UNIWERSYTET SZCZECIŃSKI
al. Papieża Jana Pawła II nr 22a
70-453 Szczecin

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
TP/371/142/20

postępowania prowadzonego w trybie przetargu nieograniczonego pn.:

zakup, dostawa, instalacja i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum" w trzech istniejących centrach danych w ramach projektu „Zintegrowane wirtualne Herbarium Pomorza Herbarium Pomeranicum – digitalizacja i udostępnienie zbiorów herbariów jednostek akademickich Pomorza poprzez ich połączenie i udostępnienie cyfrowe" współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020"

CPV	**48800000-6 Systemy i serwery informacyjne;** **48820000-2 Serwery** **48821000-9 Serwery sieciowe** **48822000-6 Serwery komputerowe**

Rozdział 1: Instrukcja dla Wykonawców wraz załącznikami
Rozdział 2: Opis przedmiotu zamówienia
Rozdział 3: Projekt umowy

Informacje ogólne

1. Wykonawca winien zapoznać się z całością niniejszej dokumentacji.

1.1. Wszystkie formularze zawarte w niniejszej dokumentacji, a w szczególności formularz oferty, załączniki do *Rozdziału 1* zostaną wypełnione przez Wykonawcę ściśle według wskazówek. W przypadku, gdy jakakolwiek część dokumentów nie dotyczy Wykonawcy - wpisuje on *„nie dotyczy"*.

2. Niniejszą dokumentację można wykorzystać wyłącznie zgodnie z przeznaczeniem, nie należy udostępniać jej osobom trzecim.
3. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
4. Nie dopuszcza się składania ofert częściowych.
5. Nie dopuszcza się składania ofert wariantowych.
6. Dopuszcza się składanie ofert równoważnych.
7. Aukcja elektroniczna przy wyborze najkorzystniejszej oferty nie będzie stosowana.
8. Umowa ramowa – nie dotyczy.
9. Zamawiający przewiduje możliwość wykluczenia wykonawcy na podstawie art. 24 ust. 5 pkt 1, 2 i 4 PZP.
10. Platforma zakupowa: https://platformazakupowa.pl/pn/usz

ROZDZIAŁ 1
INSTRUKCJA DLA WYKONAWCÓW
UNIWERSYTET SZCZECIŃSKI
al. Papieża Jana Pawła II 22a 70-453 SZCZECIN

Reprezentowany przez **Rektora US prof. dra hab. Waldemara Tarczyńskiego** działając w oparciu o *Ustawę z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych* (Dz. U. z 2019 r., poz. 1843) – dalej PZP, lub ustawa PZP, jako Zamawiający Upoważniony na podstawie Porozumienia zawartego na podstawie art. 16 ust. 1 ustawy PZP do przeprowadzenia wspólnego postępowania przetargowego i udzielenia zamówienia pomiędzy:

1) **Uniwersytetem Szczecińskim**, z siedzibą w Szczecinie przy al. Papieża Jana Pawła II nr 22a, 70 - 453 Szczecin, NIP 851-020-80-05, REGON 001208777, (zamawiający wiodący);
2) **Akademią Pomorską w Słupsku** z siedzibą w Słupsk 76-200, przy ul. Krzysztofa Arciszewskiego 22a, NIP: 8391028460, REGON: 000001459;
3) **Uniwersytetem Gdańskim**, z siedzibą w Gdańsku przy ul. Bażyńskiego 8, 80-309 Gdańsk, NIP 584-020-32-39, REGON 000001330,

zaprasza do złożenia ofert w przetargu nieograniczonym pn.:

zakup, dostawa, instalacja i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum" w trzech istniejących centrach danych w ramach projektu „Zintegrowane wirtualne Herbarium Pomorza Herbarium Pomeranicum – digitalizacja i udostępnienie zbiorów herbariów jednostek akademickich Pomorza poprzez ich połączenie i udostępnienie cyfrowe" współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020"

Zakres zadań Wykonawcy opisany został w **Rozdziale 2** niniejszej *Specyfikacji istotnych warunków zamówienia.*

I. Opis sposobu przygotowania ofert

1. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty, w tym koszty poniesione z tytułu nabycia kwalifikowanego podpisu elektronicznego.
2. Wykonawca zobowiązany jest do zdobycia wszelkich informacji, które mogą być konieczne do przygotowania oferty oraz podpisania umowy.
3. Wykonawca składa ofertę wraz z załącznikami za pośrednictwem platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz
4. Korzystanie z platformy zakupowej przez Wykonawcę jest bezpłatne.
5. Celem prawidłowego złożenia oferty Zamawiający zamieścił na stronie platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz plik pn. Instrukcja składania oferty dla Wykonawcy.
6. Oferta powinna być sporządzona w języku polskim, z zachowaniem formy elektronicznej pod rygorem nieważności i podpisana kwalifikowanym podpisem elektronicznym.
7. Dokumenty lub oświadczenia, o których mowa w niniejszej SIWZ, składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem, z zastrzeżeniem zdania 2. Ofertę, w tym Jednolity Europejski Dokument Zamówienia (ESPD), sporządza się, pod rygorem nieważności, w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym.
8. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o

udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.

9. Poświadczenie za zgodność z oryginałem elektronicznej kopii dokumentu lub oświadczenia, o której mowa w pkt. 8) powyżej następuje przy użyciu kwalifikowanego podpisu elektronicznego.
10. W przypadku załączania do oferty dokumentów lub oświadczeń sporządzonych w języku obcym należy je złożyć wraz z tłumaczeniem na język polski.
11. Zamawiający zaleca wykorzystanie formularzy załączonych do SIWZ. Dopuszcza się złożenie w ofercie załączników opracowanych przez Wykonawców pod warunkiem, że będą one zgodne co do treści z formularzami określonymi przez Zamawiającego.
12. W zakresie nieuregulowanym niniejszym SIWZ, zastosowanie mają przepisy rozporządzenia Prezesa Rady Ministrów z dnia 27 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.
13. Każdy Wykonawca przedłoży tylko jedną ofertę na daną część, sam lub jako reprezentant spółki czy konsorcjum. Złożenie więcej niż jednej oferty przez jednego Wykonawcę spowoduje odrzucenie wszystkich jego ofert złożonych w ramach danej części.
14. Oferty będą oceniane według kryteriów określonych w pkt. VI Specyfikacji Istotnych Warunków Zamówienia, według zasad określonych w pkt. VII SIWZ. Wykonawcy przedstawią oferty zgodnie z wymaganiami SIWZ.
15. Ilekroć w treści SIWZ, w tym w opisie przedmiotu zamówienia, użyte są znaki towarowe, patenty lub pochodzenie, europejskie oceny techniczne, aprobaty, certyfikaty, normy i inne wymienione w ustawie PZP, Zamawiający dopuszcza rozwiązanie równoważne i zastrzega sobie prawo do weryfikacji oferowanych rozwiązań równoważnych na etapie badania i oceny ofert. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać (zgodnie z treścią art. 30a i 30b PZP), że oferowane przez niego dostawy/usługi spełniają wymagania określone przez Zamawiającego, w szczególności poprzez przedłożenie wraz z ofertą szczegółowego opisu oferowanego asortymentu zawierającego oznaczenie producenta/producentów, nazw handlowych oraz numerów katalogowych. Ze złożonego wraz z ofertą w/w dokumentu musi wynikać, iż wymagania Zamawiającego odnośnie oferowanego przedmiotu zamówienia są spełnione co najmniej w stopniu opisanym w SIWZ (parametry i funkcjonalności).
16. Formularz oferty oraz wszystkie załączniki zostaną podpisane przez upełnomocnionego przedstawiciela Wykonawcy. Pełnomocnictwo do podpisania oferty winno być dołączone do oferty, o ile nie wynika ono z ustawy albo z innych dokumentów załączonych do oferty, lub dokumentów, o których mowa w art. 26 ust. 6 PZP. Dokument pełnomocnictwa winien zostać złożony w postaci elektronicznej, opatrzony kwalifikowanym podpisem elektronicznym lub elektronicznej kopii, poświadczonej kwalifikowanym podpisem elektronicznym przez notariusza.
17. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz w terminie najpóźniej do dnia **10.12.2020 r. do godziny 11:30.**
18. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego składają jeden lub kilka dokumentów tak, aby wspólnie udokumentować spełnianie warunków podmiotowych, brak podstaw do wykluczenia oraz dotyczących przedmiotu zamówienia. Wymagane oświadczenia należy złożyć w sposób wyraźnie wskazujący, iż oświadczenie składają wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego. Nadto, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Stosowne pełnomocnictwo musi opatrzone kwalifikowanym podpisem elektronicznym.
19. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 PZP oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca, nie później niż w terminie składania ofert zastrzegł,

że nie mogą one być udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wszelkie informacje stanowiące tajemnice przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać załączone na platformie zakupowej zgodnie z instrukcją składania oferty dla Wykonawcy.

- Protokół wraz załącznikami jest jawny. Załączniki do protokołu udostępnia się po dokonaniu wyboru najkorzystniejszej oferty lub unieważnieniu postępowania, z tym, że oferty są jawne od chwili ich otwarcia.
- Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4.
- Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r., poz. 1010) rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującymi się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzenia nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich poufności, tzn. składając ofertę zastrzegł, iż nie mogą być one udostępnione innym uczestnikom postępowania oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

20. Ujawnienie niezastrzeżonej treści ofert dokonywane będzie wg poniższych zasad:
    - osoba zainteresowana zobowiązana jest wystąpić do Zamawiającego o udostępnienie treści protokołu lub/i załączników do protokołu,
    - Zamawiający ustali, z uwzględnieniem złożonego w ofercie zastrzeżenia o tajemnicy przedsiębiorstwa, zakres informacji, które mogą być udostępnione,
    - po przeprowadzeniu powyższych czynności Zamawiający niezwłocznie udostępni wnioskodawcy protokół lub/i załączniki do protokołu.

II. Odrzucanie ofert

1. Oferta zostanie odrzucona, jeżeli:
    - będzie niezgodna z ustawą,
    - jej treść nie będzie odpowiadała treści *SIWZ, **z zastrzeżeniem art. 87 ust. 2 pkt. 3 PZP**,*
    - Wykonawca w terminie 3 dni od daty otrzymania zawiadomienia nie zgodził się na poprawienie omyłek, o których mowa w *art. 87 ust. 2 pkt 3 PZP*,
    - jej złożenie będzie stanowiło czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji,
    - będzie zawierała rażąco niską cenę w stosunku do przedmiotu zamówienia,
    - zostanie złożona przez Wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia publicznego,
    - będzie zawierała błędy w obliczeniu ceny
    - będzie nieważna na podstawie odrębnych przepisów.
2. Oferty odrzucone nie będą poddane ocenie.

III. Dokumenty wymagane w ofercie

Dokumenty wymagane w celu wykazania spełniania warunków oraz braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego:

1. **Dokumenty wymagane na etapie składania ofert:**
   1) Do oferty Wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert oświadczenie, że nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Przedmiotowe oświadczenie Wykonawca składa w formie **Jednolitego Europejskiego Dokumentu Zamówienia (ESPD)**, stanowiącego Załącznik nr 2 do Rozporządzenia Wykonawczego Komisji (EU) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającego standardowy formularz jednolitego europejskiego dokumentu zamówienia. Informacje zawarte w ESPD stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Zamawiający informuje, iż instrukcję wypełnienia ESPD oraz edytowalną wersję formularza ESPD można znaleźć pod adresem: https://www.uzp.gov.pl/baza-wiedzy/jednolity-europejski-dokument-zamowienia. Zamawiający zaleca wypełnienie ESPD za pomocą serwisu dostępnego pod adresem: https://espd.uzp.gov.pl/ . W tym celu przygotowany przez Zamawiającego Jednolity Europejski Dokument Zamówienia (ESPD) w formacie *.xml, stanowiący **Załącznik nr 2 do SIWZ**, należy zaimportować do wyżej wymienionego serwisu oraz postępując zgodnie z zamieszczoną tam instrukcją wypełnić wzór elektronicznego formularza ESPD, z zastrzeżeniem poniższych uwag:
      a) w Części II Sekcji D ESPD (*Informacje dotyczące podwykonawców, na których zdolności Wykonawca nie polega*) Wykonawca oświadcza czy zamierza zlecić osobom trzecim podwykonawstwo jakiejkolwiek części zamówienia (w przypadku twierdzącej odpowiedzi podaje ponadto, o ile jest to wiadome, wykaz proponowanych podwykonawców), natomiast Wykonawca nie jest zobowiązany do przedstawienia w odniesieniu do tych podwykonawców odrębnych ESPD, zawierających informacje wymagane w Części II Sekcja A i B oraz w Części III;
      b) w Części IV Zamawiający żąda jedynie ogólnego oświadczenia dotyczącego wszystkich kryteriów kwalifikacji (sekcja α), bez wypełniania poszczególnych Sekcji A, B, C i D;
      c) Część V (*Ograniczenie liczby kwalifikujących się kandydatów*) należy pozostawić niewypełnioną.

Jednolity dokument (JEDZ), **sporządza się, pod rygorem nieważności, w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.** Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia składa także jednolite dokumenty dotyczące tych podmiotów na formularzu JEDZ, który musi mieć formę dokumentu elektronicznego, podpisanego kwalifikowanym podpisem elektronicznym przez każdego z nich w zakresie w jakim każdy z Wykonawców wykazuje brak podstaw wykluczenia. Analogiczny wymóg dotyczy JEDZ składanego w przypadku wspólnego ubiegania się o zamówienie przez wykonawców. Dokumenty te potwierdzają brak podstaw wykluczenia. ***W przypadku składania oferty wspólnej ww. dokument składa każdy z Wykonawców składających ofertę wspólną.*** **Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu składa także jednolite dokumenty dotyczące tych podmiotów.**

   2) Wykonawca, który powołuje się na zasoby innych podmiotów na zasadach określonych w art. 22a PZP w celu potwierdzenia spełniania warunków udziału w postępowaniu, musi udowodnić zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. W celu oceny, czy wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a PZP, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, zamawiający żąda dokumentów, które określają w szczególności zakres dostępnych wykonawcy zasobów innego podmiotu; sposób wykorzystania zasobów innego podmiotu,

przez wykonawcę, przy wykonywaniu zamówienia publicznego; zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego.

3) Pełnomocnictwo do podpisania oferty, o ile nie wynika ono z ustawy albo z innych dokumentów załączonych do oferty, lub dokumentów, o których mowa w art. 26 ust. 6 PZP. Dokument pełnomocnictwa winien zostać złożony w postaci elektronicznej, opatrzony kwalifikowanym podpisem elektronicznym lub elektronicznej kopii, poświadczonej kwalifikowanym podpisem elektronicznym przez notariusza.
4) Formularz ofertowy (załącznik nr 1) zawierający m.in oznaczenie producenta/producentów, nazw handlowych oraz numerów katalogowych oferowanego asortymentu.

2. Dokumenty wymagane po zamieszczeniu przez zamawiającego na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy PZP:

1) Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy PZP, przekaże zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Zamawiający zaleca złożenie oświadczenia zgodnie ze wzorem wskazanym w **załączniku nr 3** do SIWZ; **W przypadku składania oferty wspólnej ww. dokument składa każdy z Wykonawców składających ofertę wspólną lub upoważniony przez mocodawcę pełnomocnik.**

3. Dokumenty wymagane przed udzieleniem zamówienia:

1) Zamawiający przed udzieleniem zamówienia wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 PZP:

a) wykazu dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich **3 lat** przed upływem terminu 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, 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 okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

Zamawiający wymaga, aby Wykonawcy składający ofertę wykazali, że w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonali co najmniej 2 zamówienia o wartości nie mniejszej niż 500 000,00 zł (słownie: pięćset tysięcy 00/100 zł) brutto każde, odpowiadające swoim rodzajem przedmiotowi zamówienia, tj. polegające na realizacji dostawy i instalacji infrastruktury serwerowej;

2) Zamawiający przed udzieleniem zamówienia wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 2 PZP:

a) Szczegółowego opisu oferowanych urządzeń potwierdzającego spełnienie wymagań opisanych w Rozdziale 2 niniejszej SIWZ;
b) Kart katalogowych – w języku polskim lub angielskim, pochodzących od producenta (producentów) oferowanych urządzeń, których autentyczność musi zostać poświadczona przez wykonawcę.

3) **Zamawiający przed udzieleniem zamówienia wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 3 PZP:**
   a) informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 PZP, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert; Wykluczenie wykonawcy następuje w przypadkach, o których mowa w art. 24 ust. 1 pkt 13 lit. a–c i pkt 14 PZP, gdy osoba, o której mowa w tych przepisach została skazana za przestępstwo wymienione w art. 24 ust. 1 pkt 13 lit. a–c, jeżeli nie upłynęło 5 lat od dnia uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia, zaś w przypadkach, o których mowa w art. 24 ust. 1 pkt 13 lit. d i pkt 14 PZP, gdy osoba, o której mowa w tych przepisach, została skazana za przestępstwo wymienione w art. 24 ust. 1 pkt 13 lit. d, PZP, lub jeżeli nie upłynęły 3 lata od dnia uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia;
   b) odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 PZP;
   c) oświadczenia wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności. Wykluczenie wykonawcy następuje w przypadku, o którym mowa w art. 24 ust. 1 pkt 15 PZP, jeżeli nie upłynęły 3 lata od dnia odpowiednio uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia lub od dnia w którym decyzja potwierdzająca zaistnienie jednej z podstaw wykluczenia stała się ostateczna;
   d) aktualnego na dzień złożenia oświadczenia wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne; Wykluczenie wykonawcy następuje, jeżeli nie upłynął okres obowiązywania zakazu ubiegania się o zamówienia publiczne.

Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w pkt 3 ppkt 1 – składa informację z odpowiedniego rejestru 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 lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 PZP. Dokumenty, o których mowa powyżej, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów o których mowa w pkt 3 ppkt 2 składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Dokumenty, o których mowa powyżej, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa powyżej, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu

na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Dokumenty, o których mowa powyżej, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

UWAGI:

- Zgodnie z treścią art. 22a ust. 3 ustawy Pzp, Zamawiający ocenia czy udostępniane wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu oraz bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 i ust. 5 ustawy Pzp. W związku z powyższym Zamawiający żąda od wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy PZP, przedstawienia w odniesieniu do tych podmiotów **dokumentów wymienionych w § 5 pkt 1–9 Rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r.** w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r., poz. 1126) – dalej r.r.d., tj.
    a. informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
    b. odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy;
    c. oświadczenia podmiotu o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności;
    d. oświadczenia podmiotu o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne;
- Zamawiający nie żąda od wykonawcy przedstawienia dokumentów wymienionych w § 5 pkt 1–9 r.r.d., dotyczących podwykonawcy, któremu zamierza powierzyć wykonanie części zamówienia, a który nie jest podmiotem, na którego zdolnościach lub sytuacji wykonawca polega na zasadach określonych w art. 22a ustawy PZP.
- Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 ustawy Pzp, jeżeli zamawiający posiada oświadczenia lub dokumenty dotyczące tego wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r., poz. 346).
- Oświadczenia, o których mowa w Dziale III pkt 1 (Dokumenty wymagane na etapie składania ofert), dotyczące wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a ustawy Pzp oraz dotyczące podwykonawców, składane są w oryginale. Dokumenty i oświadczenia, o których mowa w Dziale III pkt 2 oraz 3, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.

IV. Wykluczenie z postępowania

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

1) w art. 24 ust. 1 pkt 12-23 ustawy PZP;

2) w art. 24 ust. 5 pkt 1,2,4 ustawy PZP, tj.:

a) w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2019 r. poz. 243 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2019 r. poz. 498 ze zm.);

b) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;

c) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 PZP, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania.

2. Wykluczenie Wykonawcy następuje zgodnie z art. 24 ust. 7 ustawy PZP.

3. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13-14 oraz 16-20 lub ust. 5 pkt. 1 ustawy PZP, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Regulacji, o której mowa w zdaniu pierwszym nie stosuje się, jeżeli wobec wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.

4. Wykonawca nie podlega wykluczeniu, jeżeli zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające przedstawione przez Wykonawcę dowody, o których mowa w ust. 3.

5. Zamawiający może wykluczyć wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

V. Termin realizacji zamówienia

Wymagany maksymalny termin realizacji niniejszego zamówienia: do 90 dni kalendarzowych od podpisania umowy.

VI. Kryteria oceny ofert

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami i ich wagami oraz w następujący sposób będzie oceniać spełnianie kryteriów:

1) Cena brutto	**- 60 %**
2) Termin realizacji	**- 40 %**

VII. Sposób oceny ofert według przyjętych kryteriów (1% = 1 pkt)

Kryterium 1 będzie obliczone za pomocą następującego wzoru:

C = [(Cn : Cb) x 60 %] x 100
gdzie:
Cn - cena najniższa (brutto)
Cb - cena badana (brutto)
Maksymalną ilość punktów w obrębie kryterium otrzyma oferta z najniższą ceną.

Kryterium 2 obliczone zostanie za pomocą następującego wzoru:
Termin realizacji = [(Tn : Tb) x 40 %] x 100

gdzie:
Tn - najkrótszy termin dostawy
Tb -termin dostawy w ofercie badanej

Maksymalna liczba 40 punktów, zostanie przyznana za zaoferowanie najkrótszego terminu dostawy. W przypadku zaoferowania terminu wykonania krótszego niż 40 dni kalendarzowych, do oceny kryterium będzie brany termin 40-dniowy. Maksymalny termin dostawy — 90 dni kalendarzowych. Zaoferowanie dłuższego terminu dostawy, lub brak informacji w zakresie terminu dostawy w ofercie spowoduje odrzucenie oferty. Termin musi być podany w dniach kalendarzowych oraz musi dotyczyć całego ZADANIA.

Wynik zostanie zaokrąglony do dwóch miejsc po przecinku.

a. W wyniku komisyjnej analizy i oceny otrzymanych ofert, stosując kryteria ustawowe i określone w *SIWZ* dokonany zostanie wybór najkorzystniejszej oferty.
b. W toku dokonywania oceny złożonych ofert, Zamawiający zgodnie z art. 87 ust. 1 ustawy, może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
c. Zgodnie z art. 87 ust. 2 ustawy, Zamawiający poprawi w treści oferty oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek oraz inne omyłki polegające na niezgodności treści oferty z SIWZ, niepowodujące istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

VIII. Opis sposobu obliczenia ceny oferty

1. Wykonawcy podadzą ceny jednostkowe netto dla każdej pozycji zadania na formularzu oferty, oraz wartość netto oraz brutto zadania na formularzu oferty, zgodnie z tabelami w formularzu oferty.
2. Wszystkie ceny określone przez Wykonawcę są wiążące i zostaną wprowadzone do umowy.
3. Wszystkie elementy oferty powinny zawierać w sobie ewentualne upusty stosowane przez Wykonawcę, tzn. muszą być one wkalkulowane w cenę oferty.
4. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
5. Wszystkie ceny należy podać z zaokrągleniem do dwóch miejsc po przecinku.

UWAGA:

Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w walucie PLN.

IX. Wymagania dotyczące wadium

1. Zamawiający nie wymaga wniesienia wadium.

X. Termin związania ofertą

Okres związania Wykonawców złożoną ofertą wynosi **60 dni** licząc od upływu terminu składania ofert.

XI. Składanie i otwarcie ofert

1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: **https://platformazakupowa.pl/pn/usz** w terminie najpóźniej do dnia **10.12.2020 r. do godz. 11:30.**
2. Otwarcie ofert nastąpi w dniu **10.12.2020 r.** w budynku administracji US, al. Papieża Jana Pawła II nr 31, 70-453 Szczecin (Dział Zamówień Publicznych, pok. 204) o godzinie **12:00** za pomocą platformy zakupowej.
3. Niezwłocznie po otwarciu ofert zamawiający zamieści na stronie http://zp.univ.szczecin.pl lub za pośrednictwem platformy zakupowej pod adresem: **https://platformazakupowa.pl/pn/usz** informacje dotyczące:
   1) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia,
   2) firm oraz adresów wykonawców, którzy złożyli oferty w terminie,
   3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

XII. Informacje o trybie otwarcia i oceny ofert

Oceny ofert dokona Komisja Przetargowa.
1. Podczas otwarcia ofert Przewodniczący Komisji ogłosi:
   - imię i nazwisko, nazwę (firmę) oraz adres (siedzibę) Wykonawców,
   - ceny ofert,
   - termin wykonania zamówienia,
   - warunki płatności zawarte w ofercie.
2. Otwarcie ofert jest jawne.
3. Bezpośrednio przed otwarciem ofert Zamawiający podaje kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Niezwłocznie po otwarciu ofert zamawiający zamieszcza na stronie internetowej https://zp.univ.szczecin.pl informacje dotyczące kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia; firm oraz adresów wykonawców, którzy złożyli oferty w terminie oraz ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.
5. Zamawiający przed udzieleniem zamówienia, **wezwie** wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż **10 dni**, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 PZP.
6. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, zamawiający może na każdym etapie postępowania wezwać wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu lub kryteria selekcji, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.

7. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 PZP, jeżeli zamawiający posiada oświadczenia lub dokumenty dotyczące tego wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346).
8. W toku badania i oceny złożonych ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert jak również dokumentów potwierdzających prawdziwość danych zawartych w ofercie.
9. Zamawiający dokona badania ofert. Jeżeli okaże się, że nie złożono żadnej oferty niepodlegającej odrzuceniu, postępowanie zostanie unieważnione.
10. W toku dokonywania oceny złożonych ofert Zamawiający, zgodnie z art. 87 ust. 1 ustawy, może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
11. Zamawiający przyzna zamówienie Wykonawcy, którego oferta odpowiada zasadom określonym w ustawie i niniejszej specyfikacji oraz została uznana za najkorzystniejszą.
12. Wybrany Wykonawca zostanie powiadomiony o decyzji Zamawiającego oraz określony będzie termin zawarcia umowy.
13. O wyborze oferty najkorzystniejszej zostaną powiadomieni pisemnie, drogą elektroniczną, wszyscy Wykonawcy, którzy złożyli oferty w niniejszym postępowaniu.

Wyniki przetargu zostaną niezwłocznie wywieszone w siedzibie Zamawiającego oraz zamieszczone na jego stronie internetowej.

XIII. Sposób udzielania wyjaśnień dotyczących dokumentacji

1. Komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu platformy zakupowej (**https://platformazakupowa.pl/pn/usz**)
2. Osobą uprawnioną do porozumiewania się z wykonawcami jest: Wojciech Bereszko, adres e-mail: przetargi@usz.edu.pl
3. W sytuacjach awaryjnych np. w przypadku braku działania platformy zakupowej **https://platformazakupowa.pl/pn/usz** Zamawiający może również komunikować się z wykonawcami za pomocą poczty elektronicznej
4. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń, o których mowa w niniejszej SIWZ, składane są przez Wykonawcę za pośrednictwem **https://platformazakupowa.pl/pn/usz**
5. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.
6. Wykonawcy mogą zwracać się do Zamawiającego o wyjaśnienie treści SIWZ, zgodnie z art. 38 ust. 1 PZP, kierując swoje zapytania do Zamawiającego, ze wskazaniem numeru postępowania określonego w SIWZ. Zapytania winny być składane w sposób określony w pkt. 1.
7. Każdy Wykonawca ma prawo zwrócić się do Zamawiającego o udzielenie wyjaśnień *Specyfikacji Istotnych Warunków Zamówienia*. Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści *SIWZ* wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści *SIWZ* wpłynął po upływie terminu składania wniosku lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. **Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku.**

8. Treść wyjaśnień zostanie udzielona przez Zamawiającego zgodnie z art. 38 ust. 2 PZP.
9. Wszelkie wyjaśnienia i modyfikacje, w tym zmiany terminów stają się integralną częścią specyfikacji istotnych warunków zamówienia i są wiążące dla Zamawiającego i Wykonawców.

XIV. Środki odwoławcze

W prowadzonym postępowaniu przysługują środki ochrony prawnej przewidziane w art. 179-198 ustawy PZP.

XV. Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XIV. Ustalenia końcowe

1. Z tytułu odrzucenia oferty Wykonawcom nie przysługuje roszczenie przeciwko Zamawiającemu.
2. Oferty po dokonaniu wyboru nie będą zwracane Wykonawcom.
3. Zamawiający informuje, iż zmiana istotnych postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy jest zakazana, za wyjątkiem sytuacji, wskazanych we wzorze umowy. Zmiana musi nastąpić w formie obustronnie podpisanego aneksu.
4. W sprawach nie ujętych w niniejszej specyfikacji będzie stosowana *Ustawa z 29 stycznia 2004 r. - Prawo Zamówień Publicznych.*
5. Zamawiający nie przewiduje możliwości udzielenia zamówień uzupełniających.
6. Jeżeli umowę ma podpisać osoba lub osoby reprezentujące Wykonawcę, inne niż osoby podpisujące ofertę, Wykonawca najpóźniej w dniu wyznaczonym na zawarcie z nim umowy, przed jej podpisaniem przekaże Zamawiającemu pełnomocnictwo upoważniające wskazane osoby do zawarcia umowy. Przedłożenie pełnomocnictwa nie jest wymagane, jeżeli upoważnienie do zawarcia (podpisania) umowy przez wskazane osoby wynika z dokumentów załączonych do oferty.

ROZDZIAŁ 2
OPIS PRZEDMIOTU ZAMÓWIENIA

zakup, dostawa, instalacja i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum" w trzech istniejących centrach danych

Opis przedmiotu zamówienia stanowiący podstawę wyceny:

Zastosowanie:
Zamówienie obejmuje: zakup, dostawę, instalację i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum", w trzech istniejących centra danych:

1. **Podstawowe Centrum Przetwarzania (PCP)** umieszczone w Akademii Pomorskiej w Słupsku, który będzie miało za zadanie gromadzenie wszystkich danych oraz obsługę edycji danych jak i ich przeglądanie przez interesariuszy,
2. **Awaryjne Centrum Przetwarzania (ACP)** centrum danych umieszczone na Uniwersytecie Gdańskim, które w razie wystąpienia awarii przejmie na siebie wszystkie funkcje głównego centrum,
3. **Zapasowe Centrum Przetwarzania (ZCP)** centrum danych na Uniwersytecie Szczecińskim przechowujące wersjonowane w określonym zakresie czasowym dane kopii bezpieczeństwa.

Każde Centrum Przetwarzania zostanie wyposażone w autonomiczny zestaw urządzeń i oprogramowania zapewniający możliwość wprowadzanie zeskanowanych danych.

W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia sprzętu oraz oprogramowania, którego parametry minimalne wskazane zostały w niniejszym dokumencie. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne oraz:

- wszystkie oferowane urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta bezpośrednio na odpowiednio: Zamawiającego, Akademię Pomorską w Słupsku lub Uniwersytet Gdański jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.
- w momencie oferowania wszystkie elementy oferowanego systemu muszą być dostępne (dostarczane przez producenta) w dacie złożenia oferty i nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
- urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
- do każdego urządzenia i oprogramowania musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku angielskim lub polskim.
- sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
- wszystkie urządzenia posiadają oznakowanie CE produktu albo spełniają normy równoważne.
- wszystkie urządzenia, jeśli nie podano inaczej, muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
- korzystanie przez Zamawiającego z dostarczonego produktu nie narusza majątkowych praw autorskich osób trzecich

Zamawiający zastrzega sobie:

- prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.
- żądanie dostarczenia przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych.

Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu oraz oprogramowania.

1. **Sprzęt**
   Zamawiający wymaga, aby wszystkie dostarczone urządzenia został uruchomione i umieszczone (zamontowane) w miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu powinien być dostosowany do technologii wykonania oraz ma być przeprowadzony zgonie z zaleceniami producenta dostarczonych rozwiązań.
2. **Oprogramowanie**
   Dostarczone systemy operacyjne, oprogramowanie aplikacyjne oraz wszystkie niezbędne oprogramowanie dodatkowe mają być kompletnie zainstalowane oraz aktywowane o ile jest to wymagane.

Przez sformułowania: „ma umożliwić, ma zapewnić" Zamawiający rozumie możliwość pełnego, zgodnego z opisem wymagań, wykorzystania danej funkcjonalności, bez konieczności zakupu dodatkowych licencji lub ponoszenia dodatkowych opłat.

Mając na uwadze nadrzędność celu jakim jest skuteczne uruchomienie planowanych rozwiązań Zamawiający zastrzega, że zadaniem Wykonawcy jest dostarczenie wszelkich niezbędnych elementów sprzętowych, oprogramowania, licencji oraz wykonanie wszystkich niezbędnych prac instalacyjnych, konfiguracyjnych i wdrożeniowych, które konieczne są do osiągnięcia zakładanego celu, nawet jeśli nie zostały one wymienione w dalszej części niniejszego dokumentu.

1.1 Elementy dostawy

W ramach zadania zaplanowano instalację następującego sprzętu teleinformatycznego w każdej serwerowni (szczegółowe wymagania dla wskazanych niżej elementów znajdują się w tabelach w dalszej części dokumentacji):

1. **Szafa Rack 19"** wraz z niezbędnymi akcesoriami zgodnymi ze specyfikacją szczegółową:
   a. Zasilacz awaryjny z modułami bateryjnymi umożliwiający utrzymanie zasilania urządzeń elektronicznych zainstalowanych w szafie w przypadku wystąpienia przerw lub nieprawidłowych parametrów zasilania sieci energetycznej. Pojemność baterii musi umożliwić bezpieczne wyłączenie pracujących urządzeń w ciągu 20 minut przy obciążeniu równym 40% nominalnej mocy podłączeniowej dostarczonych urządzeń.
   b. Redundantne listwy dystrybucji zasilania, zarządzane, z monitorowaniem parametrów środowiskowych wewnątrz szafy (temperatura, pobór prądu).
2. **Warstwę dedykowanych Serwerów Pamięci Masowej** z funkcjami wybiórczego szyfrowania, deduplikacji, kompresji, detekcji i usuwaniu zer oraz tzw. cienkich woluminów realizowanych w locie dla całej dostarczonej przestrzeni użytkowej netto (przestrzeń po uwzględnieniu oferowanego mechanizmu zabezpieczenia RAID oraz przestrzeni hotspare), liczonej bez uwzględnienia mechanizmów redukcji ilości przechowywanych danych w wymiarze **260TB** i wsparciem dla replikacji pomiędzy ośrodkami badawczymi w trybie synchronicznym i asynchronicznym opisanym powyżej.
3. Redundantną **Warstwę Sieciową Data Center** umożliwiającą podłączenie do 24 portów dostarczonych urządzeń o wydajności nie mniejszej niż 10GbE, w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej szafie stelażowej 19".
4. Redundantną **Warstwę Sprzętowych Serwerów Wirtualizacji x86_64**, na potrzeby platformy „Herbarium Pomeranicum", w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej szafie stelażowej 19".

5. **Warstwę Sprzętowych Firewall/UTM** umożliwiający podłączenie do infrastruktury sieciowej w danej lokalizacji, zapewniający minimalną przepustowość komunikacji szyfrowanej VPN 2750Mb/s, w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej szafie stelażowej 19”.
6. **Urządzenia brzegowe** umożliwiające podłączenie zintegrowanej infrastruktury sieciowo-serwerowej do sieci Internet oraz połączenie wymienionych wyżej trzech centrów danych.
7. **Licencje oprogramowania wirtualizacyjnego** wymagane przez proponowane rozwiązanie w ilości wymaganej dla dostarczonych elementów infrastruktury.
8. **Certyfikowane Szkolenia** obejmujące komponenty dostarczonej platformy infrastrukturalnej oraz oprogramowania wirtualizacyjnego dla 6 osób.
9. **Dokumentację powykonawczą oraz 1-dniowe nieodpłatne warsztaty szkoleniowe** jako element zakończenia projektu i przekazania go do działu utrzymania.

Wszystkie urządzenia wymienione powyżej:

1. Powinny zostać dostarczone, w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej oraz standardowej szafie stelażowej 19”.
2. Urządzenia dostarczone wraz z kompletem niezbędnych wkładek/kabli umożliwiających połączenie serwerów z przestrzenią dyskową lub jej nośnikiem, firewall’a, listw PDU i UPS’a oraz podłączenia do istniejącej sieci LAN (pkt. 1.7 urządzenia brzegowe), kablami światłowodowymi o długości 7 metrów.
3. Być objęte wsparciem NBD (Next Business Day).
4. Wykonawca jest zobowiązany dostarczyć wszystkich innych zasobów niezbędnych do działania oferowanego rozwiązania zgodnie z dobrą praktyką w powyższej architekturze oraz po dokonaniu wizji lokalnej. Oferent jest zobowiązany do przedstawienia szczegółowego wykazu dostarczanych komponentów i ich konfiguracji, opisu architektury z uwzględnieniem realizacji wymaganych usług w celu i umożliwienia analizy rzetelności składanej oferty. Informacje te nie mogą podlegać utajnieniu w postępowaniu.

Specyfikacje i wymagania techniczne dla komponentów.

1.2 Szafa Rack 19”

Ilość: 3 sztuki - po jednej do każdej lokalizacji

Lp.	Opis wymagania / Element	Wymaganie / Wymagany parametr
1.	Wymiary szafy RACK 19”	Szafa stelażowa 19” 42U wewnętrznego miejsce do instalacji urządzeń. Wysokość szafy max 201cm. Szerokość szafy max. 60cm Głębokość szafy max. 112 cm pozwalająca na montaż urządzeń o dł. 1075mm
2.	Wyposażenie szafy RACK 19”	Szafa wyposażona w: a) Drzwi przednie perforowane (perforacja min. 80%), wyposażone w zamek b) Drzwi tylne, dzielone, wyposażone w zamek c) Obie ściany boczne zamykane na zamek. d) Każda ze ścian bocznych składająca się 2 elementów. e) Zaślepki montowane bez użycia narzędzi z przodu szafy, pozwalające na zamaskowanie miejsca o wysokości 30U; wysokość pojedynczej zaślepki równa 1U f) Element stabilizujący – podpora. g) Styk uziemiający h) 6 x wertykalnych listew PDU 3,6 kVA, każda wyposażona w: ● 20 gniazd C12 ● 2 gniazda C19.
3.	Standardy przemysłowe dla szafy RACK19”	Szafa RACK 19” zgodna ze standardami: a) EIA-310 b) WEEE c) RoHS compliant d) UL/CES Certification
4.	Awaryjne podtrzymanie zasilania	Systemy awaryjnego podtrzymania zasilania (UPS) o nominalnej mocy nie mniejszej niż 85% sumy nominalnych mocy wszystkich zasilaczy, dostarczonych w ramach zadania urządzeń. UPS musi posiadać moduł sieciowy (LAN) pozwalający na automatyczne zamknięcie wszystkich dostarczonych elementów infrastruktury w przypadku awarii zasilania. Pojemność dostarczonego UPS musi zapewniać 12 minutowe podtrzymanie zasilania przy obciążeniu 50% nominalnej mocy dostarczonego UPS. UPS musi być: a) Wyposażony w moduły zasilania formujące tzw. „pełną sinusoidę”. b) wyposażony w 6 niezależnie zarządzanych sekcji zabezpieczonych własnym zabezpieczeniem prądowym (bezpiecznik). c) zasilany z 2 niezależnymi jednofazowymi źródłami prądu 240V.
5.	Inne	Możliwość instalacji sprzętu o wadze min. 1360kg (obciążenie statyczne). Dopuszczalne obciążenie podczas przemieszczania/przesuwania szafy 1100kg (obciążenie dynamiczne) bez użycia dodatkowych środków technicznych (wózek, platforma itp.)

1.3 Warstwa Serwerów Pamięci Masowej

Ilość: 3 sztuki - po jednej w każdej lokalizacji

Lp.	Parametr	Charakterystyka parametru

Lp.	Parametr	Charakterystyka parametru
1.	Opis urządzenia	Zoptymalizowany pod kątem technologii *flash* hybrydowy serwer pamięci masowej z dostępem przez interfejsy 10GbE oraz wewnętrzną magistralą 12Gbps. Przez Serwer Pamięci Masowej Zamawiający rozumie zestaw nośników do składowania danych obsługiwanych przez dedykowane węzły (bez dodatkowych urządzeń pośrednich, serwerów wirtualizujących, oprogramowania wirtualizującego itp.). Spełnienie wymagań poniżej powinno być udokumentowane w ogólnodostępnych materiałach producenta.
2.	Wsparcie klastrów i systemów operacyjnych	Urządzenie musi być na listach wsparcia i wspierać główne systemy operacyjne i klastry, w tym: system operacyjny Windows Server 2012, Windows Server 2016, Windows Server 2019, VMware 6.7, Linux (Centos 7.x, SUSE12, Redhat 7.x) i Unix (Solaris, Aix, HP-UX). Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Preferowane jest rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2012 i nowsze, Linux RedHat 7.x+, Suse12+, VMware 5,5+. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów/pojemności obsługiwanych przez oferowane urządzenie.
3.	Partycjonowanie zasobów	Serwer pamięci masowych musi umożliwiać podział na minimum 8 odseparowanych urządzeń logicznych zarządzanych przez dedykowanych administratorów.
4.	Pojemność i skalowalność	Oferowane Urządzenie musi być wyposażone w co najmniej: a) Surową pojemność zbudowaną z $(1+W_2+W_4)*42$ nośników/dysków. b) Pojemność netto $(1+W_3+W_4)*260$TB (po odjęciu narzutu na RAID, przestrzenie/dyski *hotspare* oraz metadane). c) Dedykowaną pamięć *flash* zbudowaną z dysków SSD o pojemności użytecznej $(1+W_5)*26$TB zbudowaną z minimum 9 dysków SSD. oraz zapewniać rozbudowę: a) W trybie „scale-up” do $(1+W_2+W_4)*128$ nośników danych o łącznej przestrzeni surowej 504TB przez rozbudowę kontrolerów/dodanie dysków/półek dyskowych w trybie na gorąco. b) „scale-out” do 5PB przestrzeni surowej przez integrację do 8 kontrolerów w sposób zapewniający stworzenie pojedynczej, jednolitej puli dyskowej dla świadczonych serwisów z wykorzystaniem wbudowanego w macierz oprogramowania. Używane jednostki pojemności: a) 1TiB=1024GiB=240B, 1GiB=1024MiB=2^{40}B b) 1TB=1000GB=1012B, 1GB=1000MB=10^{12}B
5.	Bufor danych RAM	Każdy redundantny węzeł oferowanego urządzenia musi być wyposażony w minimum dwa procesory oraz 64GB pamięci RAM dedykowanej dla operacji odczytu i zapisu z zastrzeżeniem: a) Wyszczególniona pojemność musi być dedykowana na dane i informacje kontrolne. FW/OS musi posiadać własną dedykowaną pamięć operacyjną różną od wyspecyfikowanej powyżej. b) Pamięć zapisów musi być zabezpieczona dodatkową kopią zabezpieczającą przed awarią kontrolera i utratą zasilania (na drugi kontroler). c) Rozbudowa opisana w pkt 4, ppkt. d) musi pozwalać na zwiększenie RAM kontrolera do 128GB – oraz rozbudowę szybkiej przestrzeni flash do $(1+W_5)*50$TB

Lp.	Parametr	Charakterystyka parametru
6.	Efektywność obsługi nośników danych	Zamawiający dla urządzeń zapewniających: a) wielokrotną redukcję wszystkich operacji zapisu przez grupowanie i sekwencyjny zrzut zdeduplikowanych oraz skompresowanych danych z bufora na wewnętrzne nośniki danych paskiem nie mniejszym niż 8MB b) ochronę RAID, zabezpieczającą przed jednoczesną awarią co najmniej 2 dysków pozwala na stosowanie dysków o pojemności do 12TB i dowolnej długości grupy RAID. Dla pozostałych (tradycyjnych) przypadków grup należy do wyceny stosować grupę RAID6 (4+2) i dyski o pojemności nie przekraczającej 6TB. Zamawiający przez „zrzut paskiem" rozumie sposób agregacji wszystkich bieżących zapisów (losowych i sekwencyjnych) dla wszystkich wystawianych LUN'ów w ciągły strumień danych zapisywanych jako pełen pasek grupy RAID (to jest wymagające jednokrotnego naliczenia i zapisu danych nadmiarowych), zapisywany sekwencyjnie na dyskach twardych bez konieczności odczytu istniejących danych. Architektura zapisu musi (w odróżnieniu od tradycyjnych architektur RAID5/6+, które dla realizacji pojedynczego zapisu losowego wymagają wykonania wielu operacji odczytu i zapisu), redukować kilkudziesięciokrotnie ilość fizycznych operacji na nośnikach. Efektywne wykorzystanie nośników typu HDD pozwala zredukować ilość nośników tradycyjnie wymaganych dla RAID6 w celu uzyskania wymaganej wydajności.
7.	Bufor Flash	Oferowane urządzenie musi zapewniać możliwość rozbudowy buforu flash do pojemności $(1+W_5)*50$ TB netto przez dodanie nośników SSD w trybie pracy zlecanym przez producenta (flash cache, SSD tier) a) Współczynnik $W_5=0$ należy stosować dla urządzeń przechowywujących w buforze flash zdeduplikowane i skompresowane dane. W pozostałych przypadkach $W_5=3$ Termin deduplikacja i kompresja odnosi się do urządzeń zapewniających deduplikację z granulacją 4kB oraz kompresję algorytmem lze realizowane w trybie w locie (inline), to jest przed zapisem na dyski/nośniki danych. Zamawiający dopuszcza, aby urządzenie, w celu zapewnienia wymaganej wydajności, dynamicznie redukowało algorytm kompresji na nie gorszy niż lz4 dla obciążenia kontrolera powyżej 70% pod warunkiem, że kompresja zawsze odbywa się w locie (inline).
8.	Brak pojedynczego punktu awarii	Oferowane urządzenie musi być wolne od Pojedynczych Punktów Awarii, czyli wszystkie komponenty węzły, kontrolery, bufor flash, wentylatory, zasilacze itp. muszą być nadmiarowe. Awaria pojedynczego komponentu w tym węzła nie może powodować spadku wydajności urządzenia poniżej wyspecyfikowanych w Zapytaniu parametrów wydajnościowych.
9.	Wsparcie dysków i szyfrowania	Oferowane urządzenie musi wspierać dyski SSD o pojemnościach 240, 480, 960, 1920, 3840, 7680 GB na potrzeby bufora danych oraz dyski HDD 1, 2, 4, 6, 10TB dla przechowywania danych. Oferowane urządzenie musi wspierać certyfikowane szyfrowanie zgodne z AES-256 XTS FIPS z granulacją i dedykowanym kluczem dla każdego prezentowanego LUN.

Lp.	Parametr	Charakterystyka parametru
10.	Woluminy: wspierana ilość i zabezpieczenie RAID	Oferowane Urządzenie (W_4=0) musi: a) zabezpieczać przed jednoczesną utratą dowolnych 2 dysków bez utraty danych i dostępu do nich w dowolnym ośrodku przetwarzania. b) zapewnić przestrzeń *distributed hot spare* w wymiarze nie mniejszym niż 1 dysk na każde 24 dyski c) Urządzenie udostępniające jednolitą, pojedynczą pulę złożoną ze wszystkich wewnętrznych dysków HDD na potrzeby udostępniania danych. d) Oferowane urządzenie musi wspierać udostępnianie nie mniej niż 10000 woluminów (LUN) per kontroler. e) Zamawiający dopuszcza Urządzenie wymagające dedykowanych pul dla migawek zabezpieczonych RAID6. W takim przypadku należy zastosować współczynnik ekwiwalentności W_4=0,5 *Distributed hotspare* to technologia, w której przestrzeń *hotspare* jest alokowana na wszystkich dyskach grupy RAID – zapewniając wielokrotnie szybszą rozbudowę w porównaniu do tradycyjnego rozwiązania z dedykowanymi dyskami *hotspare*.
11.	Dostępność	a) Urządzenie ma charakteryzować się udokumentowaną dostępnością 99,9999%. b) Być wolne od pojedynczych punktów awarii c) Zapewnić wydajność (1+W6)*90000 IOps dla obciążenia typu losowego, blokiem 4kB przy stosunku odczytów do zapisów 50/50 (dla oferowanej konfiguracji): ● Przypadku awarii (niedostępności) jednego kontrolera ● W trakcie procesów aktualizacji oprogramowania i poprawek kontrolerów, sterowników/firmware'u. ● Przy zabezpieczeniu RAID/deduplikacji i kompresji zgodnych z deklarowanymi odpowiednio w punktach 6, 7, 10. ● Dla konfiguracji z aktywnymi migawkami na każdym udostępnianym LUN
12.	Raportowanie i zalecenia dla kierownictwa	Oferowane rozwiązanie musi zapewniać tworzenie raportów w następującym zakresie: a) Bieżące wykorzystanie przestrzeni w rozbiciu na: ● przestrzeń danych wykorzystywanych przez serwery (przed technologiami redukcji danych) ● redukcję zajętości dzięki kompresji ● redukcję zajętości dzięki deduplikacji ● redukcję zajętości z uwagi na migawki niewymagające pełnej kopi danych ● przestrzeń danych faktycznie zajęta na Urządzenie y ● współczynnik redukcji danych b) Ilość otwartych dla środowiska zgłoszeń serwisowych w rozbiciu na: ● zgłoszenia, dla których natychmiastowo zalecono rozwiązanie ● zgłoszenia wymagające interakcji z serwisem c) Raport RPO zasobów chronionych migawkami w podziale na grupy aplikacyjne d) Raport Retencji (RET) zasobów chronionych migawkami w podziale na grupy aplikacyjne e) Raport odporności na katastrofy zasobów replikowanych w podziale na grupy aplikacyjne f) Rekomendacje rozbudowy wraz ze wskazaniem przyczyn dla wszystkich posiadanych Urządzeń Raporty muszą być udostępniane w trybie online dla uprawnionych osób oraz wysyłane na listę odbiorców email.

Lp.	Parametr	Charakterystyka parametru
13.	Chmurowy Monitoring i analityka	Oferowane rozwiązanie musi zapewniać monitoring w minimalnym zakresie: a) Zdarzeń związanych z Urządzeniem (błędów, procedur utrzymania itp.) w podziale na zaproponowane przez wykonawcę priorytety (co najmniej Ważny, Pilny, Krytyczny) i obszary (Pule, Urządzenie, grupy zasobów, migawki); b) Obciążenia Urządzenia z rozbiciem na obciążenie procesorów i buforu Urządzenia c) Zajętości urządzenia: historycznej i przewidywanych trendów z okresu 3-12 miesięcy w podziale na aplikacje np. serwery wirtualne, Exchange, Oracle, MS SQL, SPS, Docker, woluminy (z migawkami) oraz pule/grupy. d) Trendów pojemności udostępnianych zasobów (woluminy, pule/grupy) w przedziale 1-365 dni z granulacją odpowiednio 10min-24h. e) Trendów wydajności udostępnianych zasobów w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h. f) Historii i bieżącego statusu otrzymanych zgłoszeń serwisowych,
1	Monitoring i zarządzanie środowiskami	Oferowane rozwiązanie musi zapewniać raportowanie analiz wydajności platformy wirtualizacji na poziomie: a) serwerów w klastrze ● wykorzystanie CPU/RAM, wykorzystania Swap, ilość przeciążonych serwerów w klastrze, ● średnia wartość oraz histogram obciążenia CPU/RAM serwerów zarządzanych przez wskazane centrum wirtualizacji w przedziałach czasowych od ostatniego dnia (granulacja: 10 minut) do 12 miesięcy wstecz (granulacja 24h) . ● Trend: Top 10 „Virtual Machine" wykorzystujących CPU/RAM w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h. b) Datastore w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h. ● listy maszyn wirtualnych (host, zaalokowana przestrzeń, śr. obciążenie vCPU, vMEM z ostatnich 24h ● trendy zajętości: lista top 10 „Virtual Machine" w przedziałach 7-365 dni z granulacją 24h. ● obciążenia IO oraz śr. czas realizacji IO ● Trend Top 10 „Virtual Machine" obciążających data store c) maszyn wirtualnych w przedziale 1-365 dni z granulacją odpowiednio 10min -24h. ● bieżące wykorzystanie zasobów: średnie: zajętość, wykorzystanie vCPU, vMEM, przepustowość MB/s oraz IO/s (w rozbiciu na zapisy i odczyty) w ciągu ostatnich 24h; histogramu wykorzystanej pojemności, czasu obsługi ze wskazaniem składowych generowanych na serwerze, sieci LAN/SAN, Urządzenie), ● histogramu czasu realizacji IO ● średniej sumarycznej przepustowości (MB/s) i ilości IOps ● średniej przepustowości dysku wirtualnego (MB/s), czasu obsługi, ilości IOps z ostatnich 24h. ● dysku wirtualnego (przepustowość MB/s oraz IO/s (w rozbiciu na zapisy i odczyty) Interfejs musi zapewniać dla danych liczbowych możliwość eksportu do pliku csv.
15.	Ochrona inwestycji	Oferowane urządzenie musi zapewniać możliwość uaktualnienia do nowej generacji kontrolerów (bez konieczności zakupu pojemności dyskowej) w nieprzerwanym trybie pracy. W przeciwnym przypadku należy zastosować współczynnik równoważności W_6=2.

Lp.	Parametr	Charakterystyka parametru
16.	Wsparcie	Urządzenie musi być certyfikowane i wspierać specyfikację VASA 3/VVOL2 w zakresie: a) sprzętowej realizacji migawki pojedynczych maszyn wirtualnych. b) natychmiastowe i automatyczne odzyskiwanie przestrzeni w przypadkach skasowania i/lub migracji maszyny wirtualnej c) automatycznej, sprzętowej realizacji funkcji „VVols array-based thin provisioning". d) sprzętowej realizacji funkcji „Thin deduplication" z granulacją na poziomie wybranych maszyn wirtualnych. e) sprzętowej realizacji funkcji QoS zarządzana przez „VM resource controls and Storage I/O Control" z granulacją na poziomie wybranych maszyn wirtualnych. f) sprzętowej realizacji funkcji „Storage based replication" Zamawiający dopuszcza Urządzenie wspierające VASA 2/VVOL 1 pod warunkiem zastosowania współczynnika W_3=1
17.	Wsparcie dla technologii kontenerów	Urządzenie musi wspierać i oferować integrację z Docker, Redhat Openshift, Kubernetes oraz MESOS. Urządzenie musi oferować ogólnodostępny sterownik CSI z możliwością definicji usług QoS oraz zintegrowany z dostarczonym systemem zarządzania kopiami zapasowymi.
18.	Porty udostępniające usługę	Urządzenie musi być wyposażone w minimum dwa redundantne węzły z minimalną łączną ilością portów: a) 4 x 10GbE-T b) 8 x 10GbE SFP+ do podłączenia Serwerów Wirtualizacji. W przypadku konieczności dedykowania portów dla realizacji zadań replikacji Zamawiający wymaga, aby doposażono dostarczone Urządzenia w ilość interfejsów zgodną z zaleceniami dobrej praktyki producenta w tym zakresie ni mniej niż 2 na każdy węzeł oferowanego rozwiązania (redundancja). Urządzenie musi pozwalać na rozbudowę do łącznie 24 portów udostępniających LUN'y (bez wymiany zainstalowanych modułów) działających z prędkością nie mniejszą niż 10Gb.
19.	Zarządzanie jakością usług	Urządzenie musi zapewniać kontrolę jakości usług (QoS) co najmniej w zakresie ograniczenia parametrów IOps i MBps z granularnością per LUN/VVol/zasób CSI.
20.	Technologia Thin oraz optymalizacja wykorzystania przestrzeni.	Urządzenie musi zapewniać możliwość granularnej (per LUN) aktywacji funkcji redukcji zajętości przestrzeni w nieprzerwanym trybie pracy (inline) na poziomie kontrolera: a) deduplikacji blokiem nie większym niż 16kB b) kompresji algorytmem nie gorszym LZ4 dla wszystkich oferowanych dysków HDD i SSD. Urządzenie musi umożliwiać równoczesne udostępnianie dowolnej kombinacji zdeduplikowanych, skompresowanych, niezdeduplikowanych i nieskompresowanych LUN.
21.	Migawki Urządzenie owe	Urządzenie musi wspierać tworzenie co najmniej 100 000 migawek per Urządzenie i 500 per LUN w technologii "redirect on write". Zamawiający dopuszcza Urządzenie używające technologii „copy on write" pod warunkiem zastosowania współczynnika równoważności W_1=0,5. Technologia migawek musi być zgodna i integrować się z oprogramowaniem np. MS SQL, VMware, Hyper-V, Oracle oraz Kontenerami (CSI) w celu tworzenia koherentnych aplikacyjnie kopii zapasowych w trybie na gorąca (online) z licencjami na pełną pojemność dostarczonego Urządzenia.

Lp.	Parametr	Charakterystyka parametru
22.	Zdalna replikacja	Urządzenie musi wspierać sprzętową replikację synchroniczną i periodyczną/asynchroniczną: a) danych z granularnością na poziomie pojedynczych LUN lub grup LUN przez sieć WAN pomiędzy ośrodkami przetwarzania b) migawek z wykorzystaniem polityk i harmonogramów Replikacji mają podlegać wyłącznie zmienione skompresowane sprzętowo bloki danych urządzeń LUN dla których zdefiniowano relacje replikacji pomiędzy Urządzeniami w 3 ośrodkach przetwarzania. Oferowane Urządzenia muszą wspierać Metro Cluster pomiędzy 2 Urządzeniami wykorzystując sieć LAN/WAN (IP4) oraz jednocześnie repikację asynchroniczną do drugiego ośrodka.
23.	Ochrona danych	. Kopie zapasowe muszą być przechowywane z zastosowaniem deduplikacji i kompresji zmiennym blokiem o wielkości 4kB+. Oprogramowanie musi być w pełni zintegrowane z konsolą do zarządzania. Kopie zapasowe maszyn wirtualnych muszą być wykonywane koherentnie/zintegrowane z hypervisorem i nie mogą wymuszać instalacji agenta lub dodatkowych zasobów dostarczonej infrastruktury produkcyjnej poza opisaną przez Zamawiającego. System ma objąć usługami ochrony danych wszystkie dane na dostarczonych serwerach pamięci masowych i pozwalać na odtworzenie danych w każdym ośrodku przetwarzania. System musi być zintegrowany (to jest nie wymaga dodatkowych narzędzi, zasobów, skryptów) i w pełni chronić replikowane pomiędzy 3 ośrodkami dane. System zarządzania kopiami zapasowymi musi zapewnić jakość opisywaną parametrami RPO=RTO=BW<=15 minut dla pełnych kopii zasobu o poj. 250 TB, oraz umożliwiać zarządzanie retencją kopii zapasowych (RET) w zakresie nie mniejszym niż 32 dni (1 miesiąc). Pod określeniem - tryb DR, należy rozumieć taką konfigurację wskazanych zasobów pamięci masowych, w której dane produkcyjne i migawki są replikowane przez dostarczone Serwery Pamięci Masowych pomiędzy ośrodkami przez przesyłanie wyłącznie zmodyfikowanych bloków. Zamawiający traktuje rozwiązania, w których migawka tworzona jest w ośrodku zapasowym względem aktywnych danych produkcyjnych jako rozwiązanie tożsame z replikacją migawek. Zamawiający wymaga, aby dostarczone licencje nie miały ograniczeń czasowych w ramach wyspecyfikowanych funkcjonalności. Oferowane Urządzenie musi umożliwiać integrację zadań wykonania i odtworzenia (w tym granularnego) kopii zapasowych z migawkami Urządzenia z co najmniej dwoma systemami backupu z ćwiartki „Leader" bieżącego raportu firmy Gartner (Data Center Backup and Recovery Solutions). Zamawiający zastrzega, że migawki muszą być integralną częścią polityki przechowywania danych. Integracja nie może wymagać tworzenia, utrzymywania i/lub modyfikacji skryptów i ma być w pełni zarządzana z jednego GUI. Oferent musi dostarczyć linki do stron internetowych producenta potwierdzających taką integrację. Jeśli funkcjonalność integracji wymaga zakupu dodatkowych komponentów (w tym licencji) muszą być dostarczone w ilości umożliwiającej objęcie taką ochroną środowiska o pojemności nie mniej niż 800TB danych użytkowych i serwerów z 36 procesorami łącznie.
24.	Licencje	Urządzenie powinno być dostarczone z licencją na wszystkie krytyczne funkcjonalności do pełnej pojemności Urządzenia, w tym co najmniej: tworzenie migawek sprzętowych zarządzanych przez aplikację, klonów, replikacji, QoS, zarządzanie i monitoring. Wymagane są licencje stałe (bez subskrypcji).
25.	Fizyczne wymiary rozwiązania	Oferowane urządzenie musi mieć możliwość instalacji w standardowej szafie stelażowej 19" o głębokości 1050 mm, i być wyposażonej w redundantne zasilanie 230V. Urządzenie nie może zajmować więcej niż 12U.

Lp.	Parametr	Charakterystyka parametru
26.	Usługi serwisowe	Gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez 24 godziny na dobę. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z Urządzeniem oraz oprogramowania wewnętrznego Urządzenia. Nośniki SSD muszą być objęte usługami wsparcia i gwarancji przy nieograniczonej intensywności wykorzystania (bez względu na intensywność zapisów).
27.	Szkolenia	Oferent dostarczy **nieodpłatne** certyfikowane szkolenia dla 6 osób z zakresu: a) podstawowego i zaawanasowanego zarządzania Urządzeniem b) integracji z platformą wirtualizacji c) integracji poszczególnych z klastrów Microsoft Hyper-V/MSCS d) replikacji i procedur DR e) integracji z dostarczonymi urządzeniami deduplikacyjnymi Oferent wykona 1 dniowe warsztaty obsługi dostarczonego rozwiązania w ramach procedury przekazania.

1.4 Warstwa Sieciowa Data Center

Ilość: - 6 sztuk - po 2 w każdej lokalizacji

Lp	Cecha	Wymagania minimalne/opis
1.	Ilość i typ portów przełącznika (obudowa/chassis)	Przełącznik montowany w standardowej szafie 42U o głębokości nieprzekraczającej 1075mm, umożliwiający w oferowanej konfiguracji: a) podłączenie serwerów co najmniej 20 portami w standardzie 10 GbE. b) podłączenie do istniejących urządzeń sieciowych Zamawiającego 1x10GbE SR LC. c) opisane w niniejszym punkcie przełączniki rdzeniowe, w części serwerowej danego ośrodka muszą być połączone ze sobą poprzez link wewnętrzny o sumarycznej przepustowości wynoszącej co najmniej 4x10Gbps. d) Porty stack/breakout oraz porty wymagane do podłączenia serwera pamięci masowej nie mogą ograniczać ilości podpiętych urządzeń wyspecyfikowanych powyżej. e) Podłączenia oferowanych serwerów pamięci masowych. Wykonawca jest zobowiązany dostarczyć okablowanie/transceivery w ilości niezbędnej do podłączenia dostarczonych serwera pamięci masowej, serwerów z istniejącą infrastrukturą Centrum Przetwarzania Danych Zamawiającego.
2.	Interfejs użytkownika	Web oraz CLI (SSH lub bezpośrednio przez port urządzenia) CLI musi wspierać zredefiniowane tryby pozwalające na dostęp do wybranych grup/poziomów komend systemowych. Urządzenie musi zapewniać ograniczenie dostępu do interfejsów zarządzających do wskazanych fizycznych interfejsów Ethernet (ang. out-of-band (OOB))
3.	SNMP	Oferującej bazę MIB pozwalającej na monitoring na poziomach: modułu, urządzenia oraz sensora.
4.	Wsparcie usług sieciowych	NTP, Clock & Time Zones PTP (IEEE-1588)
5.	Zarządzanie konfiguracją	Zapis, załadowanie oraz reset do ustawień fabrycznych konfiguracji.
6.	Logowanie zdarzeń i debugging	Logowanie musi zapewniać kategoryzację zdarzeń na kilkanaście poziomów krytyczności oraz konfigurowalny czas przechowywania informacji o zdarzeniach. Urządzenie musi zapewniać możliwość uruchomienia tzw. „debug traces” dla modułów Ethernet oraz protokołów. W szczególności musi wspierać tzw. „Link Diagnostic” per każdy wskazany port pozwalający na wgląd i konfigurację fizycznych parametrów pracy portu w tym „bit error rate (BER)”, tzw. „samplowanie” zajętości bufora i zmiany jego zajętości w czasie.
7.	Kontrola dostępu i bezpieczeństwo	Różne poziomy autoryzacji dostępu dla użytkowników i grup, wsparcie dla RADIUS, TACACS+ & LDAP. Implementacja zabezpieczeń zgodnych z FIPS 140-2 w zakresach: kryptografii (X.509, IPSec) i szyfrowania, konfiguracja generowanie i modyfikacja certyfikatów x.509 do wykorzystania przez urządzenie. Wsparcie dla protokołu 802.1x w zakresie autentykacji hostów (suplikantów) i definicji dostępnych połączeń pomiędzy nimi.

Lp	Cecha	Wymagania minimalne/opis
8.	Realizowane funkcje	a) Przełączanie Ethernet, izolacja/grupowanie interfejsów, w tym Link Aggregation Group (LAG) – z rozszerzeniem wspierającym agregację interfejsów wielu urządzeń/przełączników). b) VLANs (segmentacja na poziomie L2 z wykorzystaniem TAG) c) Wsparcie dla Rapid Spanning Tree Protocol (RSTP): BPDU Filter, BPDU Guard, Loop Guard, Root Guard, MSTP & RPVST d) VXLAN (Virtual eXtensible Local Area Network) w zakresie wirtualnych sieci (tenantów) na poziomach L2 i L3 pozwalającej na rozszerzenie domeny broadcastowej L2 przez sieć poziomu 3. e) IGMP Snooping f) Link Layer Discovery Protocol (LLDP) g) Quality of Service: QoS Classification, QoS ReWrite, Queuing and Scheduling, RED & ECN h) Access Control List (ACL) na poziomie obiektu w celu monitorowania lub filtrowania pakietów. i) Port Mirroring j) sFlow (ver. 5) k) RDMA over Converged Ethernet (RoCE) l) Priority Flow Control m) IP Routing (interfejsy: VLAN, Loopback, Router port) dla IPv4/IPv6 n) Open Shortest Path First (OSPF) o) BGP p) BFD Infrastructure q) Multicast (IGMP and PIM) r) VRRP s) DHCP Relay
9.		Wraz z przełącznikiem należy dostarczyć transceivery oraz kable do połączenia z istniejącą infrastrukturą sieciową, Serwerami Pamięci Masowych i Wirtualizacji

1.5 Warstwa Sprzętowych Serwerów Wirtualizacji x86_64

Ilość: - 6 sztuk - po 2 w każdej lokalizacji

LP	Cecha	Wymagania minimalne/opis
1.	Obudowa	Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi oraz ramieniem do zarządzania kablami.
2.	Procesor(y)	Minimum 16 rdzeni procesorowych łącznie, x86 - 64 bity, osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 116 punktów w oferowanej konfiguracji. Wynik testu musi być opublikowany na stronie http://spec.org w dniu złożenia oferty.
3.	Liczba procesorów	Zgodnie z określoną ilością rdzeni procesorowych powyżej
4.	Pamięć operacyjna	256GB RDIMM DDR4 2800 MHZ w konfiguracji DPC=1. Płyta główna z minimum 16 slotami na pamięć i umożliwiająca rozbudowę do minimum 640GB.
5.	Sloty rozszerzeń	Serwer musi być wyposażony w: a) 2 aktywne gniazda PCI-Express generacji 3 lub nowsze gotowe do obsadzenia kartami sieciowymi, każde gniazdo x16 (bus width) Serwer musi mieć dodatkowo dedykowane dwa gniazda PCI-Express: a) jeden na kontroler dyskowy; b) drugi na kartę sieciową 10/25Gb Ethernet dwuportową.
6.	Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków typu Hot Swap, SAS/SATA/SSD, 2,5” Zainstalowane 2 dyski SSD o pojemności 480GB każdy, DWPD min.2
7.	Kontroler	Serwer wyposażony w sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 2GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
8.	Interfejsy sieciowe i FC	Serwer musi być wyposażony w dwa porty 10 Gb SFP+. Oferowane karty LAN muszą znajdować się na liście kart certyfikowanych z ESXi 6.7 lub nowszym i wspierać sprzętowe SRIOV oraz ROCE2.0.
9.	Karta graficzna	Zintegrowana karta graficzna
10.	Porty	a) 2 x USB 3.0 lub nowsze b) 1x VGA Możliwość rozbudowy o: a) port szeregowy typu DB9/DE-9 (9-pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI.
11.	Zasilacze	2 szt., typu Hot-plug, nadmiarowe – o mocy zapewniającej prace serwera w przypadku awarii jednego zasilacza.
12.	Chłodzenie	Zestaw nadmiarowych wentylatorów typu „hot-plug”
13.	Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w gnieździe PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: a) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe b) dostęp do karty zarządzającej poprzez c) dedykowany port RJ45 z tyłu serwera lub d) przez współdzielony port zintegrowanej karty sieciowej

		serwera e) dostęp do karty możliwy f) z poziomu przeglądarki webowej (GUI) g) z poziomu wiersza poleceń; h) poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) i) wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i i wirtualnych folderów j) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji k) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (*capping*) l) zdalna aktualizacja oprogramowania (firmware) m) wsparcie dla Microsoft Active Directory n) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API o) możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) p) automatyczne wysyłanie zgłoszeń do serwisu Wymagane dodatkowe oprogramowanie umożliwiające centralne monitorowanie i zarządzanie serwerami w tym zarządzanie za pomocą profili serwerowych (sekwencja *bootowania* systemu, ustawienia BIOS, wersja oprogramowania układowego i sterowników (dla Windows, VMware i Red Hat);
14.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	a) Microsoft Windows Server 2016 b) Microsoft Windows Server 2019 c) Red Hat Enterprise Linux (RHEL) d) SUSE Linux Enterprise Server (SLES) 15 e) VMware ESXi 6.7 U3, 7.0
15.	Certyfikaty i standardy	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

1.6 Warstwa Sprzętowych Firewall/UTM

Ilość: - 3 sztuk - po jednym w każdej lokalizacji

ARCHITEKTURA SYSTEMU OCHRONY	
Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane przez odrębne moduły w postaci zamkniętych platform sprzętowych lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Typ systemu ochrony	Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
Wymagania systemowe	System ochrony powinien spełniać wymagania w niżej wymienionym zakresie: a) Obsługa nielimitowanej ilości hostów w sieci chronionej. b) Typ procesora: Intel lub AMD multi-core technology c) Pamięć RAM: nie mniej niż 12 GB

	d) Obudowa przeznaczona do montażu w szafie RACK. e) Minimalna liczba i typ interfejsów fizycznych: 8x 1GbE Base-T, 2x 1GbE SFP, 6x 10GbE SFP+ f) Minimalna liczba nowych połączeń na sekundę: 200 000 g) Minimalna liczba jednoczesnych połączeń: 17 500 000 h) Minimalna przepustowość Firewall: 28 000 Mbps i) Minimalna przepustowość IPS: 5 500 Mbps j) Minimalna przepustowość Web Proxy AV: 3 300 Mbps k) Minimalna przepustowość VPN: 2 750 Mbps l) Dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 150 GB.
PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	a) Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). b) Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. c) Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. d) Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. e) Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. f) System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności. g) System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów, w zakresie minimalnej ilości znaków czy złożoności hasła. h) System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. i) Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). j) System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. k) Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. l) System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. m) Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej. n) System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP. o) Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i

	v3 oraz co najmniej Netflow v5 (lub odpowiednik). p) System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. q) System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on-premise lub on-cloud. r) Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email. s) Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych np. codziennie, raz w tygodniu lub raz w miesiącu. t) Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. u) Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. v) Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). w) System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.
Zapora sieciowa, konfiguracja sieciowa oraz routing	a) Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. b) Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas. c) System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. d) Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług. e) Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. f) System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN. g) Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. h) Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading. i) System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). j) System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking). k) System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). l) Rozwiązanie powinno zapewniać obsługę routingu statycznego. m) Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). n) Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). o) System powinien oferować wsparcie dla IGMP snooping. p) Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do

	nadrzędnego serwera proxy (upstream/parrent proxy). q) Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. r) Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). s) System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. t) System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. u) Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. v) Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów. w) Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules. x) Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta. y) Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). z) System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP. aa) System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania. bb) Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
Podstawowe kształtowanie pasma oraz limity ilości danych	a) System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników. b) Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. c) System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Bezpieczna sieć bezprzewodowa	a) System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. b) Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater. c) Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. d) Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. e) Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej. f) Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej. g) Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.

	h) Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication). i) Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). j) System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. k) Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. l) System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden. m) System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe. n) Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
Autoryzacja użytkowników	a) Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication. b) Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. c) System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+. d) Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. e) Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password). f) Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server. g) System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. h) Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. i) Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
Samoobsługowy portal dla użytkowników	a) Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci. b) Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). c) Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows. d) Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android. e) Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła. f) Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika. g) Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.
Podstawowe opcje VPN	System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: a) Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem

	klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) b) Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	a) Dodatkowy moduł ochrony klasy IPS z bazą minimum 2500 sygnatur. b) Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS. c) Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. d) Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. e) System powinien generować alerty w przypadku wykrycia ataku.
ATP	System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.
Clientless VPN	Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	a) Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. b) Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP). c) System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. d) System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego. e) Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups). f) Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch). g) Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów. h) System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma. i) System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. j) Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów, cookies. k) System powinien zapewniać możliwość emulacji skryptów JavaScript. l) Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. m) Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. n) Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS. o) Rozwiązanie powinno umożliwiać blokadę stron HTTPS. p) Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS. q) Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/ tygodniowe/ miesięczne/ roczne dla użytkowników i grup użytkowników. r) System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość

	edytowania treści komunikatu i dodania logo organizacji.
Ochrona i kontrola aplikacji	a) Rozwiązanie powinno oferować bazę danych opisująca co najmniej 1500 aplikacji. b) Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. c) Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. d) Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania. e) Rozwiązanie powinno umożliwiać blokowanie: › aplikacji, które pozwalają na transfer plików (np. P2P). › komunikatorów internetowych, przynajmniej Skype, Gadu-gadu. › proxy uruchamianych poprzez przeglądarki internetowe. › streaming media (radio internetowe, Youtube, Vimeo). f) Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.
Kształtowanie pasma dla Web i Aplikacji	a) Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie. b) Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. c) Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared).
OCHRONA SERWERÓW APLIKACYJNYCH WEB	
WAF	a) Ochrona klasy Web Application Firewall. b) Funkcjonalność oparta o mechanizm Reverse Proxy. c) Rozwiązanie powinno oferować mechanizm URL hardening with deep-linking and directory traversal prevention. d) Rozwiązanie powinno oferować mechanizm Form hardening. e) Rozwiązanie powinno oferować ochronę przed SQL injection. f) Rozwiązanie powinno oferować ochronę przed Cross-site scripting. g) System powinien zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL). h) System powinien pozwalać na podpisywanie plików cookies. i) Rozwiązanie powinno oferować wsparcie dla Path-based routing. j) Rozwiązanie powinno oferować wsparcie dla Outlook Anywhere. k) Mechanizm Reverse authentication z automatycznym dodawaniem prefixu lub suffixu w trakcie autoryzacji użytkownika. l) Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych. m) Rozwiązanie powinno oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing). n) System powinien umożliwiać stosowania masek typu wildcard dla ścieżek dostępowych. o) System powinien umożliwiać stosowanie operatorów logicznych AND/OR.
LOGOWANIE I RAPORTOWANIE	
	a) System powinien umożliwiać składowanie oraz archiwizację logów. b) System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.

	c) System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali. d) System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. e) System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). f) Rozwiązanie powinno umożliwiać wysyłanie raportów via email. g) Rozwiązanie powinno generować raporty w PDF, HTML i XLS. h) Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. i) System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza j) System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację k) Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. l) System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora. m) System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.

1.7 Urządzenia brzegowe

Umożliwiają podłączenie zintegrowanej infrastruktury sieciowo-serwerowej do sieci Internet oraz połączenie trzech centrów danych między sobą.

Nazwa urządzenia	sztuk
Uniwersytet Szczeciński (ZCP)	
Switch minimum **4x10Gb SFP+**	4
Switch minimum **8x10Gb SFP+** oraz 10 portów RJ45 x 1Gb	1
Wkładki SFP+ LC MM 10Gb (min. 300 m)	10 (5 kompletów)
Wkładki SFP+ LC SM WDM 10Gb (min. 10km)	16 (8 kompletów)
Uniwersytet Gdański (ACP)	
Switch minimum **8x10Gb SFP+** oraz 10 portów RJ45 x 1Gb	2
Wkładki SFP+ LC SM WDM 10Gb (min. 800 m)	16 (8 kompletów)
Akademia Pomorska w Słupsku (PCP)	
Switch minimum **8x10Gb SFP+** oraz 10 portów RJ45 x 1Gb	3
Wkładki SFP+ LC SM WDM 10Gb	16 (8 kompletów)

1.8 Licencje oprogramowania wirtualizującego

Zamawiający wymaga dostarczenia licencji wirtualizatora zgodnego z opisem:

Pożądane parametry oprogramowania wirtualizacji:

1. Wirtualizator ma być zgodny natywnie z używanym w jednostkach zamawiającego (VMWARE 6.0 lub nowszym) .
2. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
3. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
4. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
5. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
6. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows, Linux.
7. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
8. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
9. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach.

10. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
11. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
12. Rozwiązanie musi mieć możliwość przenoszenia maszyn i dysków wirtualnych w czasie ich pracy pomiędzy zasobami dyskowymi i serwerami fizycznymi.
13. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
14. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

1.9 Certyfikowane Szkolenia (nieodpłatne)

W ramach oferowanej ceny, Zamawiający wymaga, przeprowadzenia / zapewnienia udziału w nieodpłatnych certyfikowanych szkoleniach prowadzonych przez podmiot posiadający uprawnienia nadane przez producenta do prowadzenia autoryzowanych szkoleń w jego imieniu, w zakresie:

1. **Serwery Pamięci Masowych na poziomie podstawowymi i zaawansowanym** – obejmującym rozległe klastry i replikację
2. **Oprogramowanie wirtualizacji** – Administracja

Liczba osób, które wezmą udział w szkoleniu: 6 osób.

1.10 Dokumentacja powykonawcza

Wykonawca dostarczy szczegółową dokumentacje powykonawczą zawierającą co najmniej opis konfiguracji oraz schematy połączeń dla każdej lokalizacji oraz pomiędzy lokalizacjami.

2 Włączenie Platformy w infrastrukturę centrów danych

Dostarczoną platformę należy włączyć, w istniejąca infrastrukturę Zamawiającego z wykorzystaniem dostarczonych urządzeń brzegowych. Opis zasobów, jakimi dysponuje Zamawiający w poszczególnych lokalizacjach zawarty jest PONIŻEJ:

UWAGA:
Zamawiający, zobowiązuje się do udostępnienia w każdym ośrodku:

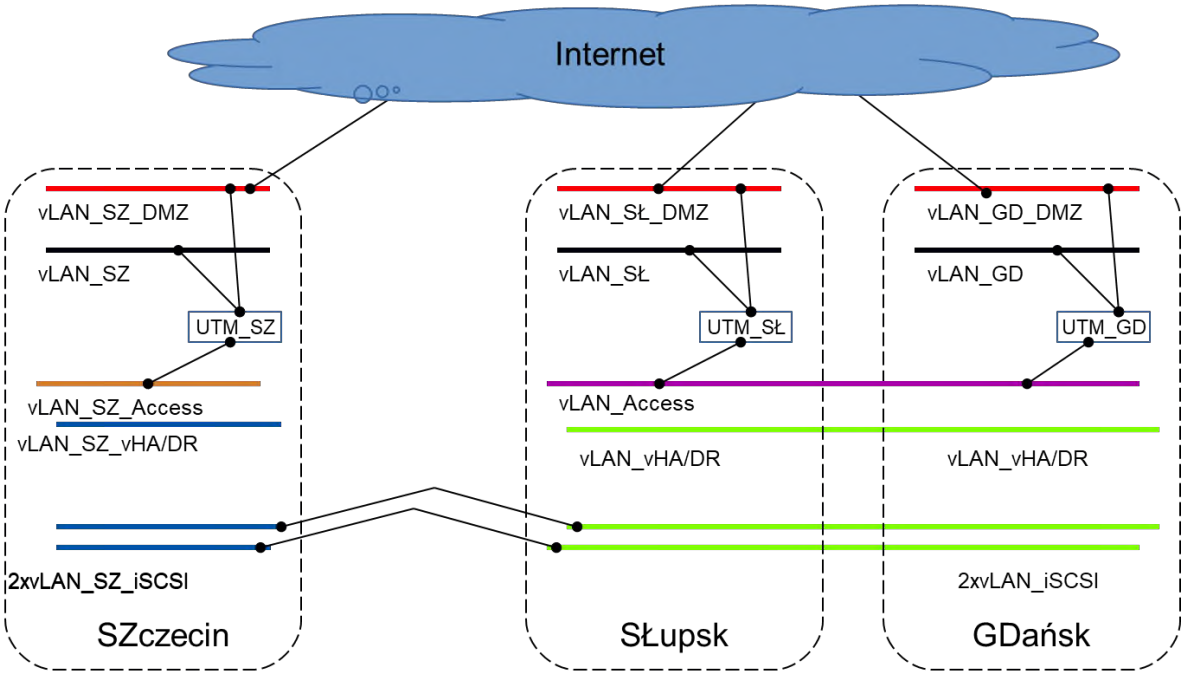
1. Przestrzeni na instalację szafy stelażowej 19” o wysokości 42U i wymiarach 600x1300.
2. Podłączenia dostarczonej infrastruktury do sieci energetycznej jednofazowej 4x 16A
3. Podłączenia dostarczonej platformy usługowej do istniejącej infrastruktury sieciowej LAN, w zależności od możliwości danego ośrodka, za pomocą jednego lub 2 portów 10GbE SR LC.
4. 10 portów 1GbE RJ45 (sieć zarządzająca)
5. Punktów podpięcia rozwiązań UTM/Firewall (wraz z dostosowaniem trybu ich pracy/strefy bezpieczeństwa/DMZ) w standardzie 1GbE RJ45 lub 10GbE SFP+.
6. Zamawiający zapewni wysokodostępne symetryczne łącza:

a. pomiędzy ośrodkami PCP i ACP o przepustowości 10 Gbps
b. pomiędzy ośrodkiem ZPC a ośrodkami PCP i ACP o przepustowości 10Gbps wspierające QinVNI funkcji VXLAN oraz Jumbo frames do 9200 B.

Rekomendowana konfiguracja logiczna segmentów sieciowych:

3. Segmenty sieciowe: vLAN_vHA/DR, vLAN_Access rozciągnięte pomiędzy ośrodkami **PCP i ACP** przy użyciu tunelowania QinVNI - funkcja VXLAN.
4. Podsieci vLAN_SZ_iSCSI_(1|2) oraz vLAN_ iSCSI_(1|2) połączone między sobą przy zastosowaniu routing'u (zamknięte podsieci obsługujące ruch techniczny – nie wymagają UTMa)
5. VLAN_SZczecin, VLAN_Słupsk, VLAN_GDańsk – segmenty sieciowe pozwalające na bezpośredni dostęp do platformy „Herbarium Pomeranicum" odpowiednio z sieci uczelnianych ośrodków.

Poglądowy schemat połączeń sieciowych dla planowanego rozwiązania przedstawia poniższy rysunek.



Rysunek 1: Schemat poglądowy połączeń sieciowych rozwiązania

3 Gwarancja i serwis

Dla każdej części zamówienia, o ile wymagania szczegółowe nie stanowią inaczej, Zamawiający wymaga udzielenia gwarancji na okres nie mniejszy niż 3 lata, zgodnie z warunkami podanymi poniżej.

3.1 Ogólne wymagania dotyczące sprzętu

1. Dostarczony sprzętu musi być objęta gwarancją zgodną z deklaracją Wykonawcy, zawartą w formularzy ofertowym.
2. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów lub ich autoryzowanych, w zakresie serwisu, partnerów.
3. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
4. Firma serwisująca musi posiadać autoryzacje producenta.

5. W przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, producent przejmie na siebie wszelkie zobowiązania związane z serwisem.
6. Wykonawca dostarczy wraz z towarem dokument gwarancji, jakości sprzętu wystawiony przez siebie lub producenta urządzenia, zobowiązujący wystawcę dokumentu (gwaranta) do usunięcia wady fizycznej towaru lub do dostarczenia towaru wolnego od wad, jeżeli wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
7. Okres gwarancji, które Wykonawca udzieli Zamawiającemu, będzie zgodny z wymaganiami wyspecyfikowanymi dla poszczególnych urządzeń i oprogramowania.
8. Bieg okresów gwarancyjnych rozpoczyna się z dniem podpisania Protokołu Odbioru Końcowego bez uwag (zastrzeżeń).
9. Czas naprawy wyłączony będzie z okresu gwarancyjnego. Czas trwania gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.
10. W okresie gwarancji, wszelkie koszty związane z usunięciem awarii, w tym dostarczenie uszkodzonego sprzętu do punktu serwisowego, obciążają wykonawcę.
11. Gwarancja obejmie wszystkie wykryte podczas eksploatacji sprzętu usterki i wady oraz uszkodzenia powstałe w czasie poprawnego zgodnego z instrukcją użytkowania.
12. Dla wszystkich urządzeń, które posiadają dyski twarde w razie awarii, Zamawiający wymaga, aby na czas naprawy dysk pozostał w siedzibie Zamawiającego.
13. Zasady eksploatacji i konserwacji urządzeń zostaną określone w przekazanej przez wykonawcę „Instrukcji użytkowania i eksploatacji urządzeń" wraz z wykazem urządzeń, które wymagają przeglądów serwisowych, które Wykonawca wykona na własny koszt.
14. W przypadku awarii sprzętu, która nie została usunięta w terminie 30 dni, Wykonawca zobowiązuje się do wymiany sprzętu na nowy o parametrach nie gorszych od sprzętu uszkodzonego. Wymiana sprzętu na nowy nastąpi najpóźniej w 35 dniu od zgłoszenia.
15. Wykonawca gwarantuje Zamawiającemu, że udzielając licencji na korzystanie z oprogramowania nie narusza żadnych praw osób trzecich oraz że nie zachodzą jakiekolwiek podstawy do zgłoszenia przez osoby trzecie roszczeń wobec tych praw. Wykonawca zabezpieczy Zamawiającego w zakresie zakupionych przez niego licencji przed roszczeniami osób trzecich. Wykonawca zobowiąże się do podjęcia na swój koszt i ryzyko wszelkich kroków prawnych zapewniających należytą ochronę przed roszczeniami osób trzecich oraz pokrycia wszelkich kosztów i strat z tym związanych, jak również związanych z naruszeniem przepisów Ustawy o prawie autorskim i prawach pokrewnych.
16. Wykonawca zapewni możliwość zgłaszania awarii sprzętu w okresie gwarancji telefonicznie, faksem oraz drogą mailową w godzinach od 8.00 do 17.00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy. Zgłoszenie awarii po godz. 17.00 będzie traktowane, jak zgłoszenie o godz. 8.00 następnego dnia roboczego.
17. Wykonawca, od momentu zgłoszenia, musi podjąć czynności serwisowych w czasie określonym dla poszczególnych urządzeń w tabelach powyżej.
18. W przypadku stwierdzenia wady ukrytej sprzętu (towaru) wykonawca musi wymienić go na nowy, w ciągu 14 dni roboczych od daty zgłoszenia tej wady.
19. Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu w godz. 7.30 -15.30.
20. W przypadku, kiedy Wykonawca uzna za konieczna naprawę sprzętu w serwisie, Wykonawca zapewni:
    a) odbiór na własny koszt wadliwego sprzętu (towaru) w terminie nieprzekraczającym 2 dni roboczych;
    b) dostawę naprawionego sprzętu na własny koszt w terminie nie przekraczającym 2 dni roboczych od dnia usunięcia awarii przez serwis, a w uzasadnionych przypadkach w terminie nie dłuższym niż 14 dni roboczych od odebrania sprzętu z siedziby zamawiającego
    c) w przypadku braku możliwości usunięcia awarii w terminie 14 dni roboczych od dnia odebrania wadliwego sprzętu (towaru) z siedziby zamawiającego, wykonawca zobowiąże się do bezpłatnego dostarczenia i uruchomienia nowego sprzętu zastępczego o

parametrach równoważnych z oferowanymi. Podstawiony sprzęt będzie miał zainstalowany uzgodniony z Zamawiającym system operacyjny i wszystkie dodatkowe, standardowe poprawki niezbędne do jego poprawnej pracy.

21. Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszty transportu sprzętu naprawianego w ramach gwarancji pokryje wykonawca.

3.2 Minimalne i wymagane okresy gwarancji

3.2.1 Szafa Rack 19”

- 60 miesięcy gwarancji na systemy awaryjnego podtrzymania zasilania (UPS)

3.2.2 Warstwa Serwerów Pamięci Masowej

- 7-letnia gwarancja producenta w miejscu instalacji.
- Możliwość zgłoszenia awarii przez 24 godziny na dobę.
- W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z Urządzeniem oraz oprogramowania wewnętrznego Urządzenia.
- Nośniki SSD muszą być objęte usługami wsparcia i gwarancji przy nieograniczonej intensywności wykorzystania (bez względu na intensywność zapisów).

3.2.3 Warstwa Sieciowa Data Center

- 60 miesięcy gwarancji i wsparcia w siedzibie klienta w trybie NBD

3.2.4 Warstwa Sprzętowych Serwerów Wirtualizacji x86_64

- 5-letnia gwarancja producenta serwera w miejscu instalacji świadczona w trybie NBD (9x5)
- Czas reakcji w miejscu instalacji to kolejny dzień roboczy.
- Wsparcie techniczne realizowane jest przez organizację serwisową producenta oferowanego serwera

3.2.5 Warstwa Sprzętowych Firewall/UTM

- Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 60 miesięcy
- Gwarancja i wsparcie techniczne producenta w trybie 8x5 na okres nie krótszy niż 60 miesięcy
- Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.

3.2.6 Urządzenia brzegowe

- 60 miesięcy gwarancji i wsparcia w siedzibie klienta w trybie NBD

3.2.7 Licencje oprogramowania wirtualizującego

- Okres wsparcia licencji ma być równy czasowi wsparcia oferowanych Urządzeń, jednak nie krócej niż 60 miesięcy

3.3 Opłaty utrzymaniowe

Zamawiający wymaga, aby cena ofertowa zawierała wszelkie opłaty serwisowe, utrzymaniowe (subskrypcje, aktualizacje, poprawki, dostęp do najnowszej wersji oprogramowania), licencyjne oraz wsparcia technicznego, w okresie zgodnym z deklaracją zawartą w formularzy ofertowym, jednak nie krótszym, o ile w tabelach powyżej nie wskazano inaczej, niż 60 miesięcy od daty podpisania protokołu odbioru końcowego.

3.4 Oprogramowanie

1. O ile w tabelach powyżej nie wskazano inaczej, Wykonawca, zapewni wsparcie techniczne producenta oprogramowania na okres zgodny z deklaracją zawartą w formularzy ofertowym, jednak nie krótszą niż 60 miesięcy.
2. Wsparcie techniczne obejmie co najmniej:

a) aktualizacje,
b) poprawki,
c) dostęp do najnowszych wersji oprogramowania

3. Wykonawca zapewni możliwość dokonywania nielimitowanej liczby zgłoszeń oraz pomoc techniczną w trybie 24h/7 lub 9h/5;
4. Wsparcie techniczne producenta musi być świadczone w formie zgłoszeń telefonicznych lub przez stronę www producenta oprogramowania;
5. Usługi wsparcia technicznego i subskrypcji edycji muszą być świadczone przez producenta oprogramowania;

3.5 Inne

Oferowane przez Wykonawcę w dniu składania ofert rozwiązania, nie mogą być przeznaczone przez ich producenta do wycofania z produkcji, sprzedaży lub z wsparcia technicznego.
Zamawiający wymaga, aby dostarczone wraz ze sprzętem oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.

UWAGA:
Zamawiający informuje, iż Infrastruktura będąca przedmiotem niniejszego zamówienia gwarantować musi skuteczne uruchomienie planowanych rozwiązań informatycznych – środowiska Platformy Herbarium Pomeranicum. Zamawiający pomocniczo wskazuje, celem należytego doboru oferowanych rozwiązań linkt, pod którym dostępna jest dokumentacja postępowania obejmującego realizację Platformy:
https://platformazakupowa.pl/transakcja/381931
Postępowanie prowadzone przez Akademię Pomorską w Słupsku.

ROZDZIAŁ 3

Zawarta w dniu …… w Szczecinie pomiędzy:

Uniwersytetem Szczecińskim, z siedzibą przy al. Papieża Jana Pawła II nr 22a, 70 - 453 Szczecin, NIP 851-020-80-05, reprezentowanym przez:

zwanym dalej w treści umowy **Zamawiającym, działającym w imieniu swoim oraz:**

- **Akademii Pomorskiej w Słupsku z siedzibą w: Słupsk 76-200, przy ul. Krzysztofa Arciszewskiego 22a, NIP: 8391028460, REGON: 000001459;**
- **Uniwersytetu Gdańskiego, z siedzibą w Gdańsku przy ul. Bażyńskiego 8, 80-309 Gdańsk, NIP 584-020-32-39, REGON 000001330**

a

……
……
……
……
zwanym dalej w treści umowy **Wykonawcą**

W wyniku przeprowadzonego postępowania w trybie przetargu nieograniczonego (TP/371/142/20) zgodnie z Ustawą z dnia 29 stycznia 2004 r. *Prawo Zamówień Publicznych* zawarta została umowa następującej treści:

§ 1
Przedmiot umowy

1. Przedmiotem niniejszej umowy jest zakup, dostawa, instalacja i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum" w trzech istniejących centrach danych w ramach projektu „Zintegrowane wirtualne Herbarium Pomorza Herbarium Pomeranicum – digitalizacja i udostępnienie zbiorów herbariów jednostek akademickich Pomorza poprzez ich połączenie i udostępnienie cyfrowe" współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020", w tym:
   1) ……. dla Akademii Pomorskiej w Słupsku (Herbarium SLTC)
   2) ……. dla Uniwersytetu Gdańskiego (Herbarium UGDA)
   3) ……. dla Uniwersytetu Szczecińskiego (Herbarium SZUB)
2. Zakres rzeczowy przedmiotu umowy określa Rozdział 2 SIWZ oraz oferta Wykonawcy stanowiąca integralną część niniejszej umowy.
3. Wykonanie przedmiotu zamówienia, o którym mowa w ust. 1 obejmuje nieodpłatny transport wraz z wniesieniem do wskazanych pomieszczeń oraz montaż.
4. Wykonawca wykona nieodpłatnie instruktaż obsługi sprzętu dla personelu Zamawiającego, Akademii Pomorskiej w Słupsku a także Uniwersytetu Gdańskiego, nie później niż w terminie dostawy.
5. Wykonawca gwarantuje, że dostarczony przedmiot Umowy będzie fabrycznie nowy i wolny od wad, a także nie jest urządzeniem odnawianym, demonstracyjnym, powystawowym, prototypowym i reprezentuje model bieżącej linii produkcyjnej oraz będzie w pełni zgodny z Ofertą Wykonawcy.
6. Wykonawca przekaże Zamawiającemu, Akademii Pomorskiej w Słupsku oraz Uniwersytetowi Gdańskiemu instrukcję w formie elektronicznej dla każdego typu urządzenia, opisującą zasady jego właściwej eksploatacji, napisaną w języku polskim, która będzie przygotowana przez producenta urządzenia albo przez Wykonawcę lub na jego zlecenie. Instrukcja zostanie dostarczona Zamawiającemu najpóźniej w dniu ustawienia pierwszego z urządzeń danego typu. Dostarczenie instrukcji dla danego typu urządzenia będzie każdorazowo potwierdzone w Protokole odbioru sporządzanym po dostarczeniu urządzeń.
7. Wykonawca oświadcza, że znane mu są warunki dostępu do lokali Zamawiającego, Akademii Pomorskiej w Słupsku a także Uniwersytetu Gdańskiego, oraz możliwych miejsc ustawienia urządzeń, w szczególności rodzaj i wielkość ciągów komunikacyjnych prowadzących do miejsc przewidzianych do ustawienia urządzeń i ograniczenia w zakresie wjazdu i parkowania pojazdów przy wejściach do budynku. Zamawiający zobowiązuje się zapoznać Wykonawcę z ograniczeniami i wymogami związanymi z ruchem osobowo-materiałowym na terenie obiektów Zamawiającego, Akademii Pomorskiej w Słupsku oraz Uniwersytetu Gdańskiego, do których przedstawiciele Wykonawcy oraz wszystkie inne osoby, którymi Wykonawca będzie się posługiwał przy realizacji Umowy, będą zobowiązane stosować się do obowiązujących w obszarach Zamawiającego, Akademii Pomorskiej w Słupsku oraz Uniwersytetu Gdańskiego zasad bezpieczeństwa fizycznego.
8. Termin realizacji przedmiotu umowy …… dni od dnia podpisania umowy.
9. Potwierdzeniem wykonania umowy w zakresie dostarczenia wszystkich urządzeń, wdrożenia Przedmiotu Umowy, oraz przeprowadzenia szkoleń/instruktażu będzie:
   1) W zakresie przedmiotu zamówienia wskazanego w ust. 1 pkt 1 - podpisany przez przedstawiciela Akademii Pomorskiej w Słupsku wskazanego w § 5 Umowy i Wykonawcę Protokół odbioru;
   2) W zakresie przedmiotu zamówienia wskazanego w ust. 1 pkt 2 - podpisany przez przedstawiciela Uniwersytetu Gdańskiego wskazanego w § 5 Umowy i Wykonawcę Protokół odbioru;
   3) W zakresie przedmiotu zamówienia wskazanego w ust. 1 pkt 3 - podpisany przez przedstawiciela Zamawiającego wskazanego w § 5 Umowy i Wykonawcę Protokół odbioru;

§ 2

Wynagrodzenie

1. Wartość niniejszej umowy zostaje określona na …….. zł netto: (słownie złotych netto: …….…… złotych /100), w tym:
   1) Wartość odpowiadająca zobowiązaniu Akademii Pomorskiej w Słupsku wynikająca z realizacji zamówienia wskazanego w § 1 ust. 1 pkt 1 Umowy - …….. zł netto: (słownie złotych netto: …….…… złotych /100);
   2) Wartość odpowiadająca zobowiązaniu Uniwersytetu Gdańskiego wynikająca z realizacji zamówienia wskazanego w § 1 ust. 1 pkt 2 Umowy - …….. zł netto: (słownie złotych netto: …….…… złotych /100);
   3) Wartość odpowiadająca zobowiązaniu Zamawiającego wynikająca z realizacji zamówienia wskazanego w § 1 ust. 1 pkt 3 Umowy - …….. zł netto: (słownie złotych netto: …….…… złotych /100);
2. Wartość umowy wskazana w ust. 1 zawiera wszystkie składniki cenotwórcze za wyjątkiem podatku VAT.
3. Zapłata wynagrodzenia należnego Wykonawcy nastąpi w częściach, po dostarczeniu do siedziby:
   1) Akademii Pomorskiej w Słupsku prawidłowo wystawionej faktury obejmującej łączną kwotę brutto (netto + VAT) za wykonanie całości przedmiotu zamówienia wskazanego w § 1 ust. 1 pkt 1 Umowy wraz z załączoną do niej specyfikacją cen jednostkowych oraz załączonym protokołem odbioru bez uwag podpisanego przez przedstawiciela Akademii Pomorskiej w Słupsku;
   2) Uniwersytetu Gdańskiego prawidłowo wystawionej faktury obejmującej łączną kwotę brutto (netto + VAT) za wykonanie całości przedmiotu zamówienia wskazanego w § 1 ust. 1 pkt 2 Umowy wraz z załączoną do niej specyfikacją cen jednostkowych oraz załączonym protokołem odbioru bez uwag podpisanego przez przedstawiciela Uniwersytetu Gdańskiego;
   3) Zamawiającego prawidłowo wystawionej faktury obejmującej łączną kwotę brutto (netto + VAT) za wykonanie całości przedmiotu zamówienia wskazanego w § 1 ust. 1 pkt 3 Umowy wraz z załączoną do niej specyfikacją cen jednostkowych oraz załączonym protokołem odbioru bez uwag podpisanego przez przedstawiciela Zamawiającego.
4. Części wynagrodzenia należnego Wykonawcy, o którym mowa w ust. 1 uiszczane będą przez:
   1) Akademię Pomorską w Słupsku za wykonanie całości przedmiotu zamówienia wskazanego w § 1 ust. 1 pkt 1 Umowy;
   2) Uniwersytet Gdański - za wykonanie całości przedmiotu zamówienia wskazanego w § 1 ust. 1 pkt 2 Umowy;
   3) Zamawiającego - za wykonanie całości przedmiotu zamówienia wskazanego w § 1 ust. 1 pkt 3 Umowy.
5. Wynagrodzenie netto określone w ust. 1 podlega powiększeniu o należny w dniu wystawienia faktury przez Wykonawcę podatek od towarów i usług, z zastrzeżeniem postanowień ust. 6.
6. Wykonawca gwarantuje dostawy sprzętu informatycznego z podatkiem VAT = 0% (zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług po dostarczeniu odpowiednio przez Zamawiającego, Akademię Pomorską w Słupsku oraz Uniwersytet Gdański niezbędnych dokumentów. Zmiany aktów prawnych w tym zakresie zobowiązują strony do odpowiedniej zmiany umowy.
7. Zamawiający nie przewiduje możliwości prowadzenia rozliczeń w walutach obcych. Rozliczenia będą dokonywane w złotych polskich (PLN).
8. W przypadku stwierdzenia wad przy odbiorze przedmiotu umowy lub w trakcie weryfikacji wypłata wynagrodzenia należnego Wykonawcy nastąpi po usunięciu wad.
9. Wierzytelności wynikające z realizacji niniejszej umowy nie mogą być przenoszone przez *Wykonawcę* na rzecz osób trzecich bez zgody *Zamawiającego* wyrażonej na piśmie pod rygorem nieważności.

10. Zapłaty wynagrodzenia nastąpi przelewem, na konto *Wykonawcy* wskazane na fakturze, w terminie do 21 dni kalendarzowych od daty otrzymania faktury wraz z podpisanym protokołem odbioru bez wad.
8. Wynagrodzenie Wykonawcy jest współfinansowane przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego.
9. Wykonawca oświadcza, iż został poinformowany o fakcie współfinansowania projektu oraz wynagrodzenia ze środków Europejskiego Funduszu Rozwoju Regionalnego.

§ 3
Gwarancja i rękojmia.

1. Wykonawca udziela odpowiednio Zamawiającemu, Akademii Pomorskiej w Słupsku oraz Uniwersytetowi Gdańskiemu gwarancji i rękojmi na okres wskazany w ofercie Wykonawcy, początek licząc od daty podpisania Protokołu końcowego odbioru bez uwag.
2. Zamawiający, Akademia Pomorska w Słupsku oraz Uniwersytet Gdański który otrzymał wadliwy przedmiot umowy, wykonując uprawnienia z tytułu rękojmi względem Wykonawcy, może żądać bezpłatnego usunięcia wad w terminie uzgodnionym z Wykonawcą. Wykonawca nie może odmówić usunięcia wady, choćby wymagało to poniesienia dodatkowych nakładów finansowych przez Wykonawcę.
3. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów lub ich autoryzowanych, w zakresie serwisu, partnerów.
4. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
5. Firma serwisująca musi posiadać autoryzacje producenta.
6. Zasady wykonywania napraw urządzeń oraz oprogramowania, w przypadku niesprawności urządzenia lub oprogramowania (awarii):
    1) za „awarię" uznaje się stan niesprawności urządzenia lub oprogramowania polegający na tym, że urządzenie (jedno lub więcej) lub oprogramowanie albo jakakolwiek ich część składowa, nie funkcjonuje albo nie funkcjonuje poprawnie. Stan niesprawności urządzenia lub oprogramowania będzie uznany za „awarię" niezależnie od przyczyny jego wystąpienia, w tym również w przypadku, gdy spowodowany on będzie działaniami lub zaniechaniami pracowników Zamawiającego, za wyjątkiem przypadków, gdy niesprawność powstała na skutek winy umyślnej pracownika lub pracowników odpowiednio Zamawiającego, Akademii Pomorskiej w Słupsku lub Uniwersytetu Gdańskiego;
    2) za „zgłoszenie serwisowe" uznaje się przekazanie przez wskazanych pracowników odpowiednio Zamawiającego, Akademii Pomorskiej w Słupsku lub Uniwersytetu Gdańskiego informacji o awarii, telefonicznie na numer …… lub w formie elektronicznej, na adres: ……. zawierającej dane potrzebne do podjęcia przez Wykonawcę działań zmierzających do usunięcia awarii. Powyższy numer telefonu oraz adres poczty elektronicznej będą wykorzystywane przez Strony wyłącznie do przekazywania przez odpowiednio Zamawiającego, Akademię Pomorską w Słupsku lub Uniwersytet Gdański zgłoszeń serwisowych;
    3) zgłoszenia serwisowe przekazywane będą w dni robocze, za dzień i godzinę przekazania przez odpowiednio Zamawiającego, Akademię Pomorską w Słupsku lub Uniwersytet Gdański zgłoszenia serwisowego uznaje się dzień i godzinę przekazania przez odpowiednio Zamawiającego, Akademię Pomorską w Słupsku lub Uniwersytet Gdański informacji zawierającej zgłoszenie serwisowe na powyższy numer telefonu lub adres poczty elektronicznej Wykonawcy, przy czym przekazanie informacji jest dokonane w momencie:
        a) podjęcia rozmowy telefonicznej przez przedstawiciela Wykonawcy (rozpoczęcia połączenia głosowego) albo;
        b) wprowadzenia informacji do pamięci serwera, na którym utworzone zostało konto dla odpowiedniego adresu poczty elektronicznej odpowiednio Zamawiającego, Akademii Pomorskiej w Słupsku lub Uniwersytetu Gdańskiego. W przypadku, gdy

Zamawiający, Akademia Pomorska w Słupsku lub Uniwersytet Gdański przekaże informację drogą telefoniczną oraz nada dokument za pomocą poczty elektronicznej, za dzień i godzinę przekazania zgłoszenia serwisowego uznaje się dzień i godzinę wykonania przez odpowiednio Zamawiającego, Akademię Pomorską w Słupsku lub Uniwersytet Gdański pierwszej z powyższych czynności;

7. W przypadku niewywiązywania się z obowiązków gwarancyjnych przez Wykonawcę lub firmę serwisującą, producent przejmie na siebie wszelkie zobowiązania związane z serwisem.
8. Wykonawca dostarczy wraz z towarem dokument gwarancji, jakości sprzętu wystawiony przez siebie lub producenta urządzenia, zobowiązujący wystawcę dokumentu (gwaranta) do usunięcia wady fizycznej towaru lub do dostarczenia towaru wolnego od wad, jeżeli wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
9. Okres gwarancji, które Wykonawca udzieli odpowiednio Zamawiającemu, Akademii Pomorskiej w Słupsku oraz Uniwersytetowi Gdańskiemu, będzie zgodny z wymaganiami wyspecyfikowanymi dla poszczególnych urządzeń i oprogramowania.
10. Bieg okresów gwarancyjnych rozpoczyna się z dniem podpisania Protokołu Odbioru Końcowego bez uwag (zastrzeżeń).
11. Czas naprawy wyłączony będzie z okresu gwarancyjnego. Czas trwania gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.
12. W okresie gwarancji, wszelkie koszty związane z usunięciem awarii, w tym dostarczenie uszkodzonego sprzętu do punktu serwisowego, obciążają wykonawcę.
13. Gwarancja obejmie wszystkie wykryte podczas eksploatacji sprzętu usterki i wady oraz uszkodzenia powstałe w czasie poprawnego zgodnego z instrukcją użytkowania.
14. Dla wszystkich urządzeń, które posiadają dyski twarde w razie awarii, Zamawiający wymaga, aby na czas naprawy dysk pozostał w siedzibie odpowiednio Zamawiającego, Akademii Pomorskiej w Słupsku lub Uniwersytetu Gdańskiego.
15. Zasady eksploatacji i konserwacji urządzeń zostaną określone w przekazanej przez wykonawcę „Instrukcji użytkowania i eksploatacji urządzeń" wraz z wykazem urządzeń, które wymagają przeglądów serwisowych, które Wykonawca wykona na własny koszt.
16. W przypadku awarii sprzętu, która nie została usunięta w terminie 30 dni, Wykonawca zobowiązuje się do wymiany sprzętu na nowy o parametrach nie gorszych od sprzętu uszkodzonego. Wymiana sprzętu na nowy nastąpi najpóźniej w 35 dniu od zgłoszenia.
17. Wykonawca gwarantuje, że udzielając licencji na korzystanie z oprogramowania nie narusza żadnych praw osób trzecich oraz że nie zachodzą jakiekolwiek podstawy do zgłoszenia przez osoby trzecie roszczeń wobec tych praw. Wykonawca zabezpieczy Zamawiającego, Akademię Pomorskiej w Słupsku oraz Uniwersytet Gdański w zakresie zakupionych przez nich licencji przed roszczeniami osób trzecich. Wykonawca zobowiąże się do podjęcia na swój koszt i ryzyko wszelkich kroków prawnych zapewniających należytą ochronę przed roszczeniami osób trzecich oraz pokrycia wszelkich kosztów i strat z tym związanych, jak również związanych z naruszeniem przepisów Ustawy o prawie autorskim i prawach pokrewnych.
18. Wykonawca zapewni możliwość zgłaszania awarii sprzętu w okresie gwarancji telefonicznie, faksem oraz drogą mailową w godzinach od 8.00 do 17.00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy. Zgłoszenie awarii po godz. 17.00 będzie traktowane, jak zgłoszenie o godz. 8.00 następnego dnia roboczego.
19. Wykonawca, od momentu zgłoszenia, musi podjąć czynności serwisowych w czasie określonym w Rozdziale 2 SIWZ dla poszczególnych urządzeń.
20. W przypadku stwierdzenia wady ukrytej sprzętu (towaru) wykonawca musi wymienić go na nowy, w ciągu 14 dni roboczych od daty zgłoszenia tej wady.
21. Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu w godz. 7.30 -15.30.
22. W przypadku, kiedy Wykonawca uzna za konieczna naprawę sprzętu w serwisie, Wykonawca zapewni:
    1) odbiór na własny koszt wadliwego sprzętu (towaru) w terminie nieprzekraczającym 2 dni roboczych;

2) dostawę naprawionego sprzętu na własny koszt w terminie nie przekraczającym 2 dni roboczych od dnia usunięcia awarii przez serwis, a w uzasadnionych przypadkach w terminie nie dłuższym niż 14 dni roboczych od odebrania sprzętu z siedziby zamawiającego
3) w przypadku braku możliwości usunięcia awarii w terminie 14 dni roboczych od dnia odebrania wadliwego sprzętu (towaru) z siedziby zamawiającego, wykonawca zobowiąże się do bezpłatnego dostarczenia i uruchomienia nowego sprzętu zastępczego o parametrach równoważnych z oferowanymi. Podstawiony sprzęt będzie miał zainstalowany uzgodniony z Zamawiającym system operacyjny i wszystkie dodatkowe, standardowe poprawki niezbędne do jego poprawnej pracy.

23. Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszty transportu sprzętu naprawianego w ramach gwarancji pokryje wykonawca.

§ 4

Odbiory i przeglądy gwarancyjne

1. Strony postanawiają, że odbiorowi końcowemu podlegać będzie przedmiot umowy, o którym mowa w §1 niniejszej umowy.
2. Podczas odbioru przeprowadzone będą testy sprawności dostarczonego sprzętu i oprogramowania.
3. Wykonawca zgłosi odpowiednio Zamawiającemu, Akademii Pomorskiej w Słupsku oraz Uniwersytetowi Gdańskiemu gotowość do odbioru przedmiotu umowy w formie zgłoszenia pisemnego.
4. Zamawiający, Akademia Pomorska w Słupsku oraz Uniwersytet Gdański zobowiązują się do wyznaczenia terminu odbioru i jego rozpoczęcia w terminie 7 dni kalendarzowych od daty dokonania zawiadomienia o gotowości, zawiadamiając o tym pisemnie Wykonawcę.
5. Wykonawca przekaże odpowiednio Zamawiającemu, Akademii Pomorskiej w Słupsku oraz Uniwersytetowi Gdańskiemu wszelkie dokumenty potwierdzające gwarancję na zainstalowany sprzęt oraz ewentualne certyfikaty użytkowania
6. Zamawiający, Akademia Pomorska w Słupsku oraz Uniwersytet Gdański zastrzega sobie możliwość dokonania odbioru przedmiotu umowy także podczas nieobecności prawidłowo zawiadomionego Wykonawcy.
7. Zakończenie czynności odbiorowych zostanie potwierdzone Protokołem końcowym odbioru przedmiotu umowy.
8. Wykonawca zobowiązuje się do pisemnego zawiadomienia o planowanym przeglądzie gwarancyjnym Zamawiającego, Akademię Pomorska w Słupsku oraz Uniwersytet Gdański na co najmniej 5 dni kalendarzowych przed planowanym terminem.
9. Wykonawca zobowiązuje się do przyjęcia i realizacji wniosków zawartych w protokole z przeglądu gwarancyjnego przeprowadzonego przez odpowiednio Zamawiającego, Akademię Pomorską w Słupsku lub Uniwersytet Gdański w trybie ust. 6 i 7.

§ 5

Reprezentacja stron

W sprawach związanych z realizacją niniejszej umowy:

a) Zamawiającego reprezentować będzie:
……e-mail: .....
b) Akademię Pomorską w Słupsku reprezentować będzie:
……e-mail: .....
c) Uniwersytet Gdański reprezentować będzie:
……e-mail: .....
d) Wykonawcę reprezentować będzie:
.....e-mail .....

§ 6

Kary umowne i odszkodowania

1. *Zamawiający, Akademia Pomorska w słupsku oraz Uniwersytet Gdański (odpowiednio)* może żądać od *Wykonawcy* następujących kar umownych:

a) za zwłokę w wykonaniu przedmiotu umowy – kara w wysokości 0,5 % wynagrodzenia netto, o którym mowa w § 2 ust. 1 nie zrealizowanej części przedmiotu umowy za każdy dzień zwłoki, liczony od terminu ustalonego w umowie, nie więcej jednak niż 50% wynagrodzenia umownego netto o którym mowa w § 2 ust. 1 umowy,
b) za zwłokę w wymianie sprzętu, który nie odpowiadał zamówieniu, był uszkodzony lub niesprawny w dacie odbioru – kara w wysokości 0,5 % ceny netto sprzętu podlegającego wymianie za każdy dzień zwłoki, jednak nie mniej niż 100,00 zł i nie więcej niż 50 % wynagrodzenia netto, o którym mowa w § 2 ust. 1,
c) za zwłokę w usunięciu wady sprzętu w okresie gwarancji, w tym jego naprawy lub wymiany – kara w wysokości 0,5 % wynagrodzenia netto, o którym mowa w § 2 ust. 1, nie więcej jednak niż 50% wynagrodzenia umownego netto o którym mowa w § 2 ust. 1 umowy
d) za odstąpienie od umowy z przyczyn leżących po stronie *Wykonawcy* – kara w wysokości 25 %, wynagrodzenia netto, o którym mowa w § 2 ust. 1.

2. *Zamawiający* może dokonać potrącenia naliczonych kar umownych z wynagrodzenia należnego *Wykonawcy.*
3. *Zamawiający* zastrzega sobie prawo dochodzenia na zasadach ogólnych odszkodowania uzupełniającego w przypadku, gdy szkoda przewyższa wysokość kar umownych.

§ 7
Odstąpienie od umowy

1. *Zamawiający* może odstąpić od umowy jeżeli *Wykonawca* nie wykonuje lub nienależycie wykonuje umowę. W takiej sytuacji *Zamawiający* przed odstąpieniem od umowy wzywa *Wykonawcę* do zmiany sposobu realizacji umowy wyznaczając mu odpowiedni termin, z zastrzeżeniem, że upływie wyznaczonego terminu od umowy odstąpi. *Zamawiający* może odstąpić od umowy w ciągu 14 dni od bezskutecznego upływu wyznaczonego *Wykonawcy* terminu.
2. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, *Zamawiający* może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.
3. W przypadku odstąpienia od umowy przez *Zamawiającego* z powodu okoliczności, o których mowa w ust. 1,2 *Wykonawca* może żądać wyłącznie wynagrodzenia należnego mu z tytułu wykonania części umowy, bez prawa dochodzenia odszkodowania z tego tytułu.

§ 8
Zmiana umowy

1. Dopuszcza się zmianę postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w przypadku wystąpienia następujących zdarzeń:
   1) wystąpienia zmian powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu umowy;
   2) zmiany terminu realizacji przedmiotu umowy z przyczyn niezależnych od Wykonawcy;
   3) siły wyższej lub powstałej z winy osób trzecich uniemożliwiająca wykonanie przedmiotu umowy zgodnie z Umową;
   4) rezygnacji przez Zamawiającego z realizacji części przedmiotu umowy; w takim przypadku wynagrodzenie przysługujące Wykonawcy zostanie pomniejszone, przy czym Zamawiający zapłaci za wszystkie spełnione świadczenia oraz udokumentowane koszty, które wykonawca poniósł w związku z wynikającymi z umowy planowanymi świadczeniami;
   5) wystąpienia przeszkód o obiektywnym charakterze (zdarzenia zewnętrzne i niemożliwe do zapobieżenia).
2. Niezależnie od powyższego, Strony dopuszczają możliwość zmian redakcyjnych Umowy oraz zmian będących następstwem zmian danych Stron ujawnionych w rejestrach publicznych, a także zmian korzystnych z punktu widzenia realizacji przedmiotu umowy, w szczególności

przyspieszających realizację, obniżających koszt ponoszony przez Zamawiającego na wykonanie, utrzymanie lub użytkowanie przedmiotu umowy bądź zwiększających użyteczność przedmiotu umowy. W takiej sytuacji, strony wprowadzą do umowy stosowne zmiany weryfikujące redakcyjne dotychczasowe brzmienie umowy bądź wskazujące nowe dane wynikające ze zmian w rejestrach publicznych albo też kierując się poszanowaniem wzajemnych interesów, zasadą równości Stron oraz ekwiwalentności świadczeń i przede wszystkim zgodnym zamiarem wykonania przedmiotu umowy, określą zmiany korzystne z punktu widzenia realizacji przedmiotu umowy.

3. W razie wątpliwości, przyjmuje się, że nie stanowią zmiany umowy następujące zmiany:
   1) danych związanych z obsługą administracyjno-organizacyjną Umowy,
   2) danych teleadresowych,
   3) danych rejestrowych,
   4) będące następstwem sukcesji uniwersalnej po jednej ze stron Umowy.
4. Wszelkie zmiany do Umowy wymagają pisemnego aneksu podpisanego przez strony pod rygorem nieważności.

§ 9.
[INFORMACJE PRAWNIE CHRONIONE]

1. Umowa jest jawna i podlega udostępnieniu na zasadach określonych w przepisach ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
2. Wykonawca zobowiązuje się w okresie obowiązywania Umowy oraz po jej wygaśnięciu lub rozwiązaniu, do zachowania w ścisłej tajemnicy wszelkich informacji dotyczących Zamawiającego, obejmujących:
   1) dane osobowe - chronione na podstawie 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) (Dz.U.UE. z 2016 r., L 119, poz. 1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   2) informacje stanowiące tajemnicę przedsiębiorstwa - chronione na podstawie ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
   3) informacje, które mogą mieć wpływ na funkcjonowanie lub stan bezpieczeństwa Zamawiającego.
3. Informacje, o których mowa w ust. 2 zwane są dalej „informacjami prawnie chronionymi".
4. Wykonawca oświadcza, że posiada wdrożoną i udokumentowaną politykę bezpieczeństwa informacji na dowód czego może przedstawić do wglądu Zamawiającego, na jego żądanie, stosowną dokumentację.
5. Informacje prawnie chronione mogą być udostępnione jedynie na podstawie stosownych przepisów prawa tylko w zakresie niezbędnym dla należytego wykonania przedmiotu umowy.
6. Obowiązek zachowania poufności nie dotyczy informacji ujawnionych publicznie, czy powszechnie znanych i trwa także po wykonaniu Umowy.
7. Wykonawca zobowiązany jest do realizacji postanowień umowy z zachowaniem należytej staranności, jak również zabezpieczenia i zachowania w tajemnicy - zarówno w trakcie trwania umowy, jak i po jej ustaniu - wszelkich informacji i danych osobowych, nie będących jawnymi, do których uzyska dostęp w związku z realizacją umowy.
8. Ujawnianie informacji prawnie chronionych, niezależnie od sposobu ich ujawnienia, w celu innym niż należyte wykonanie umowy, jest co do zasady niedopuszczalne chyba, że Zamawiający uprzednio wyrazi na to zgodę w formie pisemnej pod rygorem nieważności.
9. W przypadku korzystania przez Wykonawcę z usług podmiotów trzecich, w ramach realizacji których wystąpi konieczność przekazania im informacji o których mowa w niniejszym paragrafie, nakłada on na takie podmioty identyczne zobowiązania jakie ciążą na nim w związku z zapisami tego paragrafu.
10. Strona ma obowiązek zapewnić ochronę informacji prawnie chronionych według najwyższych przewidzianych prawem standardów, w tym zapewnić ochronę systemów i sieci

teleinformatycznych, w których są przetwarzane, przechowywane lub przekazywane informacje prawnie chronione drugiej Strony, a także kontrolować ochronę tych informacji.

11. W przypadku, gdy Strona została zobowiązana do ujawnienia informacji prawnie chronionych w całości lub w części uprawnionemu organowi, w granicach obowiązującego prawa, Strona ta zobowiązana jest jedynie uprzedzić drugą Stronę o nałożonym na nią obowiązku.
12. W razie powzięcia przez Stronę wiedzy o nieuprawnionym ujawnieniu informacji prawnie chronionych zobowiązana jest ona niezwłocznie powiadomić o tym fakcie drugą Stronę w celu umożliwienia jej podjęcia stosowanych środków zapobiegawczych.
13. Powierzone Wykonawcy dane osobowe mogą być przetwarzane wyłącznie w celu należytego wykonania umowy.
14. W przypadku naruszenia przepisów, o których mowa w ust. 2, z przyczyn leżących po stronie Wykonawcy, w następstwie którego Zamawiający zostanie zobowiązany do zapłaty odszkodowania, innej należności lub ukarany grzywną, Wykonawca zobowiązuje się zapłacić na rzecz Zamawiającego ww. koszty związane z zapłatą ww. odszkodowań, innych należności lub grzywien a także koszty ewentualnego postępowania toczącego się w związku z naruszeniem ww. przepisów.

§ 10.
[KLAUZULA SALWATORYJNA]

1. W razie gdyby którekolwiek z postanowień niniejszej Umowy było lub miało stać się nieważne, ważność całej Umowy pozostaje przez to w pozostałej części nienaruszona.
2. W takim przypadku strony Umowy zastąpią nieważne postanowienie innym, wiążącym prawnie postanowieniem, które możliwie najwierniej oddaje zamierzony cel gospodarczy nieważnego postanowienia. Odpowiednio dotyczy to także ewentualnych luk w Umowie.

§ 11
Adres do korespondencji

Strony podają jako adresy do korespondencji adresy wskazane we wstępie do niniejszej umowy. Każda ze stron zobowiązana jest do powiadomienia drugiej strony o zmianie adresu. W przypadku zaniechania zawiadomienia skuteczne jest skierowanie oświadczenia na ostatni znany drugiej stronie adres.

§ 12

1. Wszelkie spory powstałe w związku z umową będą rozstrzygane przez Sąd właściwy ze względu na siedzibę *Zamawiającego*.
2. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu Cywilnego, ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych wraz z przepisami wykonawczymi i inne obowiązujące przepisy prawa.
3. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Signature Not Verified
Dokument podpisany przez Wojciech Jerzy Bereszko
Data: 2020.10.24 11:49:05 CEST

……
/Dział Zamówień Publicznych/

Specyfikację istotnych warunków zamówienia zatwierdzam

Szczecin, ...

Andrzej Stanisław Jakubowski
Elektronicznie podpisany przez Andrzej Stanisław Jakubowski
Data: 2020.10.24 12:00:07 +02'00'
/Zamawiający/