Fundusze Europejskie dla Rozwoju Społecznego

Dofinansowane przez Unię Europejską

Politechnika Białostocka
Dział Aparatury i Zakupów
ul. Zwierzyniecka 10, 15-333 Białystok
tel. (85) 746 7042, (85) 746 9035
email: aparatura@pb.edu.pl

Numer sprawy: ZK-DAZ.262.592.2026

Białystok, dn. 17.11.2026

# ZAPYTANIE OFERTOWE NA:
## Przeprowadzenie szkolenia z obszaru cyberbezpieczeństwa

na potrzeby projektu: Projekt „PB 5.0 – dostosowanie oferty dydaktycznej Politechniki Białostockiej do potrzeb nowoczesnej gospodarki oraz zielonej i cyfrowej transformacji" (nr umowy FERS.01.05-IP.08-0327/23-00 z dnia 14.06.2024 r.) realizowanego w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus.

Postępowanie nie podlega ustawie z dnia 11 września 2019 r. Prawo zamówień publicznych – podstawa prawna: art. 2 ust. 1 pkt 1 ustawy Pzp

### 1. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

**Dane Zmawiającego**:

Politechnika Białostocka, Wiejska 45A, 15-351 Białystok REGON: 000001672, NIP: 542-020-87-21

**Adres strony internetowej:** http://www.pb.edu.pl/

**Osoba do kontaktu z Wykonawcami: Marta Gudel., tel. 85 746 7042**

**E-mail do korespondencji: m.gudel@pb.edu.pl**

**Godziny pracy:** Poniedziałek – Piątek: 7:30 – 15:30

### 2. PROCEDURA UDZIELENIA ZAMÓWIENIA

1) Postępowanie jest prowadzone w trybie zapytania ofertowego, zwanego dalej „Zapytaniem", dla którego nie mają zastosowania przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605, z późn. zm.).
2) **Komunikacja odbywać się będzie w formie elektronicznej** - za pośrednictwem **Bazy Konkurencyjności** pod adresem internetowym https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl, na zasadach określonych w Zapytaniu.

### 3. OPIS PRZEDMIOTU ZAMÓWIENIA

1) **Kod CPV :** 80510000-2 – Usługi szkolenia specjalistycznego,
2) **Przedmiotem zamówienia jest:**
Przedmiotem zamówienia jest przeprowadzenie szkolenia z obszaru praktycznej analizy cyberzagrożeń, zarządzania podatnościami i reagowania na incydenty bezpieczeństwa (Cybersecurity Analyst / SOC). Celem szkolenia jest rozwój praktycznych kompetencji w monitorowaniu systemów i sieci, identyfikacji zagrożeń, analizie podatności, obsłudze incydentów oraz dokumentowaniu wyników analiz.

Szkolenie obejmuje 28 godzin dydaktycznych (po 45 minut każda) i powinno mieć charakter teoretyczno-praktyczny, z przewagą ćwiczeń laboratoryjnych i warsztatowych. Szkolenie powinno być realizowane w formie zdalnej (online), w czasie rzeczywistym, z bezpośrednim udziałem trenera i możliwością bieżącej interakcji z uczestnikami.

Szkolenie jest przeznaczone dla jednej grupy liczącej 28 studentów V semestru studiów inżynierskich pierwszego stopnia kierunku Informatyka, posiadających podstawową znajomość systemów Windows i Linux, sieci TCP/IP, bezpieczeństwa systemów oraz programowania w tym tworzenia skryptów powłoki. Nie wymaga się doświadczenia zawodowego w cyberbezpieczeństwie ani znajomości narzędzi SOC.

### 2.1. Zakres merytoryczny szkolenia

Wykonawca powinien zapewnić program obejmujący co najmniej następujące zagadnienia:

a) Operacje bezpieczeństwa (Security Operations): funkcjonowanie SOC i procesów monitorowania; analiza logów systemowych i ruchu sieciowego; wykorzystanie narzędzi SIEM oraz podstawy EDR/XDR; korelacja zdarzeń i analiza alertów; identyfikacja i analiza cyberzagrożeń z wykorzystaniem informacji o zagrożeniach i technikach ataków (np. Threat Intelligence, IoC, TTP, MITRE ATT&CK); wykrywanie podejrzanej aktywności w systemach i sieciach.

b) Zarządzanie podatnościami (Vulnerability Management): proces wykrywania i obsługi podatności, podstawy patch management; metody i narzędzia skanowania systemów, sieci i usług; interpretacja wyników, CVE i CVSS; weryfikacja i kontekstowa ocena ryzyka, priorytetyzacja działań naprawczych oraz opracowanie zaleceń.

c) Reagowanie na incydenty (Incident Response): przygotowanie do obsługi incydentów, triage, klasyfikacja i eskalacja; analiza incydentów phishingowych, podejrzanych procesów, połączeń i artefaktów; podstawy zabezpieczania materiału dowodowego; ograniczanie skutków, usuwanie przyczyn, odtwarzanie działania i analiza poincydentalna.

d) Raportowanie i komunikacja (Reporting and Communication): dokumentowanie ustaleń i przebiegu analizy, przygotowywanie raportów o podatnościach i incydentach, komunikowanie ryzyka oraz rekomendowanie działań technicznych i organizacyjnych.

e) Zagadnienia uzupełniające: podstawy oceny podatności aplikacji WWW i usług chmurowych, mechanizmy ograniczania skutków ataków oraz wykorzystanie skryptów (np. Python, PowerShell, Bash) do wspomagania analizy danych bezpieczeństwa.

### 2.2. Wymagania organizacyjne i techniczne

a) Wykonawca zapewni każdemu uczestnikowi indywidualny dostęp do interaktywnego środowiska laboratoryjnego podczas szkolenia oraz przez okres co najmniej 6 miesięcy od jego zakończenia, z

możliwością korzystania z laboratoriów również poza godzinami zajęć. Dostęp powinien być realizowany preferencyjnie przez przeglądarkę internetową.

b) Laboratoria powinny obejmować przygotowane scenariusze i instrukcje ćwiczeń oraz umożliwiać praktyczną pracę co najmniej w zakresie analizy zdarzeń i ruchu sieciowego, wykrywania zagrożeń, zarządzania podatnościami oraz reagowania na incydenty bezpieczeństwa.

c) Dostęp do laboratoriów po zakończeniu szkolenia powinien umożliwiać samodzielne i wielokrotne wykonywanie ćwiczeń praktycznych odpowiadających zakresowi szkolenia. Sam dostęp do nagrań, prezentacji, materiałów szkoleniowych lub testów nie spełnia tego wymagania.

d) W cenie szkolenia powinny być uwzględnione wszystkie niezbędne licencje, konta użytkowników, materiały szkoleniowe, wsparcie techniczne w trakcie zajęć oraz koszty dostępu do laboratoriów przez wymagany okres.

**2.3. Dokumentowanie efektów uczenia się**

a) Po zakończeniu szkolenia uczestnicy powinni otrzymać certyfikat potwierdzający udział w szkoleniu. Certyfikat powinien zawierać co najmniej:

- nazwę i logo wykonawcy szkolenia,
- imię i nazwisko uczestnika,
- tytuł szkolenia,
- liczbę godzin szkoleniowych,
- datę lub okres realizacji szkolenia,
- informację o ukończeniu szkolenia,
- miejsce i datę wystawienia certyfikatu,
- numer identyfikacyjny certyfikatu (opcjonalnie),
- podpis osoby upoważnionej / pieczęć wykonawcy,
- minimum 5 efektów uczenia przewidzianych do osiągnięcia przez uczestników w ramach szkolenia, zamieszczonych na certyfikacie lub stanowiących integralny załącznik do certyfikatu, w tym co najmniej:
  - dwa efekty w zakresie wiedzy (uczestnik posiada uporządkowaną wiedzę z zakresu …; uczestnik zna aktualne regulacje / narzędzia / metody …),
  - dwa efekty w zakresie umiejętności (uczestnik potrafi zastosować …),
  - jeden efekt w zakresie kompetencji społecznych (uczestnik jest gotów do…; uczestnik jest przygotowany do samodzielnego …).

Efekty uczenia:

- powinny być spójne z programem szkolenia,

- powinny wskazywać kompetencje, wiedzę i umiejętności nabyte przez uczestnika,
- powinny umożliwiać weryfikację przyrostu wiedzy i umiejętności z wykorzystaniem pretestu i posttestu.

b) Wykonawca zobowiązany jest również do przeprowadzenia pretestu oraz posttestu umożliwiających ocenę stopnia osiągnięcia efektów uczenia przewidzianych w programie szkolenia przez uczestników szkolenia. Wyniki testów powinny zostać przekazane Zamawiającemu drogą elektroniczną na wskazane adresy e-mail.

c) Certyfikat nie może zawierać ocen, wyników testów ani procentowego poziomu osiągnięcia efektów uczenia.

3) **Możliwość składanie ofert częściowych –NIE**

4) **Termin realizacji: do 20.12.2026**

5) **Termin płatności: do 30 dni** kalendarzowych od dnia otrzymania faktury.

6) **Szczegółowe warunki realizacji zamówienia określa projekt umowy stanowiący załącznik nr 5 do Zapytania ofertowego (jeśli dotyczy)**

## 4. WARUNKI UDZIAŁU W POSTĘPOWANIU

O zamówienie mogą ubiegać się Wykonawcy, posiadający odpowiednie kwalifikacje oraz doświadczenie zawodowe i dydaktyczne w obszarze cyberbezpieczeństwa. Trener przeprowadzający szkolenie powinien spełniać następujące minimalne wymagania:

- posiadać co najmniej 5 lat doświadczenia zawodowego w obszarze cyberbezpieczeństwa, obejmującego praktyczne działania związane z analizą zagrożeń, monitorowaniem bezpieczeństwa, zarządzaniem podatnościami lub reagowaniem na incydenty;
- posiadać doświadczenie w prowadzeniu specjalistycznych szkoleń technicznych dla osób dorosłych, w szczególności zajęć o charakterze praktycznym i warsztatowym;
- wykazać przeprowadzenie co najmniej 150 godzin zajęć szkoleniowych w zakresie cyberbezpieczeństwa lub tematyki zbieżnej z przedmiotem zamówienia w okresie ostatnich 3 lat.

Spełnienie powyższych wymagań powinno zostać potwierdzone oświadczeniem Wykonawcy. Zamawiający zastrzega sobie prawo do żądania dokumentów potwierdzających doświadczenie trenera, w szczególności wykazu przeprowadzonych szkoleń lub informacji o jego doświadczeniu zawodowym.

## 5.WERYFIKACJA PRZESŁANEK WYKLUCZENIA WYKONAWCY

Zamawiający dokona weryfikacji samoistnych i obligatoryjnych przesłanek wykluczenia Wykonawcy o których mowa w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).

Na podstawie art. 7 ust. 1 ww. ustawy z postępowania o udzielenie zamówienia publicznego wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

**Zamawiający dokona weryfikacji przesłanek wykluczenia w oparciu o złożone wraz z ofertą Oświadczenie o niepodleganiu wykluczeniu (wg wzoru – zał. Nr 2 do zapytania ofertowego).**

**Zakaz konfliktu interesów**

Z udziału w postępowaniu wyklucza się Wykonawców powiązanych z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą

**Zamawiający dokona weryfikacji przesłanek braku konfliktu interesów w oparciu o złożone wraz z ofertą Oświadczenie o braku powiązań osobowych lub kapitałowych (wg wzoru – zał. Nr 5 do zapytania ofertowego).**

## 6. WYMAGANE DOKUMENTY I OŚWIADCZENIA, KTÓRE NALEŻY ZŁOŻYĆ WRAZ Z OFERTĄ

1. Zamawiający wymaga, aby oferta zawierała:
   1) **Wypełniony formularz ofertowy** (wg wzoru – zał. nr 1 do Zapytania ofertowego).
   2) **Oświadczenia**( wg załącznika nr 2 do Zapytania ofertowego)
   3) **Pełnomocnictwo** do podpisania oferty, o ile prawo do podpisania oferty nie wynika z dokumentów rejestrowych lub innych dokumentów złożonych wraz z ofertą.

4) **Oświadczenie wykonawcy** dotyczące przesłanek wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego ( wg załącznika nr 4 do Zapytania ofertowego)
5) **Oświadczenie wykonawcy o braku powiązań osobowych lub kapitałowych** ( wg załącznika nr 6 do Zapytania ofertowego).

2. Formularz oferty nie podlega uzupełnieniu. Niezałączenie lub załączenie niepodpisanego Formularza ofertowego skutkować będzie odrzuceniem oferty z postępowania.
3. Niezałączenie lub załączenie niepodpisanego Oświadczenia o niepodleganiu wykluczeniu (z zastrzeżeniem wezwania do jego złożenia) skutkować będzie wykluczeniem Wykonawcy z postępowania i uznaniem jego oferty za odrzuconą.

## 7 INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1) Wszelkie oświadczenia, wnioski, pytania, zawiadomienia oraz inne informacje Zamawiający i Wykonawcy przekazują za pośrednictwem Bazy Konkurencyjności. W tytule wiadomości e-mail należy podać numer referencyjny sprawy, której ona dotyczy.
2) Ofertę sporządzona się w języku polskim, zgodnie z treścią Formularza ofertowego, którego wzór stanowi załącznik do Zapytania. Oferta musi być podpisana przez osobę (osoby) upoważnioną(e) do reprezentowania Wykonawcy.
3) Oferta (formularz ofertowy) oraz pozostałe dokumenty składane wraz z ofertą powinny zostać złożone w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Jeśli Wykonawca nie dysponuje takimi podpisami, Zamawiający dopuszcza również złożenie oferty w postaci kopii (skanów) dokumentów podpisanych przez osoby upoważnione.
4) Załączanie dokumentów odbywa się przy użyciu funkcjonalności „Dodaj dokument" w sekcji „Dokumenty" w zakładce „Oferta" i wybraniu docelowego pliku który ma zostać wczytany. Wykonawca winien opisać załącznik nazwą umożliwiającą jego identyfikację.

## 8 TERMIN ZWIĄZANIA OFERTĄ

1) Termin związania ofertą wynosi **30 dni**.
2) Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

## 9. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1) Ofertę należy złożyć na Bazie Konkurencyjności w zakładce **„OFERTY"** do dnia 25.11.2026 **r. do godz.** 10°°
2) Otwarcie ofert nastąpi w dniu 25.11.2026 **r. do godz.** 10°°

## 10. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY

1) Przy wyborze oferty Zamawiający będzie się kierował kryteriami:

   **Cena** - waga **100 %**

   Sposób obliczenia ceny:

   Oferta z najniższą ceną brutto otrzyma 100 punktów, pozostałe oferty otrzymają punkty proporcjonalnie według wzoru:

   najniższa cena / cena badanej oferty) × 100.

2) Cena oferty winna obejmować wszelkie koszty jakie poniesie Wykonawca przy realizacji zamówienia (koszt transportu, ew. ubezpieczenia, itp.) z uwzględnieniem wszystkich opłat i podatków;
3) Za najkorzystniejszą ofertę zostanie uznana oferta przedstawiająca najkorzystniejszy bilans ceny i pozostałych kryteriów (*o ile zostały określone*);
4) O wyborze oferty Zamawiający zawiadomi poprzez upublicznienie na Bazie Konkurencyjności informacji o wyborze oferty najkorzystniejszej.

## 11. ZAMAWIAJĄCY ZASTRZEGA SOBIE PRAWO DO:

1) Zmiany terminu składania ofert;
2) Nieudzielenia odpowiedzi na pytania Wykonawców;
3) Zmiany treści Zapytania;
4) Poprawienia oczywistych omyłek pisarskich i rachunkowych w ofercie;
5) Wezwania Wykonawcy do złożenia wyjaśnień dotyczących treści złożonej oferty;
6) Wezwania Wykonawcy do uzupełnienia oferty o wymagane dokumenty i oświadczenia;
7) Odrzucenia oferty wraz z podaniem uzasadnienia;
8) Przeprowadzenia negocjacji z wybranym przez siebie Wykonawcą, w przypadku braku ofert lub gdy wszystkie oferty podlegają odrzuceniu;
9) Przeprowadzenia negocjacji cenowych z Wykonawcą, który złożył najkorzystniejszą ofertę, w przypadku, gdy cena najkorzystniejszej oferty przekracza kwotę przeznaczoną na realizację zamówienia;
10) Unieważnienia Zapytania bez podania przyczyny (na każdym etapie postępowania) i bez ponoszenia jakichkolwiek skutków prawnych i finansowych.

## 12. ZMIANY W UMOWIE

1. Zamawiający przewiduje możliwość zmiany umowy, w przypadku:
   1) gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa (w tym przepisów podatkowych) w zakresie mającym wpływ na realizację przedmiotu zamówienia;
   2) gdy konieczność wprowadzenia zmian będzie następstwem zmian wprowadzonych w umowach pomiędzy Zamawiającym, a inną niż Wykonawca stroną, w szczególności instytucją Zarządzającą,

Pośredniczącą, a także innymi instytucjami, które na podstawie przepisów prawa mogą wpływać na realizację zamówienia;

3) gdy konieczność wprowadzenia zmian będzie następstwem zmian wytycznych dotyczących programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 lub wytycznych i zaleceń Instytucji Zarządzającej lub Instytucji Pośredniczącej, w szczególności w zakresie sprawozdawczości.

2. Zamawiający dopuszcza wprowadzenie istotnych zmian do niniejszej umowy w stosunku do treści Oferty, na podstawie której dokonano wyboru Wykonawcy dotyczących:
   1) terminu wykonania zamówienia; w uzasadnionych przypadkach, po wcześniejszym uzgodnieniu z Zamawiającym,
   2) jakości lub parametrów oferty.
3. Zmiany, o których mowa w ustępie 1 i 2 mogą być dokonane w następujących przypadkach:
   1) konieczność zmiany terminu wykonania zamówienia z powodu:
      a) działania siły wyższej, tj. nadzwyczajnego zdarzenia lub okoliczności, których nie można było przewidzieć ani im zapobiec;
      b) zaistnienia okoliczności nie leżących po stronie Wykonawcy, gdy wykonywanie zamówienia nie było możliwe lub Wykonawca miał w istotny sposób utrudnione możliwości w spełnianiu świadczenia (Wykonawca może zwrócić się do Zamawiającego z uzasadnionym wnioskiem o przedłużenie terminu wykonania zamówienia);
      c) z przyczyn zależnych od Zamawiającego;
      d) jeżeli zmiany są niezbędne dla prawidłowej realizacji przedmiotu zamówienia.
   2) gdy zmiany są korzystne dla Zamawiającego,
4. Do wprowadzenia jakichkolwiek zmian niezbędne jest wyrażenie zgody przez Strony w formie pisemnego aneksu pod rygorem nieważności.
5. Zmiany mogą być inicjowane przez Zamawiającego lub Wykonawcę, z tym zastrzeżeniem, że żaden z powyższych zapisów nie obliguje Zamawiającego do wprowadzenia jakiejkolwiek zmiany, a jedynie wprowadza taką możliwość. Strona wnioskująca o zmianę Umowy, przedkłada drugiej stronie pisemne uzasadnienie konieczności wprowadzenia zmian do Umowy.
6. Zmiana musi być uzasadniona prawidłową realizacją przedmiotu umowy.
7. Zmiany umowy przewidziane powyżej dopuszczalne są w zakresie nie powodującym zwiększenia wynagrodzenia Wykonawcy określonego w niniejszej umowie.
8. Termin powiadomienia o konieczności wprowadzenia zmian w zawartej Umowie nie może nastąpić później niż 3 dni kalendarzowe od zaistnienia okoliczności uzasadniających zmiany w Umowie.
9. Nie stanowi zmiany Umowy: zmiana danych teleadresowych, zmiany osób reprezentujących oraz wskazanych do kontaktu między Stronami.

## 13. INFORMACJA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH

1. Odbiorcą Pani/Pana danych osobowych będą upoważnieni pracownicy Zamawiającego (Politechniki Białostockiej) oraz Ministerstwo Funduszy i Polityki Regionalnej (MFiPR), ul. Wspólna 2/4 00-926 Warszawa jako właściciel Bazy Konkurencyjności, na której Zamawiający (Politechnika Białostocka) prowadzi postępowania o udzielenie zamówienia publicznego, działającą pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov
2. Klauzula informacyjna z art. 13 RODO stanowi Załącznik nr 2 do Zapytania ofertowego.
3. Strony zobowiązują się do zawarcia Umowy powierzenia przetwarzania danych osobowych (Załącznik nr 7)

## 14. LISTA ZAŁĄCZNIKÓW:

1) Formularz ofertowy – *Załącznik nr 1;*
2) Wzór oświadczenia o niepodleganiu wykluczeniu – Załącznik nr 2;
3) Klauzula informacyjna RODO - *Załącznik nr 3;*
4) Oświadczenie wykonawcy dotyczące przesłanek wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego - *Załącznik nr 4,*
5) Wzór umowy - *Załącznik nr 5*
6) Oświadczenie wykonawcy o braku powiązań osobowych lub kapitałowych - *Załącznik nr 6*
7) Wzór umowy powierzenia przetwarzania danych osobowych – *Załącznik nr 7*

Prodziekan
ds. Rozwoju i Współpracy
Wydziału Informatyki
Politechniki Białostockiej
dr hab. inż.
Ireneusz Mrozek, prof. PB

.....

*Data i podpis Wnioskodawcy / przedstawiciela wnioskodawcy dokonującego opisu przedmiotu zamówienia*

Prorektor ds. Rozwoju

13 LIS. 2026

dr hab. inż.
Mirosław Świercz, prof. PB

.....

*Data i podpis kierownika jednostki (lub jego zastępcy) przeprowadzającej procedurę zapytania ofertowego*

p.o. Kierownika
Biura ds. Rozwoju i Programów
Międzynarodowych
mgr Tomasz Charkiewicz

13 LIS. 2026

Kierownik
Działu Aparatury i Zakupów
inż. Mariusz Seroka