

Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie
al. Mickiewicza 21, 31-120 Kraków
tel. 12 662-44-12, fax. 12 662-44-10

Specyfikacja Warunków Zamówienia

„Dostawa specjalistycznego sprzętu teleinformatycznego wraz z osprzętem do zarządzania infrastrukturą Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie”

Nr zamówienia: DZP- 291-930/2021

Wspólny Słownik Zamówień CPV: 48820000-2

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie przetargu nieograniczonego na dostawy o wartości zamówienia przekraczającej progi unijne, o jakich stanowi art. 3 ustawy z dnia 11 września 2019 r., Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 ze zm.).

Załączniki:

1. Formularz ofertowy - Załącznik nr 1 do SWZ
2. Parametry Techniczne Przedmiotu Zamówienia – Załącznik nr 1A do SWZ
3. Jednolity Europejski Dokument Zamówienia - Załącznik nr 2 do SWZ
4. Oświadczenie Wykonawcy o przynależności/ bądź braku przynależności do grupy kapitałowej – załącznik nr 3 do SWZ
5. Wykaz Dostaw - Załącznik nr 4 do SWZ
6. Wzór zobowiązania - Załącznik nr 5 do SWZ
7. Wzór umowy - Załącznik nr 6 do SWZ
8. Karta gwarancyjna – Załącznik nr 7 do SWZ

ROZDZIAŁ I.

Nazwa, adres i dane kontaktowe zamawiającego, tryb udzielenia zamówienia

1. Zamawiający:

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 44 12,
http: www.urk.edu.pl

2. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie **przetargu nieograniczonego na dostawę**, na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 ze zm.), zwanej dalej ustawą Pzp oraz niniejszej Specyfikacji Warunków Zamówienia, zwanej dalej SWZ.

3. Szacunkowa wartość zamówienia przekracza kwotę określoną w obwieszczeniu Prezesa Urzędu Zamówień Publicznych wydanym na podstawie art. 3 ust. 2 ustawy Pzp.

4. Zamawiający przewiduje zastosowanie tzw. procedury odwróconej, o której mowa w art. 139 ust. 1 ustawy Pzp, tj. Zamawiający najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej Wykonawcy, którego oferta została najwyżej oceniona, w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.

5. Zamawiający nie przewiduje aukcji elektronicznej.

6. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.

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

8. Zamawiający nie dopuszcza składania ofert wariantowych oraz w postaci katalogów elektronicznych.

9. Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 8 ustawy Pzp

10. Do postępowania stosuje się przepisy dotyczące nabywania dostaw

11. **Cała dokumentacja postępowania będzie dostępna pod adresem: <https://platformazakupowa.pl/pn/urk>**

ROZDZIAŁ II.

Opis przedmiotu zamówienia

I. Ogólne informacje o zamówieniu

1. Przedmiotem zamówienia jest **dostawa specjalistycznego sprzętu teleinformatycznego wraz z osprzętem do zarządzania infrastrukturą dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie**, zwanego dalej „sprzętem”.
2. Zamówienie jest realizowane w ramach Projektu pn. „*Innowacyjny program strategicznego rozwoju Uczelni*”, nr: POWR.03.05.00-00-2020/18 (CENTR) „*Zadanie 6 Stworzenie ujednoczonej infrastruktury informatycznej w celu zwiększenia bezpieczeństwa przetwarzanych danych osobowych na Uniwersytecie Rolniczym (MD6)*”
3. Zamawiający podkreśla, iż nazwy własne podane w opisie przedmiotu zamówienia są nazwami przykładowymi i winny być interpretowane jako definicje standardów, a nie jako nazwy konkretnych rozwiązań do zastosowania. Zamawiający dopuszcza złożenie oferty na sprzęt równoważny w stosunku do wymaganego w SWZ. W przypadku oferowania przez wykonawcę sprzętu równoważnego w stosunku do określonego przez zamawiającego w SWZ, ciężar udowodnienia równoważności spoczywa na wykonawcy. Przez sprzęt „równoważny” zamawiający rozumie sprzęt o parametrach i standardach jakościowych takich samych bądź lepszych w stosunku do sprzętu wymaganego przez zamawiającego. Składając ofertę, wykonawca będzie zobowiązany wskazać nazwę sprzętu (typ, producenta), który oferuje oraz wskazać wszystkie parametry, które zostały określone w Załączniku nr 1A do SWZ.
4. Zamawiający nie dokonuje podziału zamówienia na części. Tym samym zamawiający nie dopuszcza składania ofert częściowych, o których mowa w art. 7 pkt 15 ustawy Pzp. Przedmiot zamówienia nie jest podzielny, ponieważ Zamawiający chce zakupić 1 szt. sprzętu - Serwer Service Gateway. Zamawiający w 2020 roku prowadził postępowanie na dostawę specjalistycznego sprzętu teleinformatycznego wraz z osprzętem do zarządzania infrastrukturą dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie w tym jednym z zadań częściowych był zakup Serwera Service Gateway, które zostało unieważnione, ponieważ cena najkorzystniejszej oferty przewyższała kwotę, jaką Zamawiający zamierzał przeznaczyć na realizację tego Zadania. Podzielenie na części groziłoby nadmiernymi trudnościami technicznymi i kosztami wykonania zamówienia a także potrzebą skoordynowania działań różnych wykonawców realizujących poszczególne części zamówienia. Ponadto istniałoby ryzyko

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

niewykonania części zamówienia. Zamawiający kierując się zasadą optymalizacji kosztów i gospodarnością podczas wydatkowania środków publicznych oraz zachowując zasadę konkurencyjności oraz równego traktowania wykonawców nie podzielił zamówienia na części.

II. Szczegółowe informacje o zamówieniu

1. Lokalizacja dostawy:

Wykonawca zobowiązany będzie dostarczyć sprzęt do jednostki organizacyjnej zamawiającego pod adres: Dział Informatyki Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie, 31-121 Kraków, ul. Czysta 21, pok. nr 8.

2. Minimalne wymagane parametry techniczne dostarczanego sprzętu:

Konfiguracja	Minimalne wymagane parametry
1.	2.
Ogólne wymagania	<ol style="list-style-type: none"> System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 6 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 3 Gbit/s dla kontroli zawartości (w tym kontrola antywirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń. System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000, 8 portów 1Gbps/10Gbps SFP/SFP+. Należy dostarczyć 2 moduły SFP+ 10Gb-LR oraz 2 kable typu DAC 10Gb 5m (dopuszcza się dostarczenie w miejsce 2 kabli DAC - 4 modułów 10Gb-SR wraz z 2 patchcordami światłowodowymi MM 5m OM4). Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.). System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN. System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tablica routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

	<ol style="list-style-type: none">9. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).10. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.11. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.12. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 6 Gbit/s.13. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowanie aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).14. Nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.15. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.16. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.17. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.18. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.19. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.20. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.21. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.
--	--

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

	<p>22. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.</p> <p>23. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.</p> <p>24. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.</p> <p>25. System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.</p> <p>26. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.</p> <p>27. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalenie tożsamości musi odbywać się również transparentnie.</p> <p>28. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.</p> <p>29. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesję w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.</p> <p>30. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.</p> <p>31. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).</p>
--	--

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

	<p>32. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.</p> <p>33. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.</p> <p>34. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekodery taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p> <p>35. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).</p> <p>36. System zabezpieczeń firewall musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p> <p>37. System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).</p> <p>38. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.</p> <p>39. System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p> <p>40. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).</p> <p>41. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.</p> <p>42. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.</p> <p>43. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).</p> <p>44. System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.</p>
--	---

	<p>45. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.</p> <p>46. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.</p> <p>47. System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msoffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 3 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.</p> <p>48. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielanie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".</p> <p>49. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msoffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.</p> <p>50. System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.</p> <p>51. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.</p> <p>52. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.</p> <p>53. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.</p> <p>54. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.</p> <p>55. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.</p> <p>56. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentication) do wybranych zasobów. Polityki</p>
--	--

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

	<p>definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.</p> <p>57. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.</p> <p>58. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.</p> <p>59. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.</p> <p>60. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystać z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakkolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.</p> <p>61. Zarządzanie systemem zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.</p> <p>62. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.</p> <p>63. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.</p> <p>64. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.</p> <p>65. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).</p> <p>66. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.</p> <p>67. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.</p> <p>68. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).</p> <p>69. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być</p>
--	---

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

	<p>dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.</p> <p>70. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.</p> <p>71. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.</p> <p>72. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.</p> <p>73. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.</p> <p>74. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.</p> <p>75. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.</p> <p>76. System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.</p> <p>77. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.</p> <p>78. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active wraz z urządzeniem posiadanym już przez zamawiającego. Jeśli wymagane są dodatkowe licencje do urządzenia zamawiającego, należy je dostarczyć.</p> <p>79. Zamawiający wymaga, by dostarczony sprzęt był nowy oraz nieużywany (przy czym Zamawiający dopuszcza, by sprzęt był rozpakowany i uruchomiony przed jego dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania sprzętu, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem),</p> <p>80. 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 mogą być zaoferowane sprzęt i oprogramowanie, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.</p> <p>81. Oferowany sprzęt w dniu składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub ze sprzedaży.</p> <p>82. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej w dniu poprzedzającym dzień składania ofert.</p> <p>83. Wymagane jest, aby data produkcji dostarczonych urządzeń nie była wcześniejsza niż 6 miesięcy. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.</p> <p>Dostęp do nowych wersji, aktualizacji i poprawek do oprogramowania dla oferowanych urządzeń w tym w szczególności sygnatur aplikacji, sygnatur AV, ThreatPrevention (IPS), system ochrony zero-day (sandbox) na okres 12</p>
--	---

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

	<p>miesiący. Sygnatury AV, ThreatPrevention, system ochrony zero-day (sandbox) muszą mieć możliwość aktualizacji automatycznej nie rzadziej niż raz dziennie. Producent oferowanego urządzenia musi posiadać platformę umożliwiającą informowanie o znanych problemach z oprogramowaniem i sposobach ich rozwiązywania.</p> <p>Producent oferowanego rozwiązania musi umożliwiać dostęp do elektronicznych kanałów informacji i usług wsparcia (bazy wiedzy, bibliotek dokumentacji, opisów produktów, specyfikacji, literatury technicznej i innych materiałów).</p> <p>Wykonawca umożliwi dostęp do centrum serwisowego producenta.</p>
<p>Gwarancja</p>	<ol style="list-style-type: none"> 1. Gwarancja: 12 miesięcy 2. Serwis realizowany w języku urzędowym obowiązującym w Polsce. 3. Przyjęcie zgłoszenia potwierdzone telefonicznie lub mailowo. 4. W przypadku wystąpienia problemów, których nie można rozwiązać zdalnie, pomoc techniczna w miejscu instalacji. 5. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. 6. Serwis świadczony przez Wykonawcę. Wykonawca serwisu musi posiadać autoryzację producenta do świadczenia serwisu dla oferowanych rozwiązań. Autoryzowany Partner Serwisowy Producenta. 7. Długość okresu gwarancyjnego oraz serwisowego dla oferowanego urządzenia – 12 miesięcy. <ul style="list-style-type: none"> • Gwarantowany czas reakcji: 8 godzin • Gwarantowany czas naprawy przy awarii pojedynczego urządzenia: 2 dni robocze 8. W celu usunięcia awarii Zamawiający dopuszcza zastosowanie sprzętu zastępczego o parametrach wydajnościowych nie gorszych od sprzętu podstawowego.

3. Wymagania dotyczące sprzętu:

1. Wykonawca będzie zobowiązany dostarczyć sprzęt, spełniający minimalne wymagania w zakresie parametrów technicznych.
2. Wykonawca będzie zobowiązany dostarczyć sprzęt:
 - 1) pochodzący z autoryzowanego kanału dystrybucji,
 - 2) posiadający indywidualny numer fabryczny,
 - 3) fabrycznie nowy, nieużywany, wyprodukowany w 2020 lub 2021 r., wolny od wad fizycznych i prawnych,
 - 4) posiadający np. certyfikaty, atesty, świadectwa dopuszczenia do użytkowania lub inną dokumentację potwierdzającą, że oferowany sprzęt spełnia wymagane prawem normy,
 - 5) zapakowany w oryginalnym opakowaniu,
 - 6) kompletny (posiadający niezbędne wyposażenie: okablowanie, materiały startowe, baterie, złącza, zasilacze, gniazda, kable, sterowniki na płycie CD lub DVD, oprogramowanie, instrukcje, przewód zasilający, kartę gwarancyjną),
 - 7) wykonawca wskaże w formularzu ofertowym producenta (firmę), typ, model, kraj produkcji oferowanego sprzętu,
- 8) Wykonawca wraz z dostawą przedmiotu zamówienia, zobowiązany będzie dostarczyć:
 - 1) wykaz dostarczonych urządzeń z wyszczególnieniem wszystkich komponentów wchodzących w skład Sprzętu wraz z numerami seryjnymi,
 - 2) instrukcje obsługi/użytkownika Sprzętu opisującą podstawowe funkcje, instrukcje użytkownika Sprzętu,
 - 3) kartę gwarancyjną,
 - 4) oprogramowanie wraz licencjami oraz z kluczami licencyjnymi (o ile dotyczy),
 - 5) wykaz oprogramowania dla dostarczanego Sprzętu z licencją i kluczami licencyjnymi (o ile dotyczy).

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

4. Wymagania dotyczące gwarancji:

- 1) zamawiający wymaga, aby minimalny okres gwarancji, liczony od daty podpisania protokołu zdawczo-odbiorczego, wynosił 12 miesięcy,
- 2) gwarancja obejmuje bezpłatnie: diagnozy, ekspertyzy, konieczne ustawienia i regulacje (ustawienie standardowych parametrów sprzętu), naprawy, koszt transportu sprzętu do miejsca lokalizacji serwisu gwarancyjnego i z powrotem,
- 3) każda naprawa gwarancyjna przedłuża gwarancję o czas przerwy w eksploatacji sprzętu,
- 4) karta gwarancyjna winna być zgodna z wymogami zawartymi w SWZ oraz dostarczona wraz ze sprzętem. Ponadto wykonawca dostarczy oryginalną kartę gwarancyjną producenta (o ile producent wystawia gwarancję) wraz z dostawą sprzętu. Warunki gwarancji nie mogą nakazywać zamawiającemu przechowywania opakowań, w których sprzęt zostanie dostarczony. Jeżeli dla zachowania gwarancji producenta konieczna jest rejestracja sprzętu internetowo wykonawca zobowiązany jest umieścić informację o sprzęcie we właściwych systemach przekazując zamawiającemu wszystkie informacje w tym zakresie.

5. Wymagania dotyczące serwisu:

- 1) czas naprawy sprzętu: 2 dni robocze,
- 2) czas dostawy nowego sprzętu wynikającego z wykonanych trzech napraw tego samego elementu/sprzętu lub braku możliwości naprawy - nie dłużej niż 3 dni robocze,
- 3) w przypadku naprawy trwającej dłużej **niż 2 dni robocze wykonawca od 3 dnia** na czas naprawy zapewnienia sprzęt zastępczy o parametrach nie gorszych niż sprzęt naprawiany,
- 4) w przypadku naprawy trwającej dłużej niż **7 dni roboczych** wykonawca **w 8 dniu** wymieni sprzęt na nowy, w przypadku, gdy sprzęt nie będzie już produkowany, a tym samym dostępny, wykonawca wymieni sprzęt na nowy, równoważny sprzętowi naprawianemu. Wymianę będzie musiał zaakceptować zamawiający.
- 5) wykonawca będzie zobowiązany do zachowania poufności wszelkich danych uzyskanych w trakcie wykonywania czynności serwisowych,
- 6) wykonawcy nie będzie wolno wykonywać żadnych kopii dysków twardych lub danych cząstkowych w trakcie wykonywania napraw gwarancyjnych sprzętu,
- 7) w przypadku trzech napraw tego samego sprzętu/części w okresie gwarancji wykonawca będzie zobowiązany dokonać wymiany sprzętu na nowy o nie gorszych parametrach. Liczba ta nie obejmuje napraw wynikających z niewłaściwej eksploatacji sprzętu przez zamawiającego oraz przypadków losowych niezależnych od wykonawcy. Wymiana nie powoduje zwiększenia kwoty umowy.
- 8) wykonawca zobowiązany będzie do wskazania w ofercie: dokładnej lokalizacji serwisu gwarancyjnego (adres, adres e-mail, tel.) oraz osoby (imię i nazwisko) do kontaktu w sprawie napraw gwarancyjnych,
- 9) wykonawca ponosi odpowiedzialność za udzielone warunki serwisu i gwarancji w niniejszym postępowaniu,
- 10) zgłoszenia serwisowe będą dokonywane za pośrednictwem poczty elektronicznej lub telefonicznie.

6. Warunki dostawy:

- 1) termin dostawy – do 60 dni roboczych od daty zawarcia umowy (zgodnie z ofertą Wykonawcy),
- 2) cena dostarczonego sprzętu musi obejmować: koszt sprzętu, koszt dostawy/transportu do siedziby zamawiającego (bezpośrednio do Jednostki/Katedry), koszt wydania (w tym ubezpieczenia, opakowania i odebrania sprzętu), wniesienie,
- 3) wykonawca zobowiązany jest powiadomić telefonicznie zamawiającego, z co najmniej pięciodniowym wyprzedzeniem, o terminie dostawy sprzętu,
- 4) podstawą do zapłaty wynagrodzenia wykonawcy stanowić będzie protokół zdawczo-odbiorczy, podpisany przez upoważnionych przedstawicieli wykonawcy i zamawiającego,
- 5) termin płatności za dostarczenie i uruchomienie sprzętu – do 30 dni od daty podpisania protokołu zdawczo-odbiorczego i otrzymania prawidłowo wystawionej faktury, na rachunek wykonawcy wskazany w fakturze.

7. Inne wymagania:

- 1) Wykonawca musi być przedstawicielem producenta zaoferowanego sprzętu.

ROZDZIAŁ III.

Termin wykonania zamówienia

Termin dostawy sprzętu wynosi do 60 dni roboczych od daty zawarcia umowy (zgodnie z ofertą Wykonawcy).

ROZDZIAŁ IV.

Warunki udziału w postępowaniu i podstawy wykluczenia

I. Warunki udziału w postępowaniu:

I.1. Zdolności do występowania w obrocie gospodarczym, tj.

Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Brak opisu warunku.

I.2. Uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów, tj.

Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Brak opisu warunku.

I.3. Sytuacji ekonomicznej lub finansowej, tj.

Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Brak opisu warunku.

I.4. Zdolności technicznej lub zawodowej, tj.

Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże należyte wykonanie lub wykonywanie w okresie ostatnich 3 lat (okres wyrażony w latach liczy się wstecz od dnia, w którym upłynął termin składania ofert), a jeżeli okres prowadzenia działalności jest krótszy to w tym okresie, wykonał lub wykonuje co najmniej jedną dostawę sprzętu teleinformatycznego sieciowego o wartości nie niższej niż 50 000,00 zł.

Wykonawca może w celu potwierdzenia 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.

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.

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.

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.

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.

W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, warunek zostanie uznany za spełniony wyłącznie, jeżeli przynajmniej jeden z wykonawców spełnia warunek udziału w postępowaniu.

W celu wstępnego wykazania spełniania warunków udziału w postępowaniu, wykonawca złoży wypełniony formularz Jednolitego Europejskiego Dokumentu Zamówienia (wg wzoru stanowiącego załącznik nr 2 do SWZ) na zasadach określonych w rozdziale V niniejszej SWZ.

Zamawiający informuje, że Wykonawca może ograniczyć się do wypełnienia sekcji α: Ogólne oświadczenie dotyczące wszystkich kryteriów kwalifikacji w części IV JEDZ i nie musi wypełniać żadnej z pozostałych sekcji w części IV JEDZ.

II. Podstawy wykluczenia z postępowania:

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

- 1) w art. 108 ust. 1 ustawy Pzp
- 2) w art. 109 ust. 1 pkt 4) ustawy Pzp

2. Wykonawca może zostać wykluczony przez zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2-5 i 7-10, jeżeli udowodni zamawiającemu, że spełnił łącznie następujące przesłanki:

- 1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
- 2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
- 3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
 - a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
 - b) zreorganizował personel,
 - c) wdrożył system sprawozdawczości i kontroli,
 - d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
 - e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.
4. Zamawiający ocenia, czy podjęte przez wykonawcę czynności, o których mowa w pkt 3., są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w pkt 3, nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza wykonawcę.

ROZDZIAŁ V.

Wykaz dokumentów składanych przez wszystkich wykonawców ubiegających się o udzielenie zamówienia

I. Oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu:

1. Jednolity Europejski Dokument Zamówienia (zwany dalej „JEDZ”, załącznik nr 2 do SWZ)

- 1) zamawiający zaleca wypełnienie formularza JEDZ przy wykorzystaniu dostępu do serwisu internetowego Urzędu Zamówień Publicznych: <https://espd.uzp.gov.pl/>. Procedura jego wypełnienia została opisana w ppkt 3.
- 2) zamawiający dopuszcza możliwość złożenia JEDZ na standardowym formularzu, bez użycia procedury opisanej w ppkt 1, przy czym wykonawca zobowiązany jest do jego wypełnienia w zakresie wskazanym w niniejszej SWZ.
- 3) instrukcja otwarcia załącznika nr 2 do SWZ (dotyczy złożenia JEDZ przy wykorzystaniu serwisu internetowego Urzędu Zamówień Publicznych):
 - a) z Platformy zakupowej: <https://platformazakupowa.pl/pn/urk/proceedings>, w miejscu, w którym została udostępniona SWZ wraz z załącznikami do niniejszego postępowania, z folderu pn. „Załączniki do SWZ” należy pobrać plik w formacie XML (UWAGA: Plik musi zostać zapisany na dysku wykonawcy),
 - b) należy wejść na stronę pod adresem: <https://espd.uzp.gov.pl/> (UWAGA: Podany link należy skopiować i wkleić w pasku przeglądarki internetowej),
 - c) po otwarciu strony głównej serwisu, należy wybrać odpowiednią wersję językową (pl Polski),
 - d) należy wybrać opcję: „JESTEM WYKONAWCĄ” (UWAGA: Tę opcję należy, również zaznaczyć w przypadku, gdy formularz JEDZ wypełnia podmiot, na którego zasoby powołuje się wykonawca),
 - e) należy wybrać opcję: „ZAIMPORTOWAĆ ESPD”,
 - f) kolejno należy „ZAŁADOWAĆ DOKUMENT”, poprzez jego wybór z dysku komputera, o czym mowa w ppkt 3 lit a),
 - g) po poprawnym załadowaniu się dokumentu, należy kliknąć: „DALEJ”,
 - h) w kolejnym kroku wykonawca wypełnia dokument we wskazanym przez system zakresie, a następnie zapisuje go,
 - i) w celu poprawnego pobrania dokumentu należy kliknąć: „PRZEGLĄDAJ”, po czym u dołu strony kliknąć: „POBIERZ, JAKO” i wybrać jedną z opcji do wyboru (zamawiający zaleca, aby zapisać dokument, jako: „FORMAT XML” lub „FORMAT PDF”,
 - j) JEDZ należy złożyć, pod rygorem nieważności, w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
- 4) pozostałe informacje dotyczące poprawnego złożenia formularza JEDZ:

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

- a) do oferty wykonawca dołącza aktualne na dzień składania oferty oświadczenie w zakresie wskazanym przez zamawiającego w ogłoszeniu o zamówieniu lub specyfikacji warunków zamówienia. Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu z postępowania oraz spełnia warunki udziału w postępowaniu
- b) oświadczenie, o którym mowa w ppkt 4 lit. a) wykonawca składa w formie jednolitego dokumentu, na załączniku do SWZ opracowanym przez zamawiającego, o czym mowa w ppkt 3,
- c) wykonawca, który powołuje się na zasoby i podmiotów udostępniających, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu – również składa JEDZ tych podmiotów,
- d) wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia udziału w postępowaniu – również składa JEDZ dotyczący podwykonawców,
- e) w przypadku wspólnego ubiegania się o zamówienie przez wykonawców, JEDZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie,
- f) wykonawca może wykorzystać w JEDZ nadal aktualne informacje zawarte w innym JEDZ złożonym w odrębnym postępowaniu o udzielenie zamówienia,
- g) w przypadku, gdy wykonawca powołuje się w JEDZ na dostępność dokumentów w bezpłatnych, ogólnodostępnych bazach danych państw członkowskich Unii Europejskiej, zobowiązany jest wskazać te bazy danych, aby zamawiający samodzielnie pobrał te dokumenty,
- h) instrukcja wypełnienia JEDZ sporządzona w języku polskim jest dostępna na stronie internetowej Urzędu Zamówień Publicznych pod adresem: https://www.uzp.gov.pl/data/assets/pdf_file/0026/45557/Jednolity-Europejski-Dokument-Zamowienia-instrukcja-2021.01.20.pdf
- i) JEDZ powinien być złożony zgodnie z obowiązującymi aktualnie regulacjami krajowymi odnoszącymi się do składania dokumentów, w tym szczególności przy uwzględnieniu formy wymaganej dla oświadczenia o spełnieniu warunków udziału w postępowaniu.

II. Inne dokumenty:

1. Formularz ofertowy (załącznik nr 1 do SWZ)

- 1) formularz ofertowy należy wypełnić na wzorze opracowanym przez zamawiającego, stanowiącym załącznik nr 1 do SWZ,
- 2) formularz ofertowy należy złożyć, pod rygorem nieważności, w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).

2. Pisemne zobowiązanie podmiotu (załącznik nr 5 do SWZ) tylko, jeżeli wykonawca polega na zasobach podmiotu udostępniającego:

- 1) wykonawca może w celu potwierdzenia spełnienia 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,
- 2) w przypadku, o którym mowa w ppkt 1) wykonawca zobowiązany jest dołączyć do oferty „Pisemne zobowiązanie podmiotu”, którego wzór stanowi załącznik nr 5 do SWZ,
- 3) dokument, o którym mowa w ppkt 2) należy złożyć w oryginale w postaci dokumentu elektronicznego.

3. Dowód wniesienia wadium (w przypadku wadium złożonego w formie poręczeń lub gwarancji)

- 1) jeżeli wadium jest wnoszone w formie gwarancji lub poręczenia, o których mowa w art. 97 ust 7 pkt 2-4 ustawy Pzp, Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia w postaci elektronicznej.

4. Pełnomocnictwo (tylko, jeżeli wykonawcę reprezentuje pełnomocnik).

Pełnomocnictwo należy złożyć w oryginale w postaci dokumentu elektronicznego lub w formie poświadczonej przez notariusza za zgodność z oryginałem.

- 1) pełnomocnictwo należy złożyć w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP),
- 2) pełnomocnictwo poświadczone przez notariusza należy złożyć w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym notariusza, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).

III. Przedmiotowe środki dowodowe:

1. Na potwierdzenie, że oferowane dostawy spełniają wymagania określone przez Zamawiającego w stosunku do przedmiotu zamówienia, Zamawiający żąda złożenia wraz z ofertą następujących przedmiotowych środków dowodowych: opis techniczny zaoferowanego sprzętu zgodnie z Załącznikiem nr 1A do SWZ Parametry Techniczne Przedmiotu Zamówienia. W przypadku, gdy Zamawiający określił w Załączniku nr 1A wymagane parametry techniczne sprzętu poprzez podanie ich zakresu – górnej lub dolnej granicy przedziału wartości, w którym winny się one mieścić, Wykonawca zobowiązany jest do określenia oferowanego parametru poprzez podanie konkretnych wartości. Wykonawca zobowiązany jest również dostarczyć dokument/oświadczenie, że zaoferowany sprzęt pochodzi z autoryzowanego kanału dystrybucji oraz, że Wykonawca jest przedstawicielem producenta zaoferowanego sprzętu.
2. Wykonawca winien podać wszystkie parametry wskazane przez Zamawiającego, nie dopuszcza się możliwości potwierdzenia parametrów słowem TAK.
3. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
4. Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści przedmiotowych środków dowodowych.
5. Zamawiający zastrzega sobie możliwość weryfikacji parametrów technicznych oferowanego sprzętu z Producentem.
6. Parametry Techniczne Przedmiotu Zamówienia należy złożyć, pod rygorem nieważności, w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).

ROZDZIAŁ VI. Podmiotowe środki dowodowe

1. Zamawiający przed wyborem najkorzystniejszej oferty wzywa Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni, aktualnych na dzień złożenia podmiotowych środków dowodowych:

1) „wykaz dostaw (wzór stanowi - załącznik nr 4 do SWZ)”, w którym przedstawione będzie, że dostawy te były wykonane, a w przypadku świadczeń powtarzających się lub ciągłych również są wykonywane w okresie ostatnich 3 lat (okres wyrażony w latach lub miesiącach liczy się wstecz od dnia, w którym upłynął termin składania ofert), a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy.

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

3) informacja z Krajowego Rejestru Karnego w zakresie określonym w

a) art. 108 ust. 1 pkt 1 i 2 ustawy Pzp

b) art. 108 ust. 1 pkt 4 ustawy Pzp, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,

- sporządzone nie wcześniej niż 6 miesięcy przed jej złożeniem,

4) oświadczenie wykonawcy (wzór stanowi – załącznik nr 3 do SWZ), w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r., poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej,

5) oświadczenie wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp, w zakresie podstaw wykluczenia z postępowania wskazanych przez Zamawiającego, o których mowa w :

a) art. 108 ust. 1 pkt 3 ustawy Pzp,

- b) art. 108 ust. 1 pkt 4 ustawy Pzp, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
- c) art. 108 ust. 1 pkt 5 ustawy Pzp, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
- d) art. 108 ust. 1 pkt 6 ustawy Pzp.

2. Dokumenty podmiotów zagranicznych:

- 1) jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast:
 - a) informacji z Krajowego Rejestru Karnego, o której mowa w pkt 1 ppkt 3 – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w pkt 1 ppkt 3. Dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem.
 - b) odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej o której mowa w pkt 1 ppkt 2 składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury. Dokument powinien być wystawiony nie wcześniej niż 3 miesięcy przed jego złożeniem.
- 2) Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ppkt 1, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4 ustawy Pzp, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy. Przepisy dotyczące terminu wystawienia dokumentów stosuje się w odniesieniu do oświadczenia.
- 3) w zakresie nieuregulowanym niniejszą specyfikacją, mają zastosowanie przepisy Rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 r., poz. 2415).

ROZDZIAŁ VII.

Podwykonawstwo oraz wykonawcy wspólnie ubiegający się o zamówienie

1. Podwykonawstwo:

- 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) Powierzenie części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.

2. Wykonawcy wspólnie ubiegający się o zamówienie:

- 1) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty w postaci elektronicznej
- 2) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Jednolity Europejski Dokument Zamówienia (ESPD) składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie te wstępnie potwierdza spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia.
- 3) Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania, w tym oświadczenie dotyczące przynależności lub braku przynależności do tej samej grupy kapitałowej, składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

4) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wskazują w formularzu oferty, które dostawy wykonają poszczególni wykonawcy

ROZDZIAŁ VIII.

Sposób komunikacji oraz wyjaśnienia treści SWZ.

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 (Dz. U. z 2020 r., poz. 344).
2. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformazakupowa.pl pod adresem <https://platformazakupowa.pl/pn/urk>.
3. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
4. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 14 dni przed terminem składania ofert.
5. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w pkt 4 przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia oferty. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie określonym w pkt 4, Zamawiający nie ma obowiązku udzielenia wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
6. Przedłużenie terminu składania ofert, o których mowa w pkt 5, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
7. W celu skrócenia czasu udzielania odpowiedzi na pytania preferuje się, aby komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były w formie elektronicznej za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do Zamawiającego”. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień, informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do Zamawiającego”, po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.
8. Zamawiający będzie przekazywał Wykonawcom informacje w formie elektronicznej za pośrednictwem platformazakupowa.pl. Informację dotyczące odpowiedzi na pytania, zmiany SWZ, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji „Komunikaty”. Korespondencja, które zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem platformazakupowa.pl do konkretnego Wykonawcy.
9. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
10. Zamawiający, zgodnie z rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r., poz. 2452), określa niezbędne wymagania sprzętowo-aplikacyjne umożliwiające prace na 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 przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
 - 4) włączona obsługa JavaScript,
 - 5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików . pdf,
 - 6) platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej – kodowanie UTF8,
 - 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.
11. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
 - 1) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin” oraz uznaje go za wiążący,

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

- 2) zapoznał i stosuje się do Instrukcji składania ofert/wniosek dostępnej pod adresem <https://drive.google.com/file/d/1Kd1DttbBeiNwt4q4sIS4t76lZVKPbkyD/view>
12. Zamawiający informuje, że instrukcje korzystania z 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>
13. Zamawiający wyznacza osobę do bezpośredniego kontaktowania się z wykonawcami: Paulina Żurek, tel. 12 662-44-12, e-mail: paulina.zurek@urk.edu.pl (od poniedziałku do piątku w godz. 7:00 -15:00).

ROZDZIAŁ IX.

Wadium

- Wykonawca zobowiązany jest do zabezpieczenia swojej oferty wadium w wysokości 5 000,00 zł.
- Wadium wnosi się przed upływem terminu składania ofert i utrzymuje nieprzerwanie do dnia upływu terminu związania ofertą, z wyjątkiem przypadków, o których mowa w art. 98 ust. 1 pkt 2 i 3 oraz ust. 2.3. ustawy Pzp.
- Wadium może być wnoszone według wyboru Wykonawcy w jednej lub kilku następujących formach:
 - pieniądzu;
 - gwarancjach bankowych;
 - gwarancjach ubezpieczeniowych;
 - poręczeniach udzielanych 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 (Dz. U. z 2020 r. poz. 299).
- Wadium w formie pieniądza należy wnieść przelewem na konto w Banku **BPH, numer rachunku: 86 2490 0005 0000 4530 1756 3779** z dopiskiem **„Wadium- „Dostawa specjalistycznego sprzętu teleinformatycznego wraz z osprzętem do zarządzania infrastrukturą Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie”, DZP-291-930/2021.** UWAGA: Za termin wniesienia wadium w formie pieniężnej zostanie przyjęty termin uznania rachunku Zamawiającego.
- Wadium wnoszone w formie poręczeń lub gwarancji musi spełniać co najmniej poniższe wymagania:
 - musi obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez Wykonawcę określone w ustawie Pzp, bez potwierdzania tych okoliczności;
 - z jej treści powinno jednoznacznie wynikać zobowiązanie gwaranta do zapłaty całej kwoty wadium;
 - powinno być nieodwołalne i bezwarunkowe oraz płatne na pierwsze żądanie;
 - termin obowiązywania poręczenia lub gwarancji nie może być krótszy niż termin związania ofertą (z zastrzeżeniem iż pierwszym dniem związania ofertą jest dzień składania ofert);
 - w treści poręczenia lub gwarancji powinna znaleźć się nazwa oraz numer przedmiotowego postępowania;
 - beneficjentem poręczenia lub gwarancji jest: Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie;
 - w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (art. 58 ustawy 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);
 - musi zostać złożone w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym przez wystawcę poręczenia lub gwarancji.
- W przypadku wniesienia wadium w formie:
 - pieniężnej - zaleca się, by dowód dokonania przelewu został dołączony do oferty;
 - poręczeń lub gwarancji - wymaga się, by oryginał dokumentu został złożony wraz z ofertą.
- Oferta wykonawcy, który nie wnieśli wadium lub wnieśli w sposób nieprawidłowy lub nie utrzyma wadium nieprzerwanie do upływu terminu związania ofertą lub złoży wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 ustawy Pzp zostanie odrzucona.
- Zasady zwrotu oraz okoliczności zatrzymania wadium określa ustawa Pzp.

ROZDZIAŁ X.

Termin związania ofertą

- Wykonawca będzie związany ofertą od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu

- związania ofertą jest dzień, w którym upływa termin składania ofert, przez okres 90 dni, tj. do dnia 18.09.2021 r.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa 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 60 dni.
 3. Przedłużenie terminu związania ofertą, o którym mowa w pkt 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
 4. W przypadku gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa w pkt 2, następuje wraz z przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

ROZDZIAŁ XI.

Opis sposobu przygotowania ofert

1. Wykonawca może złożyć tylko jedną ofertę na dowolną ilość Zadań.
2. Treść oferty musi odpowiadać treści SWZ.
3. Oferta powinna być:
 - 1) sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
 - 2) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
 - 3) podpisana kwalifikowanym podpisem elektronicznym
4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie 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".
5. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików XAdES.
6. Sposób sporządzania i przekazywania informacji:
 - 1) Dokumenty elektroniczne przekazuje się w postępowaniu przy użyciu środków komunikacji elektronicznej wskazanych przez zamawiającego.
 - 2) Oferty, oświadczenia, o których mowa w art. 125 ust. 1 ustawy, podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust. 3 ustawy Pzp, przedmiotowe środki dowodowe, pełnomocnictwo, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568, 695, 1517 i 2320), z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, z uwzględnieniem rodzaju przekazywanych danych.
 - 3) Informacje, oświadczenia lub dokumenty, inne niż określone w pkt 2, przekazywane w postępowaniu, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej.
 - 4) W przypadku, gdy dokumenty elektroniczne w postępowaniu przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.
 - 5) Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
 - 6) W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy Pzp lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, jako dokument elektroniczny, przekazuje się ten dokument.
 - 7) W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu

- opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
- 8) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 7), dokonuje w przypadku:
 - a) podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania - odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
 - b) przedmiotowych środków dowodowych - odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;
 - c) innych dokumentów - odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
 - 9) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w 7), może dokonać również notariusz.
 - 10) Przez cyfrowe odwzorowanie należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
 - 11) Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.
 - 12) W przypadku, gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
 - 13) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 12), dokonuje w przypadku:
 - a) podmiotowych środków dowodowych - odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą
 - b) przedmiotowego środka dowodowego, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy Pzp, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;
 - c) pełnomocnictwa - mocodawca.
 - 14) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 12), może dokonać również notariusz.
7. 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.
8. Wykonawca, za pośrednictwem 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>
9. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje podlegać będzie odrzuceniu.
10. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
11. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.

12. 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.
13. 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.
14. 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 Pzp.
15. 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.
16. 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.
17. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
18. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
19. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
20. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
21. Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
22. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
23. Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.

ROZDZIAŁ XII.

Sposób i termin składania i otwarcia ofert

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: <https://platformazakupowa.pl/pn/urk> w myśl ustawy Pzp na stronie internetowej prowadzonego postępowania do dnia 21.06.2021 r. do godziny 11:00.
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
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. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 1 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 formie elektronicznej.
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 21.06.2021 r. o godzinie 11:30.
8. W przypadku awarii systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

9. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
10. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
11. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia 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 postępowania na platformazakupowa.pl w sekcji „Komunikaty” .

ROZDZIAŁ XIII.

Opis sposobu obliczania ceny

1. Cenę ofertową należy podać w formularzu „OFERTA” stanowiącym załącznik nr 1 do SWZ.
2. Podana w ofercie cena musi być wyrażona w PLN (z dokładnością do dwóch miejsc po przecinku).
3. Cenę oferty należy obliczyć jako **ryczałtowe wynagrodzenie w złotych brutto** Wykonawcy (brutto, tj.: z podatkiem VAT i innymi należnościami publicznoprawnymi zgodnie z obowiązującymi przepisami).
4. Cenę oferty należy wyliczyć w oparciu o warunki i wymagania zawarte w niniejszej SWZ, własne doświadczenie profesjonalisty, uwzględniając wykonanie całości przedmiotu zamówienia zgodnie z wymaganiami zawartymi w SWZ, ze wszelkimi tego kosztami bezpośrednimi i pośrednimi niezbędnymi do należytej oraz zgodne z obowiązującymi przepisami realizacji przedmiotu zamówienia.
5. Stawkę podatku VAT należy określić zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz.U. 2020 r., poz. 106 ze zm.).
6. Cena oferty podana w ofercie nie ulegnie zmianie przez cały okres obowiązywania umowy.
7. Wyliczona cena oferty brutto będzie służyć do porównania złożonych ofert i do rozliczenia w trakcie realizacji zamówienia.
8. W przypadku zastosowanie przez Wykonawcę wysokości podatku innego niż podstawowy , poda ona podstawę prawną jego zastosowania oraz dołączy dokumenty (certyfikaty, deklaracje) potwierdzające jego zastosowanie.
9. W przypadku zastosowania przez Wykonawcę dwóch stawek podatku VAT przy oferowaniu 1 urządzenia (Zadania), winien rozpisać wartość brutto podając cenę netto i stawki podatku VAT.
10. 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.
11. 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 miały obowiązek rozliczyć. W ofercie, o której mowa w ust. 1, Wykonawca ma obowiązek : poinformować Zamawiającego, że wybór jego oferty 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.
12. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
13. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty

ROZDZIAŁ XIV.

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:

Lp.	Kryteria oceny	Ilość punktów	Ilość punktów
1.	Cena sprzętu (C)	0-60	wg wzoru:

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

			$C = (C_{min} / C_o) \times 60$ gdzie: C – liczba punktów przyznana danej ofercie w kryterium cena Co – cena brutto badanej oferty Cmin – najniższa cena brutto spośród złożonych ofert Wykonawców Wyliczenie punktów zostanie dokonane z dokładnością do dwóch miejsc po przecinku. 1% = 1 pkt 60% = 60 pkt
2.	Okres gwarancji (G)	0-25	wg wzoru: $G = [(G_o - G_{min}) / (G_{max} - G_{min})] \times 25$ gdzie: G - liczba punktów przyznana danej ofercie w kryterium okres gwarancji Go - okres gwarancji badanej oferty Gmin - najkrótszy dopuszczalny okres gwarancji wynosi 12 miesięcy, Gmax – najdłuższy dopuszczalny okres gwarancji wynosi 60 miesięcy – Okres gwarancji udzielony na ponad 60 miesięcy nie będzie dodatkowo punktowany, a do wzoru zostanie podstawiony jako 60-miesięczny okres gwarancji. – Za zaoferowanie minimalnego wymaganego 12-miesięcznego okresu, Wykonawcy zostanie przyznane 0 pkt. w kryterium okres gwarancji. 1% = 1 pkt 25% = 25 pkt
3	Termin dostawy (D)	0-15	$D = [(D_{max} - D_o) / (D_{max} - D_{min})] \times 15$ gdzie: D - liczba punktów przyznana danej ofercie w kryterium „termin dostawy”, Do - termin dostawy badanej, nieodrzuconej oferty, Dmax - najdłuższy dopuszczalny termin dostawy – 60 dni roboczych, Dmin – najkrótszy dopuszczalny termin dostawy – 1 dzień roboczy, 1) Najkrótszy termin dostawy, jaki może zaoferować wykonawca to 1 dzień roboczy, 2) Maksymalny termin dostawy, jaki może zaoferować wykonawca to 60 dni roboczych. 3) Za zaoferowanie maksymalnego, dopuszczalnego 60-dniowego terminu dostawy, wykonawcy zostanie przyznane 0 pkt w tym kryterium.

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

			1% = 1 pkt 15% = 15 pkt
	razem	100 pkt.	
<p>✓ Ilość punktów, jaką uzyska oferta będzie stanowić końcową ocenę danej oferty i zostanie obliczona według wzoru:</p> <p style="text-align: center;">O = C + G + D</p> <p>gdzie:</p> <p>O – całkowita liczba punktów uzyskana przez badaną ofertę C – liczba punktów przyznana ofercie w kryterium cena G – liczba punktów przyznana ofercie w kryterium gwarancja D – liczba punktów przyznana ofercie w kryterium „termin dostawy”,</p> <p>✓ 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</p>			

Zamawiający w przypadku, gdy Wykonawca w formularzu ofertowym nie wskaże okresu gwarancji dla zaoferowanego sprzętu, dokona obliczenia punktów w kryterium okres gwarancji, a do wzoru zostanie wskazany najkrótszy dopuszczalny okres gwarancji.

Zamawiający w przypadku, gdy Wykonawca w formularzu ofertowym nie wskaże terminu dostawy dla zaoferowanego sprzętu, dokona obliczenia punktów w kryterium termin dostawy, a do wzoru zostanie wskazany maksymalny termin dostawy.

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 wybiera 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. Oferta Wykonawcy może otrzymać maksymalnie 100 punktów.

ROZDZIAŁ XV.

Informacje o dopełnieniu formalności po wyborze najkorzystniejszej oferty

- Zamawiający udzieli zamówienia wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszej SWZ i została oceniona jako najkorzystniejsza w oparciu o podane wyżej kryteria oceny ofert.
- Zamawiający poinformuje niezwłocznie po wyborze oferty wszystkich wykonawców, którzy złożyli oferty o:
 - wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
 - wykonawcach, których oferty zostały odrzucone,
 - podając uzasadnienie faktyczne i prawne.
- Zamawiający zamieści w na stronie prowadzonego postępowania informację, o których mowa w art. 253 ust. 1 pkt 1 ustawy Pzp.
- Zamawiający zawrze umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 ustawy Pzp, w terminie nie krótszym niż 10 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 15 dni - jeżeli zostało przesłane w inny sposób.

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

5. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt 4, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie przetargu nieograniczonego złożono tylko jedną ofertę.

ROZDZIAŁ XVI.

Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XVII.

Postanowienia końcowe

1. Wzór umowy stanowi załącznik nr 6 do SWZ.
2. W przypadku wskazania w ofercie wykonawcy podwykonawców, zamawiający dokona stosownych zmian we wzorze umowy.
3. Przed podpisaniem umowy wykonawca powinien wykazać, że osoba/y reprezentująca wykonawcę jest umocowana do jego reprezentacji i zaciągania w jego imieniu zobowiązań.

ROZDZIAŁ XVIII.

Środki ochrony prawnej

1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy Pzp.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie 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 postanowienie umowy;
 - 2) zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy;
4. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej.
6. Odwołanie wnosi się w terminie:
 - 1) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
 - 2) 15 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).
7. Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia
8. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp., stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
9. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17.11.1964 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

Projekt „Innowacyjny program strategicznego rozwoju Uczelni” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego.

23.11.2012 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 XIX.

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 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie ogólne), niniejszym informujemy, iż:

1. Administratorem Pana/Pani danych osobowych będzie Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, al. Adama Mickiewicza 21, 31-120 Kraków.

2. Uniwersytet Rolniczy powołał inspektora ochrony danych, z którym należy kontaktować się za pomocą adresu e-mail: iod@urk.edu.pl.

3. Pani/Pana dane osobowe będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn.: „*Dostawa specjalistycznego sprzętu teleinformatycznego wraz z osprzętem do zarządzania infrastrukturą Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie*”, nr zamówienia: **DZP-291-930/2021** prowadzonym w trybie przetargu nieograniczonego oraz celów związanych z realizacją i rozliczaniem umowy zawartej w wyniku tego postępowania (o ile dojdzie do zawarcia umowy), na podstawie art. 6 ust. 1 lit. c) Rozporządzenia ogólnego, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

4. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych osobowych wynikają z ustawy Pzp.

5. Posiada Pani/Pan prawo do:

- 1) dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych¹,
- 2) przenoszenia danych,
- 3) wniesienie sprzeciwu wobec przetwarzania – w przypadkach i na warunkach określonych w Rozporządzeniu ogólnym;

6. Pani/Pana dane osobowe mogą zostać udostępniane innym odbiorcom. Ewentualnymi odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp lub osoby/podmioty/organy kontrolujące, którym zamawiający zobowiązany jest udostępnić dokumentację postępowania.

7. Pani/Pana dane osobowe będą przetwarzane przez okres wynikający z obowiązujących przepisów prawa;

Posiada Pani/Pan prawo wniesienia skargi do właściwego organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z przepisami Rozporządzenia ogólnego.

8. Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym w formie profilowania.

9. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

II. Zgodnie z art 14 ust 1 i 2 Rozporządzenia ogólnego, niniejszym informujemy, iż:

1. Administratorem Pana/Pani danych osobowych będzie Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, al. Adama Mickiewicza 21, 31-120 Kraków.

2. Administrator prowadzi operacje przetwarzania następujących kategorii Pani/Pana danych osobowych:

- 1) imię, nazwisko;

¹ Skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp.

Prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

W przypadku, gdy wykonanie obowiązków prawa dostępu, przysługującego osobie, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji:

- mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.
- mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.

Wystąpienie z żądaniem ograniczenia przetwarzania, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.

- 2) służbowy numer telefonu*;
 - 3) posiadane uprawnienia i kwalifikacje (w określonym zakresie)*;
 - 4) nazwa i adres pracodawcy*;
 - 5) podstawa zatrudnienia (rodzaj umowy), datę zawarcia umowy*;
 - 6) rodzaj czynności (prac) wykonywanych w ramach umowy o pracę*;
 - 7) fakt zgłoszenia pracownika przez pracodawcę do ubezpieczenia*;
- * jeśli dotyczy.
3. Uniwersytet Rolniczy powołał inspektora ochrony danych, z którym należy kontaktować się za pomocą adresu e-mail: iod@urk.edu.pl
 4. Pani/Pana dane osobowe będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn.: **„Dostawa specjalistycznego sprzętu teleinformatycznego wraz z osprzętem do zarządzania infrastrukturą Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie”**, nr zamówienia: **DZP-291-930/2021** prowadzonym w trybie przetargu nieograniczonego oraz celów związanych z realizacją i rozliczaniem umowy zawartej w wyniku tego postępowania (o ile dojdzie do zawarcia umowy), na podstawie art. 6 ust. 1 lit. c) Rozporządzenia ogólnego, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.
 5. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych osobowych wynikają z ustawy Pzp.
 6. Posiada Pani/Pan prawo do:
 - 1) dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych²,
 - 2) przenoszenia danych,
 - 3) wniesienie sprzeciwu wobec przetwarzania – w przypadkach i na warunkach określonych w Rozporządzeniu ogólnym.
 7. Pani/Pana dane osobowe mogą zostać udostępniane innym odbiorcom. Ewentualnymi odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy Pzp, lub osoby/podmioty/organy kontrolujące, którym zamawiający zobowiązany jest udostępnić dokumentację postępowania.
 8. Pani/Pana dane osobowe będą przetwarzane przez okres wynikający z obowiązujących przepisów prawa.
 9. Posiada Pani/Pan prawo wniesienia skargi do właściwego organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, gdy uzasadnione jest, że Pana/Pani dane osobowe przetwarzane są przez administratora niezgodnie z przepisami Rozporządzenia ogólnego.
 10. Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym w formie profilowania.
 11. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.
 12. Inspektor Ochrony Danych Uniwersytetu Rolniczego w Krakowie realizuje swój obowiązek informowania kontrahentów pełniących rolę podmiotów przetwarzających o obowiązkach spoczywających na nich, wynikających 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 (ogólne rozporządzenie o ochronie danych), wynikający z art. 39 ust. 1 litera a) tego rozporządzenia, poprzez swoją stronę internetową <https://iod.urk.edu.pl>, na której umieścił stosowne informacje.

² Skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp.

Prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

W przypadku, gdy wykonanie obowiązków prawa dostępu, przysługującego osobie, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji:

- mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.
- mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.

Wystąpienie z żądaniem ograniczenia przetwarzania, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.



ROZDZIAŁ XX.

Ustalenia końcowe

W sprawach nie uregulowanych w niniejszej specyfikacji będzie stosowana ustawa z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych oraz Kodeks Cywilny.

Kraków, dnia 18.05.2021 r.

Kanclerz
/-/ mgr Tomasz Szanser

.....
(podpis)