DZIAŁ ZAMÓWIEŃ PUBLICZNYCH
UNIWERSYTETU JAGIELLOŃSKIEGO
Ul. Straszewskiego 25/2, 31-113 Kraków
tel. +4812-432-44-50, fax +4812-432-44-51 lub +4812-663-39-14;
e-mail: bzp@uj.edu.pl www.uj.edu.pl
http://przetargi.adm.uj.edu.pl/ogloszenia.php

Kraków dn., 29 czerwca 2017 r.

Zaproszenie do składania ofert zwane dalej „Zaproszeniem" lub „Z"

1) Nazwa (firma) oraz adres Zamawiającego.

1. Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków.
2. Jednostka prowadząca sprawę:

2.1 Dział Zamówień Publicznych UJ, Straszewskiego 25/2, 31-113 Kraków
2.1.1 tel. +4812-663-39-03; faks +4812-663-39-14;
2.1.2 e-mail: bzp@uj.edu.pl
2.1.3 strona internetowa: www.uj.edu.pl
2.1.4 miejsce publikacji ogłoszeń i informacji:
http://zamowienia.uj.edu.pl/ogloszenia.php

2) Tryb udzielenia zamówienia.

1. Postępowanie o udzielenie zamówienia z dziedziny nauki prowadzone jest w trybie procedury ogłoszenia zaproszenia do złożenia ofert w oparciu o art. 4d ust. 1 pkt. 1 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2015 r., poz. 2164 z późn. zm.) oraz art. 30a – 30d ustawy z dnia 30 kwietnia 2010r. o zasadach finansowania nauki (t.j. Dz. U. z2014 r., poz. 1620 z pózn. zm.) oraz ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t. j. Dz. U. 2017 poz. 459 z późn zm.).
2. Do czynności podejmowanych przez Podmiot zamawiający, zwany dalej Zamawiającym i Podmiot zainteresowany, zwany dalej Wykonawcą, w postępowaniu o udzielenie zamówienia stosuje się zapisy przedstawione w niniejszym Zaproszeniu.

3) Opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest dostawa niżej wymienionego sprzętu, oprogramowania oraz usług związanych z rozbudową i rozwojem infrastruktury sieciowej oraz IT Narodowego Centrum Promieniowania Synchrotronowego SOLARIS w następujących częściach:

Część 1:

1.1 System Monitorowania i Analizy Ruchu Sieciowego – szt. 1
1.2 System Kontroli Domeny (wraz z szkoleniem w formie Vouchera) – szt. 1
1.3 Upgrade oprogramowania Extreme Networks NetSight ver. NMS-BASE-50 do ver. NMS-ADV-100 – szt. 1
1.4 System bezpieczeństwa (wraz ze szkoleniem) – szt. 1
1.5 Usługa konsultacji wdrożenia normy ISO 27001 wraz ze szkoleniem– szt. 1
1.6 Macierz Dyskowa NAS (7x 2TB SATA) – szt. 1
1.7 Macierz Dyskowa NAS (12 x 1TB SSD) – szt. 1.

Część 2:

Wsparcie Gwarancyjne dla przełącznika Extreme Networks BD 8900 (3 lata od dnia 19.08.2018) – szt. 1.

2. Szczegółowy opis przedmiotu zamówienia zawiera Załącznik 1 do niniejszego Zaproszenia.
3. Wykonawca musi zapewnić realizację zamówienia w terminie:
   3.1 W **części 1** do 12 miesięcy od dnia zawarcia Umowy, w tym:- dostawa urządzeń i oprogramowania (w tym vouchera na szkolenie dotyczące systemu kontroli domeny) w terminie 2 miesięcy od podpisania umowy,
   - usługa konsultacji wdrożenia normy ISO 27001 wraz z pozostałymi szkoleniami w terminie 12 miesięcy od podpisania umowy.

   3.2 W **części 2** - w terminie od 1 stycznia 2018 r. do 30 czerwca 2018 r.

4. Szczegółowe warunki i terminy realizacji Umowy zawiera wzór Umowy poniżej.
5. Wykonawca musi zaoferować przedmiot Umowy objęty gwarancją jak w opisie przedmiotu zamówienia.
6. Wykonawca powinien przedstawić cenę ryczałtową oferty za przedmiot Umowy w formie indywidualnej kalkulacji, przy uwzględnieniu wymagań i zapisów Zaproszenia. Wykonawca zobowiązany jest przedstawić w ofercie lub w formie załącznika ceny jednostkowe poszczególnych elementów przedmiotu zamówienia.
7. Wykonawca musi zaoferować przedmiot zamówienia zgodny z wszystkimi wymogami Zamawiającego określonymi w Zaproszeniu.
8. Wykonawca powinien podpisać oraz wypełnić formularz oferty wraz z załącznikiem nr 1 do formularza oferty lub złożyć ofertę odpowiadającą jego treści, przy czym może podpisać oraz dołączyć do oferty wzór Umowy, stanowiące integralną część Zaproszenia.
9. Oznaczenie przedmiotu zamówienia według kodu Wspólnego Słownika Zamówień CPV: 48820000-2 (serwery), 48000000-8 pakiety oprogramowania i systemy informatyczne, 72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia, 48823000-3 Serwery plików, 32410000-0 lokalna sieć komputerowa, 32413100-2 rutery sieciowe.

4) Opis warunków podmiotowych udziału w postępowaniu:

1. Zamawiający wymaga aby Wykonawcy składając ofertę w zakresie części 1 posiadali niezbędną wiedzę i doświadczenie, tzn.: w okresie ostatnich 3 lat przed upływem terminu składania ofert o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy –w tym okresie – wykonali:

1.1 Dwie dostawy urządzeń sieciowych oraz rozwiązań z zakresu bezpieczeństwa, o porównywalnych parametrach technicznych jak w niniejszym zaproszeniu dotyczących Systemu Monitorowania i Analizy Ruchu Sieciowego, Systemu Kontroli Domeny oraz Systemu bezpieczeństwa sieci, na łączną kwotę min. 600 000 zł brutto. Wykonawca musi udokumentować, że wyżej wymienione dostawy wykonał należycie załączając dokumenty potwierdzające ich należytą realizację, a w wykazie podać ich wartość, przedmiot (zakres, rodzaj), datę(y) wykonania i odbiorcę(ów). Ocena spełnienia warunku będzie dokonywana metodą 0 – 1, tj. nie spełnia/spełnia, w oparciu o wykaz głównych dostaw, dokumenty i oświadczenia dołączone do oferty, których wzór stanowi Załącznik nr 2 do formularza oferty będącego integralną częścią Zaproszenia.

5) Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Dopuszcza się możliwość porozumiewania się w formie pisemnej lub drogą elektroniczną.
2. Zaleca się porozumiewanie drogą elektroniczną na adres poczty email jerzy.wordliczek@uj.edu.pl
3. Jeżeli Zamawiający lub Wykonawca przekazują jakiekolwiek dokumenty lub informacje drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
4. Przed złożeniem ofert Wykonawcy mogą przesyłać Zamawiającemu uwagi, co do treści niniejszego Zaproszenia. W uzasadnionych przypadkach Zamawiający uwzględniając przesłane uwagi może dokonać zmiany treści niniejszego Zaproszenia oraz odpowiednio wydłużyć termin składania ofert.
5. Do porozumiewania się z Wykonawcami upoważniony jest:
   5.1 w zakresie formalnym i merytorycznym – Jerzy Wordliczek, tel. +4812 663-10-66; faks + +4812-663-39-14;
   5.2 e-mail: jerzy.wordliczek@uj.edu.pl
   5.3 strona internetowa: www.uj.edu.pl
   5.4 miejsce publikacji ogłoszeń i informacji: http://zamowienia.uj.edu.pl/ogloszenia.php

5) Opis sposobu przygotowywania ofert.

1. Każdy Wykonawca może złożyć tylko jedną ofertę (według wzoru zamieszczonego poniżej, tj formularz oferty wraz z załącznikiem), która musi obejmować całość oferowanego przedmiotu zamówienia i winien skalkulować cenę ryczałtową dla całości przedmiotu zamówienia.
2. Wykonawca musi do oferty dołączyć opis techniczny i/lub funkcjonalny bądź katalog/i (prospekt/y) producenta/ów (wskazujące w szczególności oferowany typ, rodzaj, model, producenta, numer katalogowy, charakterystykę produktu i inne istotne parametry), wraz z wymaganymi certyfikatami, atestami, świadectwami, deklaracjami itp., pozwalające na ocenę zgodności oferowanych urządzeń oraz ich parametrów z wymaganiami Z (dopuszcza się dołączenie opisów w języku angielskim).
3. Wykonawca zobowiązany jest przedłożyć do oferty pełnomocnictwo w przypadku podpisania jej przez pełnomocnika.
4. Oferta musi być podpisana i napisana w języku polskim i złożona powinna być w formie pisemnej lub pocztą elektroniczną na adres wskazany w Zaproszeniu.
5. Zaleca się, aby wszystkie strony oferty wraz z załącznikami były podpisane przez osobę (osoby) uprawnione do składania oświadczeń woli w imieniu Wykonawcy.
6. Podmiot zainteresowany może zastrzec najpóźniej do dnia zawarcia Umowy w sprawie zamówienia z dziedziny nauki, iż informacje związane z tym zamówieniem stanowiące tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t. j. Dz. U. 2003 Nr 153 poz. 1503 z późń. zm.) nie mogą być udostępnione.
7. Rozliczenia pomiędzy Wykonawcą a Zamawiającym będą dokonywane w złotych polskich (PLN).
8. Wszelkie koszty związane z przygotowaniem i złożeniem oferty ponosi Wykonawca.
9. Składając ofertę Wykonawca oświadcza, iż wykona przedmiot zamówienia zgodnie z wszystkimi wymaganiami Zamawiającego opisanymi w niniejszym zaproszeniu wraz z załącznikami.

6) Miejsce oraz sposób, jak i termin składania i otwarcia ofert.

1. Oferty należy składać w Dziale Zamówień Publicznych Uniwersytetu Jagiellońskiego, przy ul. Straszewskiego 25/2, 31-113 Kraków, **w terminie do dnia 10 lipca 2017 r. do godziny 10:00,** w formie pisemnej lub pocztą elektroniczną na adres bzp@uj.edu.pl z oznaczeniem pozwalającym na identyfikację Wykonawcy oraz wskazaniem przedmiotu i numeru postępowania poprzez oznaczenie ***„Oferta w zakresie dostawy infrastruktury IT dla Narodowego Centrum Promieniowania Synchrotronowego Solaris, nr sprawy 80.272.148.2017 w zakresie części ….***”.
2. Ogłoszenie informacji o złożonych ofertach i zaoferowanych cenach oraz innych istotnych elementach złożonych ofert jest jawne i nastąpi w dniu **10 lipca 2017 r. do godzinie 10:05, w** Dziale Zamówień Publicznych UJ, przy ul. Straszewskiego 25/2, 31-113 Kraków.

7) Opis sposobu obliczenia ceny.

1. Cenę ryczałtową oferty należy podać w złotych polskich (PLN) i wyliczyć na podstawie indywidualnej kalkulacji Wykonawcy, uwzględniając doświadczenie i wiedzę zawodową Wykonawcy, jak i wszelkie koszty niezbędne do wykonania przedmiotu zamówienia (m.in. pakowanie, transport, ubezpieczenie, montaż, uruchomienie, przetestowanie, szkolenie pracowników i inne), podatki, koszty gwarancyjne w miejscu dostawy oraz rabaty, upusty itp., których Wykonawca zamierza udzielić. Wykonawca zobowiązany jest przedstawić w ofercie lub w formie załącznika ceny jednostkowe poszczególnych elementów przedmiotu zamówienia.
2. Sumaryczna cena ryczałtowa wyliczona na podstawie indywidualnej kalkulacji Wykonawcy winna odpowiadać cenie podanej przez Wykonawcę w formularzu oferty.
3. Zamawiający dla potrzeb oceny i porównania ofert w przypadku ofert Wykonawców skutkujących powstaniem obowiązku podatkowego po stronie Zamawiającego, zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. 2017 poz.

1221.), doliczy do przedstawionych cen podatek od towarów i usług VAT. Dotyczy wewnątrz wspólnotowego nabycia towarów ***(art. 17 ust. 1 pkt 3 ustawy o podatku VAT)***, importu towarów ***(art. 17 ust. 1 pkt 1 ustawy o podatku VAT)*** bądź importu usług ***(art. 17 ust. 1 pkt 4 ustawy o podatku VAT)*** w przypadku Wykonawców spoza terytorium RP oraz dostawy towarów wskazanych w Załączniku nr 11 do ustawy o podatku o VAT, do którego stosuje się tzw. mechanizm odwrotnego obciążenia VAT w przypadku Wykonawców krajowych ***(art. 17 ust. 1 pkt 7 ustawy o podatku VAT)***. W przypadku zawarcia Umowy obejmującej transakcję (zamówienie), do których znajdzie zastosowanie tzw. mechanizm odwrotnego obciążenia VAT, Wykonawca ma obowiązek umieścić na wystawianej przez niego fakturze stosowną adnotację „odwrotne obciążenie VAT" (art. 106e ust. 1 pkt 18 ww. ustawy).

4. Nie przewiduje się waloryzacji ceny, przy czym wyliczona cena będzie ceną ryczałtową za całość przedmiotu zamówienia.
5. Nie przewiduje się żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu zamówienia, a płatność nastąpi zgodnie z zapisem Umowy.

8) Opis czynności i kryteriów, którymi Zamawiający będzie się kierował przy wyborze najkorzystniejszej oferty.

1. Zamawiający wybiera najkorzystniejszą ofertę, spośród ważnych ofert złożonych w postępowaniu, biorąc przy ocenie i porównaniu złożonych ofert pod uwagę cenę brutto przedmiotu zamówienia.
1. Kryteria oceny ofert i ich znaczenie:

1.1 Cena ryczałtowa brutto za całość zamówienia – 100%

2. Punkty przyznawane za kryterium „cena ryczałtowa za całość zamówienia" będą liczone wg następującego wzoru:

$$C = (C_{naj} : C_o) \times 10$$

gdzie:
C – liczba punktów przyznana danej ofercie,
C_{naj} – najniższa cena spośród ważnych ofert,
C_o – cena podana przez Wykonawcę dla którego wynik jest obliczany.
Maksymalna liczba punktów, które Wykonawca może uzyskać , wynosi 10.

3. Wszystkie obliczenia punktów będą dokonywane z dokładnością do dwóch miejsc po przecinku (bez zaokrągleń).
4. Oferta Wykonawcy, która uzyska najwyższą liczbą punktów, uznana zostanie za najkorzystniejszą.
5. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert, jak również negocjować treść i ceny ofert z zachowaniem zasad przejrzystości oraz uczciwego traktowania Wykonawców.
6. Zamawiający poprawi w tekście oferty oczywiste omyłki pisarskie i oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek oraz inne omyłki polegające na niezgodności oferty z wymaganiami Zaproszenia, niepowodujące istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
7. Zamawiający może odrzucić ofertę, w szczególności, jeżeli została złożona po upływie terminu składania ofert lub jest niezgodna z wymaganiami Zaproszenia, bądź zaistnieją inne uzasadnione okoliczności powodujące, iż jest ona niezgodna z obowiązującymi przepisami.
8. Zamawiający odrzuci ofertę złożoną przez:
   – wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   a) którym mowa w art. 165a, art. 181-188, art. 189a, art. 218-221, art. 228-230a, art. 250a, art. 258 lub art. 270-309 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. poz. 553, z późn. zm.) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2016 r. poz. 176),
   b) charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,
   c) skarbowe,

d) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769);

- wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa powyżej;
- wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba, że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
- wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
- wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2015 r. poz. 1212, 1844 i 1855 oraz z 2016 r. poz. 437 i 544);
- wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;
- wykonawcę 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 2015 r., poz. 978 z późn. 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 (t.j. Dz. U. z 2015 r. poz. 233 z późn. zm.),
- wykonawcę, 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,
- wykonawcę, 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 ustawy PZP, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania,
- wykonawcę, który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w art. 24 ust. 1 pkt 15 ustawy PZP, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

9. Zamawiający unieważnia postępowanie o udzielenie zamówienia w szczególności, jeżeli nie zostanie złożona żadna oferta, lub wszystkie złożone oferty zostaną odrzucone, albo cena najkorzystniejszej oferty przekracza kwotę, którą Zamawiający może przeznaczyć na sfinansowanie zamówienia, bądź zaistnieją inne uzasadnione okoliczności skutkujące nieważnością Umowy w sprawie zamówienia z dziedziny nauki.
10. Zamawiający zawiadamia równocześnie wszystkich Wykonawców, którzy złożyli oferty, o rozstrzygnięciu postępowania, podając uzasadnienie faktyczne.

9) Informację o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia Umowy.

1. Zamawiający zamieszcza niezwłocznie na swojej stronie Biuletynu Informacji Publicznej informację o udzieleniu zamówienia, podając nazwę (firmę) albo imię i nazwisko podmiotu, z którym zawarł umowę o wykonanie zamówienia, albo informację o nieudzieleniu tego zamówienia.

10) Wzór Umowy.

UMOWA

zawarta w Krakowie w dniu …..... 2017 r. pomiędzy:

Uniwersytetem Jagiellońskim
z siedzibą przy ul. Gołębiej 24, 31-007 Kraków, NIP 675-000-22-36,
zwanym dalej „Zamawiającym", reprezentowanym przez:

1. ……. – ……. UJ, przy kontrasygnacie finansowej Kwestora UJ,

a ……,
, zwanym dalej „Wykonawcą", reprezentowanym przez:
1. ……..

W wyniku przeprowadzenia postępowania w trybie procedury zaproszenia do złożenia ofert w oparciu o art. 4d ust. 1 pkt. 1 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2015 r., poz. 2164 z późn. zm.) oraz art. 30a – 30d ustawy z dnia 30 kwietnia 2010r. o zasadach finansowania nauki (t.j. z Dz. U. z 2014 r., poz. 1620 z późn. zm.) oraz ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t. j. Dz. U. 2017 poz. 459 z późn zm.) zawarto Umowę następującej treści:

§ 1

1. Przedmiotem niniejszej umowy jest dostawa niżej wymienionego sprzętu, oprogramowania oraz usług związanych z rozbudowa i rozwojem infrastruktury sieciowej oraz IT Narodowego Centrum Promieniowania Synchrotronowego SOLARIS:
   1.1 ……..
   1.2 …….
   Szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1 do zaproszenia do złożenia ofert z dnia …… (zwanego dalej Zaproszeniem) oraz w ofercie Wykonawcy.
2. Przedmiot umowy zostanie dostarczony w formule Delivered At Place – DAP Kraków, do budynku synchrotronu SOLARIS, ul. Czerwone Maki 98 Kraków 30-392, zgodnie z regulacjami Incoterms 2010 i obejmuje również jego wniesienie do wskazanego pomieszczenia. Osobą odpowiedzialną za odbiór urządzeń i nadzór ze strony Zamawiającego jest Pan ……., lub inna osoba wskazana przez Zamawiającego.
3. Wykonawca zobowiązuje się wykonać wszelkie niezbędne czynności dla zrealizowania przedmiotu umowy określonego w ust. 1.
4. Wykonawca oświadcza, iż przedmiot umowy (w szczególności składające się na niego urządzenia i elementy) jest fabrycznie nowy, jego zakup i korzystanie z niego zgodnie z przeznaczaniem nie narusza prawa, w tym również praw osób trzecich oraz odpowiada normie CE w zakresie bezpieczeństwa urządzeń elektrycznych.
5. Integralną częścią niniejszej umowy jest Zaproszenie wraz z załącznikami i oferta Wykonawcy.
6. Wykonawca zobowiązuje się zrealizować całość przedmiotu umowy w terminie do ….. miesięcy od dnia zawarcia Umowy, w tym:
   ……..[1]
7. Wykonawca ponosi całkowitą odpowiedzialność materialną i prawną za powstałe u Zamawiającego, jak i osób trzecich, szkody spowodowane działalnością wynikłą z realizacji niniejszej umowy.

[1] *zgodnie z wymaganiami Zaproszenia odpowiednio dla każdej z części*

8. Zlecenie wykonania części umowy podwykonawcom nie zmienia zobowiązań Wykonawcy wobec Zamawiającego za wykonanie tej części umowy. Wykonawca jest odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i ich pracowników w takim samym stopniu, jakby to były działania, uchybienia lub zaniedbania własne.
9. Wraz z dostawą Wykonawca zobowiązany jest przekazać następujące dokumenty:
   a) - Wykaz ilościowo - rodzajowy przekazywanych urządzeń, zawierający w szczególności: nazwę własną urządzenia, wytwórcę, rok produkcji, nr fabryczny, charakterystyczne parametry użytkowe,
   b) - Karty gwarancyjne urządzeń, instrukcje obsługi i eksploatacji w języku polskim lub angielskim,
   c) - Atesty, certyfikaty, deklaracje zgodności, i inne dokumenty wymagane zgodnie z treścią Zaproszenia.
10. Dostawę uznaje się za zakończoną po przeprowadzeniu kontroli zgodności dostarczonego przedmiotu umowy z wymaganiami Zamawiającego określonymi w ZAPROSZENIU oraz z ofertą Wykonawcy, potwierdzonej protokołem odbioru bez zastrzeżeń podpisanym przez Zamawiającego. Wykonawca zobowiązany jest wstępnie uruchomić przedmiot umowy po jego dostawie, tj. w szczególności:
    a) Rozpakować przedmiot umowy we wskazanym pomieszczeniu po jego dostawie.
    b) Dokonać instalacji dostarczonych urządzeń.
    c) Wykazać, że wszystkie dostarczone elementy przedmiotu umowy są sprawne technicznie i są kompatybilne z zainstalowanymi urządzeniami w Narodowym Centrum Promieniowania Synchrotronowego SOLARIS.
11. Zamawiający zastrzega sobie prawo odmowy podpisania protokołu odbioru w przypadku, gdy przedmiot umowy będzie niekompletny, uszkodzony lub też nie będzie odpowiadał parametrom określonym w ZAPROSZENIU i umowie.

§ 2

1. Wykonawca oświadcza, że posiada odpowiednią wiedzę, doświadczenie i dysponuje stosowną bazą do wykonania przedmiotu umowy.
2. Wykonawca oświadcza, iż przedmiot umowy wykona z zachowaniem wysokiej, jakości użytych materiałów oraz dotrzyma umówionych terminów przy zachowaniu należytej staranności uwzględniając zawodowy charakter prowadzonej przez niego działalności.
3. W ramach niniejszej umowy i wynikającego z niej wynagrodzenia Wykonawcy, wskazanego w § 3 ust. 2 umowy, Zamawiający nabywa nieodwołalne i nieograniczone czasowo prawo do korzystania ze wszelkiego oprogramowania niezbędnego do prawidłowego funkcjonowania przedmiotu umowy w zakresie wskazanym w art. 75 ust. 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. 2016 poz. 666 z późń. zm.), to jest na następujących polach eksploatacji:
   a. sporządzenie kopii zapasowej, jeżeli jest to niezbędne do korzystania z programu komputerowego. Jeżeli umowa nie stanowi inaczej, kopia ta nie może być używana równocześnie z programem komputerowym;
   b. obserwowanie, badanie i testowanie funkcjonowania programu komputerowego w celu poznania jego idei i zasad przez osobę posiadającą prawo korzystania z egzemplarza programu komputerowego, jeżeli, będąc do tych czynności upoważniona, dokonuje ona tego w trakcie wprowadzania, wyświetlania, stosowania, przekazywania lub przechowywania programu komputerowego;
   c. zwielokrotnianie kodu lub tłumaczenie jego formy w rozumieniu art. 74 ust. 4 pkt 1 i 2 ww. ustawy, jeżeli jest to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego z innymi programami komputerowymi, o ile zostaną spełnione następujące warunki:
      ca) czynności te dokonywane są przez Zamawiającego lub inną osobę uprawnioną do korzystania z egzemplarza programu komputerowego bądź przez inną osobę działającą na ich rzecz,
      cb) informacje niezbędne do osiągnięcia współdziałania nie były uprzednio łatwo dostępne dla osób, o których mowa pod lit. ca),

cc) czynności te odnoszą się do tych części oryginalnego programu komputerowego, które są niezbędne do osiągnięcia współdziałania.

4. Wykonawca udziela licencji niewyłącznej, tj. prawa do korzystania z oprogramowania w zakresie wskazanym w ust. 3 niniejszego paragrafu umowy, w chwili podpisania protokołu odbioru wskazanego w § 4 ust. 2 umowy, bez zastrzeżeń oraz zapłaty wynagrodzenia, o którym mowa w § 3 ust. 2 umowy, bez konieczności składania przez Strony dodatkowego oświadczenia woli.

§ 3

1. Wysokość wynagrodzenia przysługującego Wykonawcy za wykonanie przedmiotu umowy ustalona została na podstawie oferty Wykonawcy.
2. **Wynagrodzenie ryczałtowe za przedmiot umowy ustala się na kwotę netto: …….. zł., słownie : …… zł. 00/100, co po doliczeniu należnej stawki podatku VAT 23% daje kwotę brutto: ……zł., słownie : …….. (w ……..)**
3. Zamawiający jest płatnikiem VAT i posiada NIP PL 675-000-22-36.
4. Wykonawca jest płatnikiem VAT i posiada NIP ……..
5. Zamawiający oświadcza, iż zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. 2016 710 z późn. zm.) będzie ubiegał się o zgodę na zastosowanie 0% stawki podatku od towarów i usług VAT na zamawiany sprzęt komputerowy w zakresie objętym zwolnieniem – zgodnie z art. 83 ust. 1 pkt 26 przywołanej ustawy.
6. Należny od kwoty wynagrodzenia podatek od towarów i usług VAT, pokryje Zamawiający na konto właściwego Urzędu Skarbowego w przypadku powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.

§ 4

1. Wykonawca otrzyma wynagrodzenie po wykonaniu całości przedmiotu umowy, potwierdzonego protokołem odbioru bez zastrzeżeń i po złożeniu prawidłowo wystawionej faktury w siedzibie jednostki organizacyjnej wskazanej w § 1 ust. 2 umowy.
2. Wykonawca zobowiązany jest odrębnie zafakturować usługę konsultacji wdrożenia normy ISO 27001.
3. Protokół odbioru zostanie podpisany przez Zamawiającego po uprzednim sprawdzeniu przez upoważnionego pracownika Zamawiającego prawidłowości realizacji zamówienia pod względem zgodności z niniejszą umową. Zamawiający zastrzega sobie prawo odmowy podpisania protokołu odbioru w przypadku, gdy przedmiot umowy będzie niekompletny, uszkodzony lub też nie będzie odpowiadał parametrom technicznym, określonym w Zaproszeniu i umowie.
4. Termin zapłaty faktury za wykonany i odebrany przedmiot umowy ustala się do 30 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury.
5. Wynagrodzenie przysługujące Wykonawcy jest płatne przelewem z rachunku Zamawiającego, na konto Wykonawcy wskazane na fakturze.
6. Miejscem płatności jest Bank Zamawiającego.

§ 5

1. Wykonawca zobowiązuje się wykonać przedmiot umowy bez usterek.
2. Wykonawca udziela gwarancji zgodnej z Zaproszeniem na dostarczony przedmiot umowy liczonej od daty odbioru całości przedmiotu umowy, z uwzględnieniem zapisów dotyczących warunków gwarancyjnych wynikających z ZAPROSZENIA, wraz z bieżącą konserwacją wynikającą z warunków gwarancji i naprawą w okresie gwarancyjnym w miejscu użytkowania. Uprawnienia z tytułu rękojmi, której okres wynosi 24 miesiące, nie zostają wyłączone.
3. Gwarancja będzie świadczona przez producenta lub autoryzowany przez niego serwis lub osoby na koszt Wykonawcy w siedzibie Zamawiającego, a jeżeli jest to technicznie

niemożliwe to wszelkie działania organizacyjne i koszty związane ze świadczeniem usługi gwarancyjnej poza siedzibą Zamawiającego ponosi Wykonawca.

4. Gwarancja ulega automatycznie przedłużeniu o okres naprawy, tj. czas liczony od zgłoszenia do usunięcia awarii czy usterki.
5. Jeżeli z jakiegokolwiek powodu leżącego po stronie Wykonawcy nie usunie on wady (usterki) w wyznaczonym terminie, Zamawiający ma prawo zaangażować inny podmiot do usunięcia wad (usterek), a Wykonawca zobowiązany jest pokryć związane z tym koszty w ciągu 14 dni od daty otrzymania wezwania wraz z dowodem zapłaty.
6. Przy odbiorze Wykonawca zobowiązany jest dołączyć dokumenty gwarancyjne i instrukcje obsługi i eksploatacji.
7. Zamawiający zobowiązuje się dotrzymywać warunków eksploatacji określonych w zapisach kart gwarancyjnych dostarczonych przez Wykonawcę.

§ 6

1. Strony zastrzegają sobie prawo do dochodzenia kar umownych za niezgodne z niniejszą umową lub nienależyte wykonanie zobowiązań z umowy wynikających.
2. Wykonawca zapłaci Zamawiającemu karę umowną w przypadku:
   a) odstąpienia od umowy przez zamawiającego lub Wykonawcę wskutek okoliczności leżących po stronie Wykonawcy w wysokości 10% wynagrodzenia brutto, o którym w **§** 3 ust.2,
   b) zwłoki większej niż 5 dni w wykonaniu przedmiotu umowy w wysokości 0,2% wynagrodzenia brutto, o którym w **§** 3 ust.2 za każdy dzień zwłoki, jednak nie więcej niż 10% wynagrodzenia brutto ustalonego w § 3 ust. 2 umowy,
   c) zwłoki w usunięciu wad przedmiotu umowy w wysokości 0,2% wynagrodzenia brutto, o którym w **§** 3 ust.2 za każdy dzień zwłoki, licząc od następnego dnia po upływie terminu określonego przez Strony w celu usunięcia wad, jednak nie więcej niż 10% wynagrodzenia brutto ustalonego w § 3 ust. 2 umowy,.
3. Zamawiający zastrzega sobie prawo potrącenia ewentualnych kar umownych z należnej faktury oraz dochodzenia odszkodowania na zasadach ogólnych ponad zastrzeżone kary umowne.
4. Roszczenie o zapłatę kar umownych staje się wymagalne z dniem zaistnienia określonych w niniejszej umowie podstaw do ich naliczenia.
5. Jeżeli kara nie pokrywa poniesionej szkody, Strony mogą dochodzić odszkodowania uzupełniającego.
6. Wykonawcy nie przysługuje odszkodowanie za odstąpienie Zamawiającego od umowy z winy Wykonawcy.
7. W przypadku odstąpienia od umowy Strony zachowują prawo egzekucji kar umownych.

§ 7

1. Oprócz przypadków wymienionych w Kodeksie cywilnym Zamawiającemu przysługuje prawo odstąpienia od niniejszej umowy, nie później niż w ciągu 21 dni od dnia powzięcia wiadomości o zaistnieniu niżej wymienionych okoliczności:
   a) zostanie podjęta likwidacja Wykonawcy,
   b) został wydany nakaz zajęcia majątku Wykonawcy
   c) opóźnienia Wykonawcy w dostawie przedmiotu umowy w stosunku do terminu określonego w § 1 ust. 6 przekraczającego 15 dni kalendarzowych.
   d) Wykonawca dostarczył sprzęt nie odpowiadający warunkom umowy i w dodatkowym, wyznaczonym przez Zamawiającego terminie nie dłuższym niż 5 dni, nie wykonał umowy zgodnie z jej zapisami.
   e) wystąpienia u Wykonawcy dużych trudności finansowych, w szczególności wystąpienie zajęć komorniczych lub innych zajęć uprawnionych organów o łącznej wartości przekraczającej 200 000,00 PLN (słownie: dwieście tysięcy złotych),
2. Odstąpienie od umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.
3. W przypadku odstąpienia od umowy Strony, zachowują prawo egzekucji kar umownych.

4. Zamawiający zastrzega sobie prawo do odstąpienia od umowy tylko w zakresie wskazanej przez niego części przedmiotu umowy, zatrzymując prawo własności pozostałej/pozostałych części przedmiotu umowy. W zakresie w którym Zamawiający nie skorzystał z prawa do odstąpienia, wszystkie zapisy umowy, w szczególności dotyczące płatności oraz gwarancji, pozostają w mocy.

§ 8

1. Przez okoliczności siły wyższej strony rozumieją zdarzenie zewnętrzne o charakterze nadzwyczajnym, którego nie można było przewidzieć ani jemu zapobiec, w szczególności takie jak: pożar, powódź, wojna, stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.
2. Jeżeli wskutek okoliczności siły wyższej Strona nie będzie mogła wykonywać swoich obowiązków umownych w całości lub w części, niezwłocznie powiadomi o tym drugą stronę. W takim przypadku Strony uzgodnią sposób i zasady dalszego wykonywania umowy lub umowa zostanie rozwiązana.

§ 9

1. Wszelkie oświadczenia Stron umowy będą składane na piśmie pod rygorem nieważności listem poleconym lub za potwierdzeniem ich złożenia.
2. Wszelkie doręczenia winny być dokonywane na poniższe adresy Stron:
   a) Uniwersytet Jagielloński – Narodowe Centrum Promieniowania Synchrotronowego SOLARIS
      ul. Czerwone Maki 98, 30-392 Kraków
      oraz
   b) …….
3. Ewentualna nieważność jednego lub kilku postanowień niniejszej umowy nie wpływa na ważność umowy w całości, a w takim przypadku Strony zastępują nieważne postanowienie postanowieniem zgodnym z celem i innymi postanowieniami umowy.

§ 10

1. Strony dopuszczają możliwość zmiany umowy po uprzednim sporządzeniu protokołu konieczności, przy zachowaniu ceny umowy, oprócz przypadków wskazanych poniżej a dotyczących możliwości zmiany wynagrodzenia, poprzez podpisanie aneksu do umowy, w następujących przypadkach:
   a) zmiany terminu realizacji przedmiotu umowy, poprzez jego skrócenie w przypadku zgodnej woli Stron, lub poprzez jego przedłużenie ze względu na przyczyny leżące po stronie Zamawiającego dotyczące w szczególności braku przygotowania/przekazania miejsca realizacji/dostawy, oraz inne niezawinione przez Strony przyczyny spowodowane przez siłę wyższą w rozumieniu § 8,
   b) poprawy jakości lub innych parametrów charakterystycznych dla danego elementu przedmiotu umowy lub zmiany technologii na równoważną lub lepszą, podniesienia wydajności urządzeń oraz bezpieczeństwa, w sytuacji wycofania z rynku przez producenta lub zakończenia produkcji zaoferowanego przez Wykonawcę przedmiotu umowy bądź jego elementów,
   c) aktualizacji rozwiązań z uwagi na postęp technologiczny lub zmiany obowiązujących przepisów,
   d) zmiany podwykonawcy ze względów losowych lub innych korzystnych dla Zamawiającego, w przypadku zadeklarowania przez Wykonawcę realizacji zamówienia przy pomocy podwykonawców,
   e) ustawowej zmiany stawki podatku od towarów i usług VAT do poszczególnych wykonanych części umowy, które zostały zrealizowane po dniu wejścia w życie przepisów dokonujących zmiany stawki podatku VAT
   f) ustawowej zmiany wysokości minimalnego wynagrodzenia za pracę ustalonego na podstawie art. 2 ust. 3 – 5 ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (t. j. Dz. U. 2017 poz. 847 z późn. zm.) wpływającej na wysokość miesięcznego wynagrodzenia Wykonawcy, którego wypłata nastąpiła po dniu

wejścia w życie przepisów dokonujących zmiany wysokości minimalnego wynagrodzeniu za pracę,

g) ustawowej zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne ustalonych na podstawie przepisów ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t. j. Dz. U. 2016 poz. 963 z późn. zm.) oraz ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t. j. Dz. U. 2016 poz. 1973 z późn. zm.) wpływającej na wysokość miesięcznego wynagrodzenia Wykonawcy, którego wypłata nastąpiła po dniu wejścia w życie przepisów dokonujących zmian ww. zasad lub wysokości stawek składek.

2. W przypadkach określonych w ust. 1 lit. f) oraz g) Wykonawca, w terminie nie dłuższym niż 14 dni od dnia wejścia w życie nowych przepisów, może zwrócić się do Zamawiającego z wnioskiem o zmianę wynagrodzenia, jeżeli zmiany te będą miały wpływ na koszty wykonania przedmiotu umowy przez Wykonawcę. Zasadność wzrostu wynagrodzenia Wykonawcy z ww. przyczyn będzie rozpatrywana w poniżej opisanym trybie:
   a) Wykonawca wraz z wnioskiem, będzie zobowiązany pisemnie przedstawić Zamawiającemu szczegółową kalkulację uzasadniającą wzrost/obniżenie kosztów, wynikający ze zmiany w/w przepisów. Z uprawnienia tego może skorzystać również Zamawiający. Jeżeli po upływie 14 – dniowego terminu, Wykonawca nie zwróci się do Zamawiającego o zmianę wynagrodzenia, Zamawiający uzna, iż zmiany przepisów nie mają wpływu na koszty wykonania zamówienia przez Wykonawcę.
   b) Zamawiający dokona analizy przedłożonej kalkulacji w terminie nie dłuższym niż 14 dni od dnia jej otrzymania. W wyniku przeprowadzenia analizy Zamawiający jest uprawniony do:
      ba) Jeżeli uzna, że przedstawiona kalkulacja potwierdza wzrost kosztów ponoszonych przez Wykonawcę, dokona zmiany umowy w tym zakresie
      bb) Jeżeli uzna, że przedstawiona kalkulacja nie potwierdza wzrostu kosztów wykonania zamówienia, w wysokości zaproponowanej przez Wykonawcę, nie wyrazi zgody na wprowadzenie zmiany, o czym poinformuje Wykonawcę, przedstawiając stosowne uzasadnienie. W takiej sytuacji, w terminie 14 dni od dnia otrzymania odmowy od Zamawiającego, Wykonawca może ponownie przedstawić kalkulację uzasadniającą wzrost kosztów, z uwzględnieniem uwag Zamawiającego. Zamawiający ponownie dokona jej analizy, w terminie nie dłuższym niż 14 dni od dnia jej otrzymania, a następnie postąpi odpowiednio w sposób opisany powyżej.
3. Zmiana wynagrodzenia Wykonawcy wchodzi w życie z dniem zawarcia aneksu nastąpi od daty wprowadzenia zmiany w umowie i dotyczy wyłącznie niezrealizowanej części umowy.
4. Zmiany nie dotyczące postanowień umownych np. gdy z przyczyn organizacyjnych konieczna będzie zmiana danych teleadresowych określonych w umowie, gdy zmianie ulegnie numer konta bankowego jednej ze Stron nastąpią poprzez przekazanie pisemnego oświadczenie Strony, której te zmiany dotyczą, drugiej Stronie.

§ 11

1. Żadna ze Stron nie jest uprawniona do przeniesienia swoich praw i zobowiązań z tytułu niniejszej umowy bez uzyskania pisemnej zgody drugiej Strony, w szczególności Wykonawcy nie przysługuje prawo przenoszenia wierzytelności wynikających z niniejszej umowy bez uprzedniej pisemnej zgody Zamawiającego.
2. Wykonawca zobowiązany jest do uzyskania pisemnej zgody Zamawiającego na przeniesienie praw i obowiązków z niniejszej umowy także w przypadku zmiany formy prawnej Wykonawcy.
3. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy prawa polskiego, w szczególności z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (t. j. Dz. U. 2014 poz. 1620 z późn. zm.) oraz przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t. j. Dz. U. 2017 poz. 459 z późn. zm.).

4. Wszelkie zmiany lub uzupełnienia niniejszej umowy mogą nastąpić za zgodą Stron w formie pisemnego aneksu pod rygorem nieważności.
5. Sądem właściwym dla wszystkich spraw spornych, które wynikną z realizacji niniejszej umowy będzie sąd miejscowo właściwy dla siedziby Zamawiającego.
6. Niniejszą umowę sporządzono w dwóch (2) jednobrzmiących egzemplarzach po jednym (1) egzemplarzu dla każdej ze Stron.

....

Zamawiający *Wykonawca*

FORMULARZ OFERTY

ZAMAWIAJĄCY – **Uniwersytet Jagielloński**
ul. Gołębia 24, 31 – 007 Kraków;
Jednostka prowadząca sprawę – **Dział Zamówień Publicznych UJ**
ul. Straszewskiego 25/2, 31-113 Kraków

Nazwa (Firma) Wykonawcy –
…….,
Adres siedziby –
……,
Adres do korespondencji –
……,
Tel. - .....; faks - .....;
E-mail: .....;
NIP - .....; REGON - .....;

Nawiązując do ogłoszonego zaproszenia na wyłonienie Wykonawcy w zakresie dostawy infrastruktury IT dla Narodowego Centrum Promieniowania Synchrotronowego Solaris, składamy poniższą ofertę:

1) oferujemy wykonanie **części 1 przedmiotu zamówienia** za łączną kwotę netto .....PLN *, plus należny podatek VAT w wysokości ……..%*, co daje kwotę brutto .....PLN * (słownie : ……..…… PLN)
2) oferujemy wykonanie **części 2 przedmiotu zamówienia** za łączną kwotę netto .....PLN *, plus należny podatek VAT w wysokości ……..%*, co daje kwotę brutto .....PLN * (słownie : ……..…… PLN)
3) oferujemy termin realizacji przedmiotu Umowy zgodnie z wymaganiami zwartymi w Zaproszeniu do złożenia ofert.
4) oferujemy okres gwarancji i wsparcia serwisowego wynoszący: zgodnie z wymaganiami zwartymi w Zaproszeniu do złożenia ofert.
5) oferujemy termin płatności wynoszący do 30 dni liczony od doręczenia faktury, odpowiednio dla wymagań określonych w Zaproszeniu,
6) oświadczamy, że zapoznaliśmy się z treścią Zaproszenia do złożenia ofert, w szczególności zawartym w nim wzorem Umowy oraz opisem przedmiotu zamówienia wraz załącznikami i uznajemy się za związanych określonymi w niej wymaganiami i zasadami postępowania,
7) oświadczamy, że uważamy się za związanych niniejszą ofertą na okres 30 dni od daty jej otwarcia,
8) oświadczamy, iż oferujemy przedmiot zamówienia zgodny z wymaganiami i warunkami określonymi przez Zamawiającego w Zaproszeniu,
9) oferta liczy **.....*** kolejno ponumerowanych kart.

Uwaga! Miejsca wykropkowane i/lub oznaczone „*" we wzorze formularza oferty i wzorach jego załączników Wykonawca zobowiązany jest odpowiednio do ich treści wypełnić lub skreślić.

Miejscowość ..... dnia ..... 2017 roku.

.....
(pieczęć i podpis osoby uprawnionej do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik nr 1 do formularza oferty

(Pieczęć firmowa Wykonawcy)

OŚWIADCZENIE

Składając ofertę na wyłonienie Wykonawcy w zakresie dostawy infrastruktury IT dla Narodowego Centrum Promieniowania Synchrotronowego Solaris, nr sprawy 80.272.148.2017 w części… oświadczam, że nie zachodzą przesłanki opisane w punkcie 8)8. „Zaproszenia do składania ofert" skutkujące odrzuceniem oferty.

Miejscowość ..... dnia ..... 2017 roku.

.....
(pieczęć i podpis osoby uprawnionej do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik nr 2 do formularza ofert

(Pieczęć firmowa Wykonawcy)

OŚWIADCZENIE

Składając ofertę na *wyłonienie Wykonawcy w zakresie dostawy infrastruktury IT dla Narodowego Centrum Promieniowania Synchrotronowego Solaris, nr sprawy 80.272.148.2017 w części 1 postępowania* oświadczam że spełniam warunki udziału w postępowaniu określone przez zamawiającego w pkt. 4) Zaproszenia, w szczególności:

wykonałem następujące dostawy :

PRZEDMIOT ZAMÓWIENIA adres, wykonany zakres rzeczowy – zakres musi potwierdzać spełnianie warunku postawionego przez Zamawiającego	**Wartość zamówienia (brutto)**	**Termin realizacji od ÷ do**	**Zamawiający**	**Sposób realizacji** (zasób własny/podmiot trzeci - w przypadku udostepnienia podać nazwę podmiotu**)**
				□ jednego z Wykonawców występujących wspólnie □ innego podmiotu udostępniającego zasoby, tj. ……..
				□ jednego z Wykonawców występujących wspólnie □ innego podmiotu udostępniającego zasoby, tj. ……..

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Miejscowość ..... dnia ..... 2017 roku.

.....
(pieczęć i podpis osoby uprawnionej do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik Nr 1 do Zaproszenia - OPIS PRZEDMIOTU ZAMÓWIEENIA

Przedmiotem zamówienia jest rozbudowa infrastruktury IT, zakup urządzeń sieciowych, systemów bezpieczeństwa oraz odnowienie umów suportowych dla urządzeń sieciowych, serwerów oraz oprogramowania dla synchrotronu.

Część 1:

	Rodzaj urządzenia	**Specyfikacja**	**Ilość**
1	System Monitorowania i Analizy Ruchu Sieciowego	1. System musi obejmować minimum trzyletnie wsparcie producenta 2. System analizy ruchu sieciowego musi składać się z trzech komponentów: kolektora gromadzącego, przechowującego i analizującego pakiety NetFlow oraz IPFIX; sondy sprzętowej zbierającej kopię ruchu ze switchy (port mirroring) i na tej podstawie generującej pakiety NetFlow v5/v9 i IPFIX oraz rozwiązania Network Behavior Anomaly Detection (NBAD) 3. Urządzenie do zbierania i przechowywania statystyk flow musi być dostarczone w postaci maszyny wirtualnej na VMware oraz umożliwiać zbieranie danych z dowolnej liczby urządzeń (‘netflow sources’) z wydajnością minimum 100 tys flow/sec 4. Maszyna wirtualna będąca kolektorem IPFIX musi posiadać 2 interfejsy do zarządzania 10/100/1000 MbE, na których będzie odbierany Netflow z urządzeń zewnętrznych oraz 2 interfejsy monitorujące do podłączenia kopii ruchu typu 10/100/1000 MbE. 5. Sonda do zbierania ruchu ze switchy musi być dostarczona jako sprzętowy appliance o wysokości 1U. Urządzenie musi posiadać 2 interfejsy monitorujące SFP+ 10G, o wydajności min. 1,5M pakietów na sekundę. Urządzeniu musi być wyposażone w dysk o pojemności minimum 500GB. Dodatkowo musi posiadać dwa interfejsy sieciowe 10/100/1000Mb do zarządzania. 6. System musi udostępniać funkcję aktywnego tworzenia próbek ruchu z analizowanej kopii ruchu sieciowego. Musi istnieć możliwość aktywnego tworzenia próbek ruchu w formatach co najmniej Netflow wersji 5 i 9, IPFIX. System musi posiadać funkcję wysyłania aktywnie tworzonych próbek ruchu do systemu kolektora statystyk Netflow tego samego producenta. 7. System musi wykrywać nowe hosty pojawiające się w sieci teleinformatycznej. 8. System musi zbierać i przechowywać informacje o MAC adresach komputerów oraz o przypisanych do nich adresów IPv4 i IPv6. 9. System musi utrzymywać centralne repozytorium informacji o analizowanym ruchu sieciowym otrzymywanych z innych urządzeń sieciowych lub własnych komponentów. 10. System musi udostępniać graficzny interfejs użytkownika do przetwarzania zebranych danych, w tym wyliczania statystyk i generowania raportów. Statystyki i raporty muszą być dostępne na bieżąco w czasie rzeczywistym. 11. System kolekcjonowania danych musi przechowywać informacje o czasie rozpoczęcia i zakończenia strumienia analizowanych danych z dokładnością do 1 milisekundy. 12. System musi posiadać funkcje tworzenia profili i widoków analizowanych danych, aktualizowanych na bieżąco, na podstawie kryteriów zdefiniowanych przez	1

		administratora. 13. System musi generować raporty pokazujące dane w formie graficznej (wykresy) jak i tabelarycznej, w oparciu o kryteria wprowadzane przez użytkowników w formie filtrów. Raporty muszą obejmować również informacje o wszystkich konwersacjach pomiędzy monitorowanymi hostami. 14. System musi mieć możliwość wyświetlenia wszystkich hostname oraz url w zadanym przedziale czasu dla danego użytkownika, grupy użytkowników, sieci. 15. System musi pozwalać na wyświetlenie listy połączeń SIP, dając informacje o stronach biorących udział w połączeniu, pomiar wydajności oraz identyfikację ruchu powiązanego z danym połączeniem 16. System musi zbierać z kopii ruchu i udostępniać za pomocą protokołu IPFIX przynajmniej następujące informacje o sieci: • adresy i sieci IP (źródłowe i docelowe), • aplikacje (protokoły, porty źródłowe, docelowe oraz NBAR2), • kraje rozpoznawane na podstawie sieci IP (dla adresów źródłowych i docelowych) • ruch z określonymi flagami TCP, • protokoły IPv4 oraz IPv6, • system operacyjny i przeglądarkę hosta korzystającego z http, • hostname'y,URLe, method, result code • DHCP minimum: Offered IP,message type,IP address lease time, server domain name, dhcp-host name, requested IP • DNS minimum: DNS flags, question, response, • SAMBA: minimum dla SMB2: file name, file type, tree structure, operation type, • VoIP: call ID, SIP called party, SIP calling party, SIP VIA, SIP ringing time, SIP RTP IP, SIP RTP audio i video, packet type, RTP jitter,, RTP codec type, • Metryki RTT i SRT (min, max, średnie), opóźnienie, jitter, retransmisje • SMTP: nadawca email, błędy uwierzytelnienia • MSSQL: sql query, error code, response type • ARP 17. System musi posiadać możliwość raportowania obciążenia sieci przez: • użytkowników (adresy źródłowe, docelowe), • aplikacje (protokoły, porty źródłowe, docelowe), • klasy ruchu QoS (ToS/DSCP), • systemy autonomiczne (AS), • protokoły, • podsieci, • ruch z określonymi flagami TCP, • IPv4 oraz IPv6. 18. System musi generować raporty zgodnie z kryteriami ustalanymi przez administratorów oraz na podstawie predefiniowanych wzorców. Raporty muszą być tworzone w różnych formatach – minimum PDF i CSV. Użytkownik musi posiadać wpływ na układ raportu poprzez dobór ilości i rodzaju informacji, z których raport będzie się składał. 19. System musi posiadać funkcję automatycznego rozwiązywania adresów IP do nazw domenowych. 20. System musi posiadać funkcję nadawania nazw własnych następującym zaobserwowanym obiektom: • podsieciom,	

		• aplikacjom (adresom IP i portom), • systemom autonomicznym BGP (AS). 21. System musi udostępniać zbiorcze dane statystyczne zawierające sumaryczną liczbę otrzymanych eksportów próbek ruchu określonego typu zebranych przez każdy interfejs monitorujący, wraz z informacjami na temat średniej oraz szczytowej liczby otrzymywanych eksportów od każdego z urządzeń. 22. System musi pozwalać na definiowanie alarmów, które będą powiadamiać administratora o ruchu sieciowym (globalnym oraz z wybranych sieci, protokołów i aplikacji) przekraczającym zdefiniowane wartości progowe wyrażone w jednostkach ilości danych (pakietach oraz bajtach), a także w jednostkach prędkości transmisji (bitach/sekundę, pakietach/sekundę). 23. Alarmy muszą być wysyłane przy wykorzystaniu co najmniej następujących metod: syslog, e-mail, SNMP trap 24. System musi posiadać funkcję Network Behavior Anomaly Detection (NBAD) tego samego producenta 25. System wykrywania anomalii musi mieć możliwość zasilania poprzez syslog lub SNMP systemów typu SIEM 26. System NBAD musi mieć możliwość analizy statystyk do 4 kfps 27. System musi posiadać możliwość wykrywania ataków Denial of Service , Distributed Denial of Service i innych ataków sieciowych, takich jak ataki słownikowe na SSH, RDP, telnet oraz skanowanie portów 28. System NBAD musi wykrywać anomalie związane z ruchem DNS,DHCP, SMTP, multicast i nietypową komunikacją 29. Wykryte zdarzenia muszą być automatycznie agregowane w jeden typ zdarzeń – atak dostępowy, błędna konfiguracja, zainfekowane 30. System musi posiadać predefiniowane priorytety zdarzeń z opcją konfiguracji własnych priorytetów zdarzeń bazujących na zakresach adresów IP, lokalizacji, typie zdarzenia 31. System musi działać w architekturze zcentralizowanej – kluczowe funkcje, czyli zbieranie danych, analiza zdarzeń, raportowanie oraz wykrywanie anomalii muszą być wykonywane na tym samym urządzeniu 32. System musi posiadać możliwość wykrywania anomalii w działaniu sieci teleinformatycznej za pomocą analizy statystycznej i behawioralnej. W tym celu system musi na bieżąco budować profile normalnego stanu i zachowania sieci oraz identyfikować odchylenia od stanu normalnego – poprzez zaobserwowanie zwiększenia lub zmniejszenie natężenia ruchu sieciowego oraz przekraczanie zdefiniowanych wartości progowych 33. System detekcji anomalii musi mieć zaimplementowane mechanizmy maszynowego uczenia się 34. System do analizy anomalii musi wykonywać deduplikację analizowanych przepływów 35. System NBAD musi mieć możliwość próbkowania przepływów przyjmowanych do analizy 36. System NBAD musi wyświetlać informacje o użytkownikach jako element uzupełniający wykryte zdarzenia 37. System NBAD musi posiadać predefiniowane reguły i algorytmy używane do wykrywania nieprawidłowości w ruchu sieciowym 38. System NBAD musi dawać administratorowi możliwość dostosowania predefiniowanych reguł pod specyfikę własnej sieci jako zmiana parametrów wykorzystywanych przez reguły i algorytmy 39. System musi dać możliwość konfiguracji przez interfejs webowy false positives jako prostą regułę wykluczenia 40. System musi posiadać listę reputacyjną hostów dostarczaną przez producenta sytemu, aktualizowaną przynajmniej raz na 24h	

41. System musi być dostarczony jako rozwiązanie gotowe do użytku, pochodzące od tego samego producenta. Nie jest dopuszczalna sytuacja, w której funkcje wymagane dla systemu realizowane są przez zestaw programów pochodzących od różnych producentów, działających na tej samej platformie sprzętowej ogólnego przeznaczenia lub jak GNU open source.
42. System musi być kompletny tzn. zawierać wszystkie licencje i zezwolenia, niezbędne do poprawnego funkcjonowania zgodnie z niniejszą specyfikacją, bez konieczności wnoszenia dodatkowych opłat.
43. Pełne zarządzanie systemem, analiza danych oraz raportowanie musi odbywać się poprzez graficzny interfejs użytkownika dostępny za pomocą standardowych przeglądarek WWW. Nie jest dopuszczalne zarządzanie przy pomocy dodatkowych aplikacji klienckich.
44. System musi pozwalać na definiowanie kont administratorów o zróżnicowanym poziomie uprawnień w zakresie co najmniej: pełnej kontroli nad systemem, kontroli na poszczególnymi modułami funkcjonalnymi systemu, kont uprawnionych tylko do odczytu. Ponadto musi istnieć funkcja ograniczania uprawnień kont użytkowników do poszczególnych źródeł informacji tj. konkretnych aplikacji, podsieci, grupy urządzeń (danych definiowanych na podstawie kryteriów z warstwy 3 i 4 modelu OSI). Tożsamość administratorów musi być weryfikowana w lokalnej bazie danych użytkowników, a także przy pomocy zewnętrznych serwerów uwierzytelniania – co najmniej LDAP, TACACS+.
45. System musi posiadać możliwość nadawania uprawnień administracyjnych na konkretne źródło pochodzenia danych flow.
46. Musi być dostępna funkcja zapisywania i odtwarzania pełnej konfiguracji systemu oraz jedynie wybranych jego komponentów.
47. System musi posiadać narzędzia do:
    - informowania o statusie systemu, zajętości pamięci, dostępności przestrzeni dyskowej,
    - konfiguracji interfejsów sieciowych,
    - zapisywania pełnego dziennika zdarzeń (logów) związanych z działaniem systemu i uruchomionym na nim usług.
48. System musi umożliwiać :
    - zbieranie informacji o ruchu w sieci komputerowej w oparciu o protokół NetFlow/ IPFIX/ sFlow/jflow oraz podobnych (NSEL,NEL), z urządzeń sieciowych obsługujących te protokoły (switche, routery, dedykowane sondy, itp.);
    - zapisywanie zebranych danych w bazie danych;
    - udostępnienie interfejsu graficznego do przetwarzania zebranych danych, tj. wykonywania statystyk i raportów.
49. System musi pozwalać na backup wybranych profili (baz danych) na zewnętrzny storage
50. System musi mieć możliwość parsowania informacji zawartych w syslogu pochodzących od systemów uwierzytelniania użytkowników w celu powiązania w czasie adresu IP z nazwą użytkownika.
51. Urządzenie do zbierania i przechowywania statystyk Flow musi posiadać wsparcie minimum dla następujących protokołów:
    - NetFlow (wersje 5, oraz 9);
    - IPFIX;
    - sFlow;
    - jFlow;
    - Netstream.
52. Wykonywanie statystyk i generowanie graficznych/ tabelarycznych wyników,

		powinno odbywać się w czasie rzeczywistym (na bieżąco wobec spływających danych NetFlow). 53. System musi posiadać możliwość natychmiastowego filtrowania bieżących danych na ekranie monitora bez konieczności uruchamiania nowego zapytania. 54. System musi posiadać możliwość filtrowania danych według różnych kryteriów dostępnych z raportu NetFlow, w tym: • adres źródłowy; • adres docelowy; • port źródłowy; • port docelowy; • czas (czas trwania raportowany z dokładnością do 1 milisekundy); • urządzenie sieciowe; • interfejs wejściowy; • interfejs wyjściowy; • protokół; • źródłowa aplikacja; • docelowa aplikacja; • ToS (Type of Service); • źródłowy system autonomiczny (AS); • docelowy system autonomiczny (AS); • źródłowa podsieć; • docelowa podsieć; • źródłowa maska podsieci; • docelowa maska podsieci; • flagi TCP. • nazwa użytkownika • parametry DHCP • Parametry DNS • Parametry VoIP • Parametry SAMBA 55. System musi posiadać możliwość automatycznego odczytywania nazw urządzeń, listy interfejsów wraz z nazwami, opisami i prędkościami poprzez protokół SNMP w wersjach 1,2c,3. 56. System musi udostępniać informacje zbiorcze oraz dla każdego urządzenia niezależnie, zawierającą sumaryczną liczbę otrzymanych eksportów określonego typu wysłanych przez każde z urządzeń, wraz z informacjami na temat średniej oraz szczytowej liczby otrzymywanych eksportów od każdego z urządzeń. 57. System musi posiadać funkcję raportowania dzienników zdarzeń (log) serwera i usług. 58. System musi posiadać funkcję konfiguracji portów nasłuchujących na dany typ eksportów.	
2	System Kontroli Domeny	1. Wdrożenie dwóch kontrolerów domeny wraz z zintegrowanymi serwerami DNS. Utworzenie ok. 100 użytkowników domeny i określenie ich przynależności do jednostek organizacyjnych oraz grup zabezpieczeń ze względu na realizowane dla nich funkcje. 2. Konfiguracja hierarchii serwerów DNS, zapytań warunkowych, funkcji przesyłania dalej. 3. Konfiguracja usługi DHCP, umożliwiająca podanie zarządzanym komputerom adresów DNS kontrolerów domeny. 4. Uruchomienie usługi NAP umożliwiającej używanie kontrolerów jako podstawowego i zapasowego serwera RADIUS, kontroli „stanu zdrowia”	1

		systemów zarządzalnych. Określenie serwerów szczepionek, poprawek koniecznych dla „uzdrawiania" systemów nie przechodzących z systemu walidacji. 5. Konfiguracja serwera poprawek Microsoft tzw. WSUS, wraz z konfiguracją sposobu dystrybucji i rodzajów kontrolowanego oprogramowania. 6. Konfiguracja serwera szczepionek systemu antywirusowgo. 7. Konfiguracja usługi Centrum Certyfikacyjnego w celu możliwości generowania i dystrybucji certyfikatów. Ze względów bezpieczeństwa główny urząd certyfikacyjny zostanie wyłączony po wygenerowaniu głównego certyfikatu i autoryzowaniu podrzędnego centrum certyfikacyjnego. Podrzędny urząd przejmie rolę bieżącej kontroli i wystawiania certyfikatów. 8. Dodanie komputerów do domeny umożliwiające zdalną kontrolę nad ich zachowaniami i wprowadzanie centralnych polityk w sposób zautomatyzowany. Migracja profili lokalnych użytkowników na konta domenowe. 9. Utworzenie polityk zapewniających uruchomienie na zarządzanych komputerach procesów odpowiedzialnych za: autentykację 802.1x, dystrybucję certyfikatów, kontrolę stanu zdrowia, mapowanie dopuszczalnych zasobów. 10. Konfiguracja serwera wydruków 11. Konfiguracja serwera plików 12. Szkolenie: Szkolenie Active Directory (Active Directory Services with Windows Server) musi odbyć się w autoryzowanym centrum szkoleniowym z certyfikatem ukończenia szkolenia. Szkolenie musi być przekazane w formie Vouchera z czasem realizacji 1 rok od daty otrzymania. Szkolenie musi odbywać się w języku polskim z lokalizacją w Krakowie. Do szkolenia należy dostarczyć materiały w formie elektronicznej.	
3	NMS Upgrade	Upgrade posiadanego oprogramowania Extreme Networks NetSight ver. NMS-BASE-50 do ver. NMS-ADV-100 Po upgrade oprogramowanie ma spełniać co najmniej poniższe wymagania • Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci. o Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jaka aplikacja dedykowana dla systemu wirtualizacyjnego VMWare o Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS • Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli • Aplikacja zarządzająca musi obsługiwać minimum 100 urządzeń (adresów IP) • Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników. • Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na	1

		oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego • Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników • Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius. • Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze. • Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES • Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu. • Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów • Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB • Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów • Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II • Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych. • Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu. • Aplikacja musi posiadać wbudowany Syslog serwer • Aplikacja musi posiadać wbudowany BootP serwer • Aplikacja musi wspierać protokół IPv4 oraz IPv6 • Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera. • Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora • Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach. • Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem o połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości o stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów o konfiguracji sieci VLAN o konfiguracji protokołu routingu OSPF • Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https • Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane: o adres IP urządzenia o adresu MAC urządzenia o nazwy urządzenia	

		○ wersji oprogramowania ○ wersji bootrom ○ lokalizacji urządzenia ○ danych kontaktowych administratora ○ numeru seryjnego • Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest: ○ możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie ○ możliwość odtworzenia wskazanej konfiguracji urządzenia ○ możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych ○ możliwość obsługi urządzeń sieciowych różnych producentów • Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie • Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach • Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych. • Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp. • Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać: ○ szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy). ○ wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne). ○ wyświetlenie alarmów, trapów SNMP, wpisów syslog itp. ○ generowanie raportów • Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową. ○ Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa). ○ Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac ○ Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje: ▪ adres IP kontrolera ▪ liczba obsługiwanych klientów ▪ szczytowe wartości zajmowanego pasma ▪ wersja oprogramowania ○ Musi być zapewniona widzialność parametrów wszystkich punktów	

		dostępowych zawierających następujące informacje: ▪ adres IP punktu dostępowego ▪ MAC adres punktu dostępowego ▪ wersja oprogramowania ▪ typ punktu dostępowego ▪ kanały pracy poszczególnych interfejsów radiowych ▪ szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych o Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje: ▪ adres IP klienta ▪ MAC adres klienta ▪ nazwa użytkownika ▪ nazwa punktu dostępowego, do którego dołączony jest użytkownik ▪ BSSID, do którego dołączony jest użytkownik ▪ SSID, do którego dołączony jest użytkownik o Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności: ▪ zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate). ▪ zaznaczenie kanałów pracy urządzeń ▪ lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych • Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością z zapewnieniem widzialności następujących informacji: o adresu MAC o adresu IP o nazwy komputera o typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp. o nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika. o adres IP urządzenia, do którego dołączony jest klient. o identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego. o typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp. o nazwa przydzielonej polityki bezpieczeństwa. • System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp. • System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa • System zarządzania tożsamością zautoryzowanych klientów musi zapewniać	

		możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List • System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci. • System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające: o liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp. o liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp. o liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android o liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa o liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp. • System zarządzania tożsamością zautoryzowanych klientów jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 500 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 100 punktów dostępowych oraz min. 100 przełączników sieciowych • System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7. • System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów. o Musi istnieć możliwość integracji systemu zarządzania z co najmniej 2 systemami firewall • System zarządzania musi być objęty 3 letnim wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.	
4	System bezpieczeństwa	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla elementów systemu bezpieczeństwa obsługujących Narodowe Centrum Promieniowania Synchrotronowego Solaris Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy: 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive. W ramach postępowania system powinien zostać dostarczony w postaci klastra HA. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.	1

		5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX oraz 4 gniazdami SFP 1Gbps. 6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 7. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę 8. Przepustowość Firewall'a: nie mniej niż 20 Gbps 9. Wydajność szyfrowania VPN IPSec: nie mniej niż 9 Gbps 10. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. 11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. 12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection • Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN • Ochrona przed atakami - Intrusion Prevention System • Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. • Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP • Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma • Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) • Możliwość analizy ruchu szyfrowanego protokołem SSL • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) 13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 6 Gbps 14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 1 Gbps 15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site	

		• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Praca w topologii Hub and Spoke oraz Mesh • Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth 16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a. 19. Translacja adresów NAT adresu źródłowego i docelowego. 20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci. 21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ 22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. 23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. 24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP 25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW. 26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. 27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne	

bazy danych

- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
30. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 3 lat.
31. Gwarancja oraz wsparcie, szkolenia
    - Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
    - Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5 /24x7. Oferent winien przedłożyć dokumenty:
      - oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
      - oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
      - certyfikat ISO 9001 podmiotu serwisującego
    - W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od

		importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. • Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych. • Szkolenia : oferent winien zapewnić 2 szkolenia wraz z egzaminami oraz materiałami w formie elektronicznej z zakresu bezpieczeństwa informacji, dla 1 osoby . Szkolenia winny być zrealizowane w okresie do 12 miesięcy od daty zawarcia umowy. ◦ Szkolenie min. na poziomie „Mile 2 CISSO” lub równoważne ◦ Szkolenie min. na poziomie „Mile2 CSLO” lub równoważne	
5	Usługa konsultacji wdrożenia normy ISO 27001	Wymagane jest aby oferent posiadał certyfikat ISO 27001. Praktyczne konsultacje z zakresu wdrożenia i zarządzania systemem zarządzania bezpieczeństwem informacji zgodnie z normą ISO 27001, tym wytwarzanie dokumentów przewidzianych normą ISO 27001. Konsultacje w wymiarze 100 godzin muszą uwzględniać aspekty projektowanego środowiska domenowego i kwestie związane z zarządzaniem tym środowiskiem w aspekcie normy ISO 27001. Oferent winien zapewnić konsultacje na miejscu u odbiorcy w terminie do 12 miesięcy od daty zawarcia umowy. Oferent winien zapewnić szkolenie dla 1 osoby z normy ISO 27001, min. na poziomie „PECB Lead Implementer” wraz z egzaminem i materiałami w formie elektronicznej. Szkolenie winno być zrealizowane w okresie do 12 miesięcy od daty zawarcia umowy.	1

6	Macierz dyskowa NAS (7x 2TB HDD)			1

Komponent	Parametr minimalny
Obudowa	RACK 2U z kompletem elementów do montażu w szafie RACK19”
CPU	Czterordzeniowy procesor o wydajności min. 8840pkt. (www.cpubenchmark.net)
Pamięć	Zainstalowana 16GB ECC RAM DDR3-1600, możliwość rozszerzenia do 32GB (co najmniej 2 wolne sloty na rozszerzenie pamięci)
Zgodny typ dysków	3,5" lub 2,5" SATA, 2.5" SATA SSD
Maksymalna wewnętrzna pojemność pierwotna	96TB (12 x 8 TB HDD)
Maksymalna pojemność surowa z jednostkami rozszerzającymi	288 TB (8 TB HDD x 36)
Dyski	Zainstalowane 7 dysków SATA HDD o pojemności min. 2TB, MTBF 2 000 000h -każdy (zainstalowane dyski muszą być w pełni zgodne z dostarczonym serwerem plików NAS i znajdować się na jego opublikowanej liście kompatybilności); gwarancja zgodna z gwarancją producenta - 5 lat
Porty zewnętrzne	USB 3.0 x 2, USB 2.0 x 2, gniazdo rozszerzenia (Infiniband) x 2
LAN	4 porty 1GbE (RJ-45), 2 porty 10GbE (RJ-45)
Gniazdo PCIe 3.0 x8	2szt. x8 fizyczny - do obsługi kart sieciowych 10GbE o podwójnych portach
Wake on LAN/WAN	Tak
Obsługa sieci bezprzewodowej (karta zewnętrzna)	Tak
Protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN, L2TP)
System plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT3
Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108 TB/200 TB (przy 32 GB RAM, dla grup RAID 5 lub RAID 6); maksymalna liczba woluminów wewnętrznych: 1024, maksymalna liczba obiektów iSCSI Target: 64, maksymalna liczba jednostek iSCSI LUN: 512, obsługa klonowania i migawek RAID; obsługiwane jednostki rozszerzające
Obsługiwane typy macierzy RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcje RAID	- Migracja macierzy RAID - RAID 1 do RAID 5, RAID 5 do RAID 6 - Hot Spare dla, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	Maksymalna liczba kont użytkowników: 16000, maksymalna liczba grup: 512; maksymalna liczba folderów współdzielonych: 512, maksymalna liczba jednoczesnych połączeń SMB/AFP/FTP/File Station: 1024
Uprawnienia	Lista kontroli dostępu (ACL) systemu Windows
Wirtualizacja	VMware, Microsoft Hyper-V, Citrix
Usługa katalogowa	Integracja z usługą Windows AD. Logowanie użytkowników domeny przez protokoły Samba (SMB)/AFP/FTP, integracja z LDAP
Bezpieczeństwo	FTP przez SSL/TLS, automatyczne blokowanie adresów IP, zapora sieciowa, szyfrowana sieciowa kopia zapasowa przy użyciu protokołu Rsync, połączenia HTTPS

7	Macierz dyskowa NAS (12x 1TB SSD)	**Komponent**	**Parametr minimalny**	1
		Obudowa	RACK 2U z kompletem elementów do montażu w szafie RA	
		CPU	Czterordzeniowy procesor o wydajności min. 8840pk (www.cpubenchmark.net)	
		Pamięć	Zainstalowana 16GB ECC RAM DDR3-1600, możliwość rozsz 32GB (co najmniej 2 wolne sloty na rozszerzenie pamięci)	
		Zgodny typ dysków	3,5" lub 2,5" SATA, 2.5" SATA SSD	
		Maksymalna wewnętrzna pojemność pierwotna	96TB (12 x 8 TB HDD)	
		Maksymalna pojemność surowa z jednostkami rozszerzającymi	288 TB (8 TB HDD x 36)	
		Dyski	Zainstalowane 12 dysków SATA SSD 2,5” o pojemności m MTBF 1000000h, DWPD 0,87, szybkość odczytu/ 550MB/s, zapisu 530MB/s - każdy (zainstalowane dyski muszą być zgodne z dostarczonym serwerem plików NAS i znajdować si opublikowanej liście kompatybilności); gwarancja zgodna z g producenta - 5 lat	
		Porty zewnętrzne	USB 3.0 x 2, USB 2.0 x 2, gniazdo rozszerzenia (Infiniband) x	
		LAN	4 porty 1GbE (RJ-45), 2 porty 10GbE (RJ-45)	
		Gniazdo PCIe 3.0 x8	2szt. x8 fizyczny - do obsługi kart sieciowych 10GbE o podwó portach	
		Wake on LAN/WAN	Tak	
		Obsługa sieci bezprzewodowej (karta zewnętrzna)	Tak	
		Protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH VPN (PPTP, OpenVPN, L2TP)	
		System plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT3	
		Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108 TB/200 TB GB RAM, dla grup RAID 5 lub RAID 6); maksymalna liczba woluminów wewnętrznych: 1024, maksymalna liczba obiektów Target: 64, maksymalna liczba jednostek iSCSI LUN: 512, obsł klonowania i migawek RAID; obsługiwane jednostki rozszerzaj	
		Obsługiwane typy macierzy RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10	
		Funkcje RAID	- Migracja macierzy RAID - RAID 1 do RAID 5, RAID 5 do R - Hot Spare dla, RAID 1, RAID 5, RAID 6, RAID 10	
		Funkcja udostępniania plików	Maksymalna liczba kont użytkowników: 16000, maksymalna li 512; maksymalna liczba folderów współdzielonych: 512, maksy liczba jednoczesnych połączeń SMB/AFP/FTP/File Station: 102	
		Uprawnienia	Lista kontroli dostępu (ACL) systemu Windows	
		Wirtualizacja	VMware, Microsoft Hyper-V, Citrix	
		Usługa katalogowa	Integracja z usługą Windows AD: Logowanie użytkowników do przez protokoły Samba (SMB)/AFP/FTP, integracja z LDAP	
		Bezpieczeństwo	FTP przez SSL/TLS, automatyczne blokowanie adresów IP, zap sieciowa, szyfrowana sieciowa kopia zapasowa przy użyciu pro Rsync, połączenia HTTPS	
		Obsługa kamer IP	Tak, min. 65 kamer (w tym min. dwie licencje bezpłatne – doda licencje opcjonalne)	
		Natężenie dźwięku	Nie więcej niż 41 dB(A)	
		Obsługiwane systemy klienckie	Od Windows 7, Mac OS X 10.10 do aktualnych	
		Obsługiwane przeglądarki	Firefox, Chrome, Internet Explorer, Safari	
		Język GUI	Polski	

		Gwarancja	Gwarancja producenta 5 lat dla serwera plików NAS (rozsz gwarancja z dostawą nowej części w miejsce uszkodzonej w try drugi dzień roboczy)	
	Dostarczenie urządzeń	Wykonawca ma dostarczyć wszystkie zamawiane urządzenia i wstępnie uruchomić je u Zamawiającego. Oznacza to: 1. Dostarczenie do Zamawiającego i rozpakowaniu we wskazanym pomieszczeniu. 2. Uaktualnienia oprogramowania wewnętrznego przełączników do najnowszej wersji dostępnej u producenta. 3. Wykazania, że dostarczone wszystkie elementy są sprawne technicznie. Zamawiający w własnym zakresie dokona modyfikacji konfiguracji urządzenia spełniającej potrzeby Zamawiającego.	

Część 2

Wsparcie Gwarancyjne dla przełącznika Extreme Networks BD 8900	1. Przedmiotem zamówienia jest przedłużenie gwarancji/serwisu producenta o 3 lata na modułowy przełącznik sieciowy Extreme Networks BD 8900 wyposażony w moduły o następujących numerach seryjnych a. Chassis : 800392-00-04 1438G-002555X4M0Z1 b. MSM-A : 800369-00-05 1449G-00074 c. MSM-B : 800369-00-06 1232G-00763 d. Licencja Core 2. Przynajmniej trzy lata gwarancji od momentu dostawy, czas reakcji maksymalnie do końca dnia od zgłoszenia, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu, naprawa najpóźniej w następnym dniu roboczym. 3. Wszystkie naprawy gwarancyjne w miejscu instalacji. W przypadku gdy naprawa na miejscu instalacji nie jest możliwa i sprzęt musi być zabrany do naprawy, należy zapewnić sprzęt zastępczy. 4. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. 5. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia dostawcy, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta. 6. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych) 7. W przypadku urządzeń wyposażonych w dyski twarde, w razie awarii dysk twardy zostaje własnością zamawiającego. Wykonawca zapewniając przedłużenie gwarancji dla ww. sprzętu zobowiązany jest poinformować gwaranta, iż Zamawiający może być zainteresowany w przyszłości dalszym przedłużeniem okresu gwarancji/serwisu na ww. sprzęt.