisk **Przejdź do podsumowania**).
5. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
6. Oferta powinna być:
    1) sporządzona na podstawie załączników niniejszej SWZ w języku polskim;
    2) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem strony internetowej: platformazakupowa.pl;
    3) podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
7. Podpisy kwalifikowane wykorzystywane przez Wykonawców do podpisywania wszelkich plików muszą spełniać wymogi Rozporządzenia Parlamentu Europejskiego i Rady w sprawie

identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku.

8. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny, Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisanych plików z danymi oraz plików XAdES.
9. Zgodnie z art. 8 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli Wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
10. Wykonawca, za pośrednictwem strony internetowej: platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
11. Każdy z Wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje odrzucenie takiej oferty/ofert.
12. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść Wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
13. Dokumenty i oświadczenia składane przez Wykonawcę powinny być sporządzone w języku polskim. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, Wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
14. Zgodnie z definicją dokumentu elektronicznego z art. 3 ust. 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego Wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, albo przez podwykonawcę.
15. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

16. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania ze strony internetowej: platformazakupowa.pl, w szczególności za sytuację, gdy Zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do Zamawiającego"). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu, ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy Pzp.
17. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
18. Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, Zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
19. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
20. Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów z późniejszą walidacją plików.
21. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
22. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Zamawiający sugeruje złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
23. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2, zamiast SHA1.
24. Jeśli Wykonawca pakuje dokumenty np. w plik ZIP, Zamawiający zaleca wcześniejsze podpisanie każdego ze skompresowanych plików.
25. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
26. Zamawiający zaleca, aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich. Może to skutkować naruszeniem integralności plików, co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.

Rozdział 12

Sposób i termin składania i otwarcia ofert

1. Ofertę wraz z wymaganymi dokumentami i oświadczeniami należy umieścić na stronie internetowej: platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/urk/proceedings tj. w Profilu Nabywcy Zamawiającego / stronie internetowej prowadzonego postępowania **do dnia 04.06.2024 r. do godz. 9:00.**
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty i oświadczenia.
3. Po wypełnieniu Formularza składania oferty, dołączenia wszystkich wymaganych załączników, należy kliknąć przycisk „Przejdź do podsumowania".
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem strony internetowej platformazakupowa.pl, Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem strony internetowej platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 2 ustawy Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
5. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku "Złóż ofertę" i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
6. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
7. Otwarcie ofert nastąpi **w dniu 04.06.2024 r. o godz. 9:15.**
8. W przypadku awarii systemu, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
9. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania tj. w swoim Profilu Nabywcy.

10. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
11. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
    1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
    2) cenach lub kosztach zawartych w ofertach.
12. Informacja zostanie opublikowana na stronie prowadzonego postępowania na stronie internetowej: platformazakupowa.pl w sekcji ,,Komunikaty".

Rozdział 13

Sposób obliczania ceny

1. Cena ofertowa powinna spełniać wymogi ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług, a w szczególności jej art. 3 ust. 1 pkt 1 oraz ust. 2, który stanowi, że „cena to wartość wyrażona w jednostkach pieniężnych, którą kupujący jest obowiązany zapłacić przedsiębiorcy za towar lub usługę". W cenie uwzględnia się podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów sprzedaż towaru (usługi) podlega obciążeniu podatkiem od towarów i usług lub podatkiem akcyzowym. Przez cenę rozumie się również stawkę taryfową.
2. Sposób przedstawienia ceny oferty:
    1) wykonawca podaję cenę oferty oraz wszystkie jej składniki w formularzu oferty (zgodnie we wzorem stanowiącym załącznik nr 1 do SWZ),
    2) cenę oferty należy podać w złotych polskich, z dokładnością do dwóch miejsc po przecinku.
3. Wykonawca zobowiązany jest w cenie oprogramowania uwzględnić wszelkie koszty niezbędne do zrealizowania przedmiotu umowy, tj. koszty oprogramowania i wdrożenia, koszty przeprowadzenia szkoleń, koszty dokumentacji powykonawczej, koszty warsztatów, podatek VAT oraz wszelkie inne koszty, które nie zostały wymienione, ale są niezbędne do należytego wykonania przedmiotu umowy.
4. Stawkę podatku należy określić zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług.

5. Cena podana w ofercie nie ulegnie zmianie przez cały okres obowiązywania umowy.
6. Wyliczona cena oferty brutto będzie służyć do porównania złożonych ofert i do rozliczenia w trakcie realizacji zamówienia.
7. Jeżeli zaoferowana cena lub jej istotne części składowe, będą wydawać się rażąco niskie w stosunku do przedmiotu zamówienia i będą budzić wątpliwości Zamawiającego, co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwróci się o udzielenie wyjaśnień, w tym złożenie dowodów, dotyczących wyliczenia ceny.
8. Jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług, dla celów zastosowania kryterium ceny Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W ofercie, o której mowa w pkt 2, Wykonawca ma obowiązek: poinformować Zamawiającego, że wybór jego oferty będzie prowadził / nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego, wskazania nazwy towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku, wskazania stawki podatku od towarów i usług, które zgodnie z wiedzą Wykonawcy, będzie miał zastosowanie.
9. Rozliczenia między Zamawiającym, a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
10. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

Rozdział 14

Kryteria oceny ofert z uwzględnieniem wag tych kryteriów i sposobu oceny ofert

1. Zamawiający oceni i porówna jedynie te oferty, które nie zostaną odrzucone oraz, gdy wykonawca nie będzie podlegał wykluczeniu z postępowania.
2. Oferty zostaną ocenione przez zamawiającego w oparciu o następujące kryteria oceny ofert:

Kryteria	**Waga**
Kryterium 1 – Cena (C)	60%
Kryterium 2 - Możliwość uruchomienia On-Premise lub chmura w Polsce (F)	10%

Instalacja na serwerach Zamawiającego konsoli centralnego zarządzania lub konsola centralnego zarządzania przechowuje i przetwarza dane na serwerach znajdujących się w Polsce lub dostarczone rozwiązanie spełnia Standardy Cyberbezpieczeństwa Chmur Obliczeniowych na poziomie SCCO2 (dostępne na stronie https://chmura.gov.pl/informacje/scco)	
Kryterium 3 - Skuteczność ewaluacji MITRE ENGENUITY, ATT&CK w ewaluacji Turla (2023) (S) Skuteczność ewaluacji MITRE ENGENUITY, ATT&CK, Turla (2023)	30%

Kryterium 1 - Cena

Oferty otrzymują liczbę punktów wg następującego wzoru:
Pc – otrzymane punkty

Cn – cena najniższa ze złożonych ofert

Cb – cena badanej oferty

Pc = (Cn : Cb) x 100 x 60%

1% = 1 pkt

60% = 60 pkt

Kryterium 2 - Możliwość uruchomienia On-Premise lub chmura w Polsce

Oferty otrzymują liczbę punktów wg następującego wzoru:

TAK - jeżeli kryterium jest spełnione = 10 pkt

NIE - jeżeli kryterium nie jest spełnione = 0 pkt

1% = 1 pkt

10% = 10 pkt

Kryterium 3 - Skuteczność ewaluacji MITRE ENGENUITY, ATT&CK w ewaluacji Turla (2023)

będzie oceniana następująco:

1) Przez zaliczony test Zamawiający rozumie wykrycie zagrożenia na poziomie Technique (4 pkt.), Tactic (3 pkt.), General (2 pkt.), Telemetry (1 pkt.)

(maksymalnie 4 x 76 punktów w scenariuszu Carbon, 4 x 67 punktów w scenariuszu Snake – łącznie maksymalnie 572 pkt.)

2) Przez niezaliczony test rozumiemy brak udziału w teście (Not applicable) lub brak wykrycia (none detections) – 0 pkt, lub brak udziału w ewaluacji Turla (2023) w ocenianych scenariuszach.

Oferty otrzymują liczbę punktów wg następującego wzoru:

Po – otrzymane punkty

Tb – punkty badanej oferty

Tm – ilość maksymalnych punktów do otrzymania w ewaluacji Turla (scenariusz Carbon i Snake)

Po = (Tb : Tm) x 100 x 30%

1% = 1 pkt

30% = 30 pkt

Adres strony internetowej z wynikami testów MITRE ENGENUITY, ATT&CK w ewaluacji Turla (2023): https://attackevals.mitre-engenuity.org/results/enterprise?evaluation=turla

Ilość punktów, jaką uzyska oferta będzie stanowić końcową ocenę danej oferty i zostanie obliczona według wzoru**:**

P = C + F + S

gdzie:

P – całkowita liczba punktów uzyskana przez badaną, nieodrzuconą ofertę,

C – liczba punktów przyznana ofercie w kryterium „cena”,

F – liczna punktów przyznana ofercie w kryterium „Możliwość uruchomienia On-Premise lub chmura w Polsce”,

S - liczna punktów przyznana ofercie w kryterium „Skuteczność ewaluacji MITRE ENGENUITY, ATT&CK w ewaluacji Turla (2023)”,

Za najkorzystniejszą zostanie uznana oferta, niepodlegająca odrzuceniu, która uzyska największą ilość punktów.

Oferta może otrzymać maksymalnie 100 punktów.

Wyliczenie punktów zostanie dokonane z dokładnością do dwóch miejsc po przecinku.

3. Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska najwyższą liczbę punktów,

przyznanych zgodnie z powyższymi zasadami. Liczba punktów przyznana poszczególnym ofertom zostanie obliczona z dokładnością do dwóch miejsc po przecinku. W przypadku osiągnięcia jednakowej liczby punktów przez dwie lub więcej ofert, Zamawiający wybierze ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybierze ofertę o najniższej cenie. Jeżeli nie można dokonać wyboru oferty, ponieważ zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty do złożenia w terminie określonym, ofert dodatkowych zawierających nową cenę.

4. Oferta Wykonawcy może otrzymać maksymalnie 100 punktów.

Rozdział 15

Informacje o dopełnieniu formalności po wyborze najkorzystniejszej oferty

1. Zamawiający zawrze umowę w sprawie zamówienia publicznego, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.
2. Zamawiający może zawrzeć umowę przed upływem terminu określonego w pkt 1, jeżeli w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie podstawowym złożono tylko jedną ofertę.
3. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.
4. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.

Rozdział 16

Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga zabezpieczenia należytego wykonania umowy w niniejszym postępowaniu.

Rozdział 17

Postanowienia końcowe

1. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
2. Zgodnie z art. 223 ust. 2 ustawy Pzp Zamawiający poprawi w ofercie:
    1) oczywiste omyłki pisarskie;
    2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek;
    3) inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty;

    - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta zostanie poprawiona.
3. W przypadku, o którym mowa w pkt 2.3), Zamawiający wyznaczy Wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.
4. Wybrany Wykonawca będzie zobowiązany do zawarcia umowy w sprawie zamówienia publicznego na warunkach określonych w projektowanych postanowieniach umowy, stanowiących Załącznik nr 4 do SWZ.
5. Zakres świadczenia Wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
6. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454-455 ustawy Pzp oraz wskazanym w projektowanych postanowieniach umowy, stanowiących Załącznik nr 4 do SWZ.
7. Zamiana umowy wymaga dla jej ważności, pod rygorem nieważności, zachowania formy pisemnej.
8. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
9. Zamawiający nie przewiduje aukcji elektronicznej.
10. Zamawiający nie dopuszcza składania ofert wariantowych.
11. Zamawiający nie przewiduje złożenia ofert w postaci katalogów elektronicznych.
12. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
13. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 ustawy Pzp.

14. Zamawiający nie przewiduje przeprowadzenia wizji lokalnej.
15. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7) i 8) ustawy Pzp.

Rozdział 18

Środki ochrony prawnej

1. Środki ochrony prawnej określone w niniejszym rozdziale przysługują Wykonawcy oraz 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 oraz dokumentów zamówienia 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:
    1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienia umowy;
    2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy Pzp.
4. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektroniczne albo postaci elektronicznej albo kopię 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 wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.
6. Odwołanie wnosi się w terminie:
    1) 5 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia - jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej;

2) 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia - jeżeli informacja została przekazana w sposób inny niż określony w ppkt 1).

7. Odwołanie w przypadkach innych, niż określone w pkt 5 i 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zaniechaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp, stronom oraz uczestnikom postepowania odwoławczego przysługuje skarga do sądu.
9. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.
10. Skargę wnosi się do Sądu Okręgowego w Warszawie – sądu zamówień publicznych, zwanego dalej „sądem zamówień publicznych".
11. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe jest równoznaczne z jej wniesieniem.
12. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.

Rozdział 19

Obowiązki informacyjne wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

I. Zgodnie z art 13 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych), zwanego dalej RODO, niniejszym informujemy, iż:

1. Administratorem Pana/Pani danych osobowych będzie Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, al. Adama Mickiewicza 21, 31-120 Kraków, adres e-mail: rector@urk.edu.pl .
2. Administrator wyznaczył Inspektora ochrony danych, z którym należy kontaktować się za pomocą adresu e-mail: **iod@urk.edu.pl.**
3. Dane osobowe pozyskaliśmy bezpośrednio od Pani/Pana, a w przypadku kiedy dane nie pochodzą od osoby, której te dane dotyczą są one pozyskane od kontrahenta, oferenta lub ze źródeł publicznie dostępnych. Administrator będzie przetwarzał następujące kategorie danych: nazwa wykonawcy, imię i nazwisko, adres, numer telefonu, adres e-mail, NIP, informacje dotyczące wykształcenia i uprawnień, inne informacje niezbędne do przeprowadzenia postępowania o udzielenie zamówienia publicznego i realizacji umowy w sprawie zamówienia publicznego.
4. Pozyskane dane osobowe będą przetwarzane w celu:
    1) wyłonienia wykonawców na realizację zamówienia publicznego, a następnie w celu zawarcia i realizacji umowy (art. 6 ust. 1 lit. b, c RODO),
    2) prawidłowej realizacji postępowania dotyczącego zamówienia publicznego oraz wypełnienia obowiązków prawnych ciążących na Administratorze, wynikających z ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych oraz innych obowiązków prawnych, w tym księgowo rachunkowych oraz archiwizacyjnych (art. 6 ust. 1 lit. c RODO),
    3) ewentualnego dochodzenia roszczeń lub obrony przed roszczeniami (art. 6 ust. 1 lit. f RODO).
5. Odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa.
6. Pani/Pana dane osobowe mogą być ponadto przekazywane podmiotom przetwarzającym je na zlecenie Administratora, np. dostawcom usług IT – przy czym takie podmioty przetwarzają dane wyłącznie na podstawie umowy z Administratorem.
7. Dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas jej trwania, a następnie okres archiwizacyjny wynikający z instrukcji kancelaryjnej.

8. Podanie danych osobowych jest niezbędne dla celów określonych w pkt 4, a ich niepodanie będzie skutkowało niemożnością rozpatrzenia oferty i zawarcia umowy.
9. W związku z przetwarzaniem Pani/Pana danych osobowych posiada Pani/Pan prawo do:
    1) dostępu do treści swoich danych osobowych,
    2) prawo do sprostowania danych,
    3) usunięcia lub ograniczenia przetwarzania danych osobowych,
    4) wniesienia sprzeciwu wobec przetwarzania,
    5) przenoszenia danych,

    - na zasadach i warunkach wynikających z RODO.
10. Posiada Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z przepisami RODO.
11. Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym w formie profilowania.
12. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

Rozdział 20

W sprawach nie uregulowanych w niniejszej Specyfikacji będzie stosowana ustawa z dnia 11 września 2019 roku - Prawo zamówień publicznych oraz Kodeks Cywilny.

Kraków, 24.05.2024 r.

Kanclerz
Uniwersytetu Rolniczego
im. Hugona Kołłątaja w Krakowie
Dyrektor ds. majątku i inwestycji
mgr Marcin Gałan