

**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**

**(SIWZ)**

**dla postępowania prowadzonego w trybie przetargu nieograniczonego o wartości poniżej wyrażonej w złotych równowartości kwoty 221 000 euro**

**na**

**Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie**

**SYMBOL : AZ.2710.15.2019.MS**

**Zatwierdził:**

**………………………………………………………………………………….**

SPIS TREŚCI:

I. Nazwa Zamawiającego

II. Tryb udzielenia zamówienia

III. Rodzaj i nazwa zamówienia

IV. Opis przedmiotu zamówienia

V. Termin realizacji zamówienia i okres gwarancji

VI. Warunki udziału w postępowaniu

VII. Podwykonawstwo

VIII. Oferty wspólne

IX. Porozumiewanie się Zamawiającego z wykonawcami oraz przekazywanie oświadczeń i dokumentów.

X. Wyjaśnienie treści specyfikacji istotnych warunków zamówienia

XI. Modyfikacja treści specyfikacji istotnych warunków zamówienia

XII. Wymagania dotyczące wadium

XIII. Opis sposobu przygotowania oferty

XIV. Miejsce oraz termin składania i otwarcia ofert

XV. Opis sposobu obliczenia ceny

XVI. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty,

XVII. Zawiadomienie o wyborze najkorzystniejszej oferty

XVIII. Unieważnienie postępowania

XIX. Informacje o formalnościach jakie należy dopełnić po wyborze oferty w celu zawarcia umowy

XX. Zabezpieczenie należytego wykonania umowy

XXI. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia

XXII. Postanowienia końcowe

XXIII. Katalog zmian umowy

ZAŁĄCZNIKI DO SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA:

Załącznik nr 1 Opis przedmiotu zamówienia (dalej zwany „OPZ”)

Załącznik nr 2 Formularz oferty

Załącznik nr 3 Formularz cenowo - przedmiotowy

Załącznik nr 4 Oświadczenie wykonawcy o spełnieniu warunków udziału w postępowaniu

Załącznik nr 5 Przykładowy wzór zobowiązania podmiotu trzeciego

Załącznik nr 6 Oświadczenie wykonawcy o braku podstaw wykluczenia

Załącznik nr 7 Informacja Wykonawcy o przynależności do grupy kapitałowej

Załącznik nr 8 Wykaz dostaw

Załącznik nr 9 Wzór umowy

Załącznik nr 10 Oświadczenie dotyczące posiadania autoryzacji producenta dostarczonych przełączników sieciowych

**I. NAZWA ZAMAWIAJĄCEGO**

Muzeum Narodowe w Szczecinie

ul. Staromłyńska 27

70-561 Szczecin

Tel. (+48) 91 4315 200

Fax (+48) 91 4315 204

e-mail: biuro@muzeum.szczecin.pl;

strona internetowa: [www.bip.muzeum.szczecin.pl](http://www.bip.muzeum.szczecin.pl)

**II. TRYB UDZIELENIA ZAMÓWIENIA**

1. Przetarg nieograniczony na podstawie art. 39 ustawy z dnia 29 stycznia 2004 r Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 z późn. zm.), zwanej dalej Ustawą Pzp.

2) Przedmiot zamówienia realizowany w ramach realizacji projektu pn. „www.muzeach” współfinansowanego ze środków Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020 oraz ze środków Ministra Kultury I Dziedzictwa Narodowego

1. Wartość zamówienia nie przekracza równowartości kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 Ustawy Pzp.
2. Zamawiający informuje, że postępowanie będzie prowadzone wg zasad określonych w art. 24 aa Ustawy Pzp (tzw. „procedura odwrócona”), tj. Zamawiający, najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
3. Do niniejszego postępowania stosuje się przepisy Ustawy Pzp
4. Rodzaj zamówienia – dostawy
5. Zamawiający nie dopuszcza do składania ofert wariantowych.
6. Zamawiający nie przewiduje zamówień uzupełniających
7. Postępowanie prowadzone jest w języku polskim. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
8. Każdy Wykonawca może złożyć tylko jedną ofertę.
9. Wykonawca jest związany ofertą, przez okres 30 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

**III.** **RODZAJ I NAZWA ZAMÓWIENIA**

1. Dostawy – Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie

**2) Kod CPV:**

 48820000-2 serwery

30233141-1 Nadmiarowa macierz niezależnych dysków (RAID)

30233160-0 Jednostki pamięci taśmowej

32413100-2 Rutery sieciowe

48710000-8 Pakiety oprogramowania do kopii zapasowych i odzyskiwania

48620000-0 Systemy operacyjne

31213300-5 Szafy kablowe

31220000-4 Elementy składowe obwodów elektrycznych

32420000-3 Urządzenia sieciowe

30231000-7 Ekrany i konsole komputerowe

31213100-3 Rozdzielnie

32420000-3 Urządzenia sieciowe

30237360-0 Kasety z taśmą LTO

**IV. OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiot zamówienia:

1. Przedmiotem zamówienia jest **Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie** a w szczególności:

|  |  |
| --- | --- |
| **Nazwa** | **ilość** |
| Serwer typu RACK | 2  |
| Macierz dyskowa  | 1  |
| Napęd taśmowy LTO | 1  |
| UTM | 1  |
| Oprogramowanie do backupu | 1 |
| System operacyjny serwera | 2  |
| Szafa dystrybucyjna  | 1 |
| Zasilacz awaryjny do szafy serwerowej | 1 |
| Przełacznik sieciowy dystrybucyjny z funkcją PoE | 1 |
| KVM | 1 |
| Listwa PDU | 2 |
| Przełącznik sieciowy szkieletowy | 1 |
| Taśmy LTO  | 20 |

|  |
| --- |
|  |
|  |
| 2. Szczegółowy opis zamówienia oraz wymagany okres udzielonej gwarancji i szczegóły dotyczące warunków gwarancji i świadczeń gwarancyjnych zawarte są w poszczególnych Specyfikacjach technicznych ( Załącznik nr 1 opis przedmiotu zamówienia). |
|  |
|  |

**V. TERMIN REALIZACJI ZAMÓWIENIA I OKRES GWRANCJI**

1) Zamawiający wymaga, aby zamówienie zostało wykonane najpóźniej w terminie **35 dni** od dnia zawarcia umowy.

 **UWAGA: termin dostawy jest kryterium oceny ofert**

2) Bieg okresu udzielonych gwarancji rozpoczyna się z dniem podpisania protokołu odbioru końcowego.

3) Minimalny okres gwarancji opisany jest w każdej Specyfikacji technicznej w Załączniku nr 1.

4) Wywiązanie się z realizacji zamówienia potwierdzone będzie przez Zamawiającego na protokole odbioru końcowego dostarczonym przez Wykonawcę w obecności przedstawicieli obu stron (wzór protokołu odbioru zamówienia – załącznik nr 10 ).

**VI. WARUNKI UDZIAŁU W POSTĘPOWANIU**

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 24 ust. 1 pkt 12) – 23) ustawy pzp.
2. Ponadto Zamawiający wykluczy wykonawcę na podstawie niżej wymienionych przesłanek określonych w art.24 ust. 5 pkt 1)-4) oraz 8)ustawy pzp, tj.;
3. **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. 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 (Dz. U. z 2015 r., poz. 233 z późn.zm.);**
4. **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;**
5. **jeżeli Wykonawca lub osoby, o których mowa w art. 24 ust. 1 pkt 14 ustawy pzp, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2-4 ustawy pzp z:**
* Zamawiającym,
* osobami uprawnionymi do reprezentowania Zamawiającego,
* członkami komisji przetargowej,
* osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a ustawy pzp; chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu;

 **d) 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, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;**

 **e) 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 bądź zawarł wiążące porozumienie w sprawie spłaty tych należności.**

3) Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16-20 lub ust. 5 pkt 1-4 oraz 8) 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. Zdania pierwszego 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. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające dowody określone w zdaniu pierwszym.

4) O udzielenie zamówienia mogą ubiegać się Wykonawcy którzy spełniają warunki udziału w postępowaniu dotyczące:

 **a) Kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej:**

Zamawiający nie stawia warunku w tym zakresie.

 **b) Sytuacji ekonomicznej lub finansowej:**

O udzielenie niniejszego zamówienia mogą ubiegać się Wykonawcy, którzy posiadają ubezpieczenie odpowiedzialności cywilnej na sumę gwarancyjną min. **200 000,00 zł.**

 **c) Zdolności technicznej lub zawodowej w tym:**

 Wykonawca musi wykazać się doświadczeniem, polegającym na tym, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał przynajmniej 1 zamówienie polegające na dostawie sprzętu serwerowego (wyposażenie szafy serwerowej) o wartości nie mniejszej niż **200 000,00**  zł brutto.

 Jako jedno zamówienie należy rozumieć dostawę/dostawy w ramach jednej umowy.

Ocena spełniania powyższego warunku będzie prowadzona w oparciu o wykaz dostaw, według kryterium spełnia/nie spełnia.

5) Informacja dla Wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 22a ustawy pzp

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach w odniesieniu do zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, 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.
2. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy pzp, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia 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;
* zakres i okres udziału innego podmiotu przy wykonywaniu Zamówienia;
* czy podmiot, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.

 c) 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 12–23 ustawy pzp.

 d) W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.

 e) Jeżeli zdolności techniczne lub zawodowe lub sytuacja ekonomiczna lub finansowa, podmiotu, nie potwierdzają spełnienia przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tych podmiotów podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego:

* zastąpił ten podmiot innym podmiotem lub podmiotami lub
* zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe lub sytuację finansową lub ekonomiczną, o których mowa w lit. a)

**VII. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW JAKIE NALEŻY DOŁĄCZYĆ DO OFERTY**

1. **Do oferty – Załącznik nr 2 Wykonawca dołącza aktualne na dzień składania ofert:**
	1. **Wypełniony Formularz cenowo – przedmiotowy – Załącznik nr 3,**
	2. **Oświadczenie o spełnieniu warunków w postępowaniu – Załącznik nr 4**
	3. **Oświadczenie o braku podstaw do wykluczenia – Załącznik nr 6**
	4. **Pełnomocnictwo do złożenia oferty, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą; pełnomocnictwo powinno być załączone w oryginale lub kopii notarialnie potwierdzonej,**
	5. **Pełnomocnictwo dla pełnomocnika ustanowionego przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, pełnomocnictwo powinno być załączone w oryginale lub kopii notarialnie potwierdzonej,**
	6. **Zobowiązanie podmiotu trzeciego albo inny dokument służący wykazaniu udostępnienia Wykonawcy potencjału przez podmiot trzeci, jeżeli Wykonawca wykazując spełnienie warunków udziału w postępowaniu polega na zdolnościach lub sytuacji innych podmiotów,**
	7. **Wadium, jeżeli zostało złożone w formie niepieniężnej**
	8. **Załącznik nr 10 do formularza ofertowego– oświadczenie dotyczące posiadania autoryzacji producenta dostarczonych przełączników sieciowych jeżeli wykonawca posiada**
2. Zamawiający, zgodnie z art.24 aa ustawy pzp, w pierwszej kolejności dokona oceny ofert, a następnie zbada czy wykonawca, którego oferta została oceniona jako najkorzystniejsza nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

**VIII. DOKUMENTY SKŁADANE NA WEZWANIE**

Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona do **złożenia w wyznaczonym, nie krótszym niż 5 dni terminie, aktualnych na dzień złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy pzp**. Zamawiający wezwie Wykonawcę, w szczególności do złożenia następujących dokumentów:

1. **Dokumenty i oświadczenia, które wykonawca składa w postępowaniu na wezwanie zamawiającego na potwierdzenie okoliczności, o których mowa w art.25 ust.1 pkt 3 ustawy w celu potwierdzenia braku podstaw wykluczenia wykonawcy z udziału w postępowaniu, Zamawiający żąda następujących dokumentów a w szczególności:**
	* informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 Ustawy Pzp, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert
	* odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy pzp;
	* zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
	* zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
	* 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,
	* oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,
	* oświadczenia Wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2016 r. poz. 716).
2. **Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w pkt 1, składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, odpowiednio:**
* W zakresie pkt 1.1 - 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 ustawy pzp powinien być wystawiony nie wcześniej niż 6 miesiący przed upływem tego terminu.
* W zakresie pkt 1.2 - Informację, że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Dokumenty te powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert
* W zakresie pkt 1.3 i 1.4 - Informację, że nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne, albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu. Dokument powinien być wystawiony nie wcześniej 3 miesiące przed upływem tego terminu.
* Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, 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.
1. **Dokumenty i oświadczenia, które wykonawca składa w postępowaniu na wezwanie zamawiającego na potwierdzenie okoliczności, o których mowa w art.25 ust.1 pkt 1 ustawy w celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu dotyczących zdolności technicznej lub zawodowej zamawiający żąda następujących dokumentów a w szczególności:**
* wykaz zamówień 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 zamówienia zostały wykonane, wraz z załączeniem dowodów określających czy te zamówienia 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;
* dokumentów potwierdzających, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną określoną przez zamawiającego.
1. Zgodnie z art. 26. ust. 2 ustawy pzp składane na wezwanie Zamawiającego dokumenty i oświadczenia powinny być aktualne na dzień złożenia oświadczeń lub dokumentów i potwierdzać okoliczności, o których mowa w art. 25 ust. 1 ustawy pzp.
2. 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, a jeżeli zachodzą uzasadnione podstawy do uznania, ze złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych lub dokumentów.
3. Wykonawca, w **terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy pzp, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej**, o której mowa w art. 24 ust. 1 pkt 23 ustawy pzp- Załącznik nr 7 do SIWZ. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
4. Ocena warunków udziału w postępowaniu nastąpi na podstawie analizy oświadczeń i dokumentów, jakie Wykonawca zawarł w swojej ofercie, z zastrzeżeniem art. 26 ust. 3 i 3a ustawy pzp.

**IX. ODRZUCENIE OFERTY**

Zamawiający odrzuca ofertę, jeżeli:

1. jest niezgodna z ustawą.
2. jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia, z zastrzeżeniem art. 87 ust. 2 pkt. 3 ustawy pzp.
3. jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.
4. jest ofertą, która zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.
5. została złożona przez wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia.
6. zawiera błędy w obliczeniu ceny lub kosztu.
7. wykonawca w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt. 3 ustawy pzp.
8. Wadium nie zostało wniesione lub zostało wniesione w sposób nieprawidłowy, jeżeli zamawiający żądał wniesienia wadium,
9. jest nieważna na podstawie odrębnych przepisów,
10. wykonawca nie wyraził zgody, o której mowa w art. 85 ust. 2 ustawy pzp, na przedłużenie terminu związania ofertą;
11. jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, w tym bezpieczeństwo podmiotów objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401 i 1560), a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;

**X. PODWYKONAWSTWO**

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.
2. W przypadku powierzenia wykonania części zamówienia podwykonawcy, Wykonawca zobowiązany jest do wykazania w formularzu ofertowym części zamówienia, której wykonanie zamierza powierzyć podwykonawcom oraz podania przez Wykonawcę nazw (firm) tych podwykonawców.
3. Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, o ile są już znane, podał nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w takie usługi. Wykonawca zawiadamia Zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację prac.
4. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby wykonawca powoływał się, na zasadach określonych w niniejszej Specyfikacji (art. 22a ust. 1 ustawy pzp.), w celu wykazania spełniania warunków udziału w postępowaniu, wykonawca jest obowiązany wykazać zamawiającemu, że proponowany inny podwykonawca lub wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby zamawiający powoływał się w trakcie postępowania o udzielenie zamówienia.
5. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.

**XI. OFERTY WSPÓLNE**

1) W przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, dokumenty potwierdzające, że Wykonawca nie podlega wykluczeniu, składa każdy z Wykonawców oddzielnie. Wykonawcy wspólnie ubiegający się o zamówienie:

1. **ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania;**
2. **zobowiązani są ustanowić Pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia publicznego albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia. Przyjmuje się, że pełnomocnictwo do podpisania oferty obejmuje pełnomocnictwo do poświadczenia za zgodność z oryginałem wszystkich dokumentów;**
3. **pełnomocnictwo musi wynikać z umowy lub z innej czynności prawnej, mieć formę pisemną; fakt ustanowienia Pełnomocnika musi wynikać z załączonych do oferty dokumentów, wszelka korespondencja prowadzona będzie z Pełnomocnikiem;**

2) W przypadku wspólnego ubiegania się o zamówienie przez wykonawców:

1. **oświadczenie w zakresie wskazanym w załączniku 4 do SIWZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnienie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnienie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.**
2. **dokumenty wspólne, takie jak np.: oferta cenowa, wykaz zrealizowanych zamówień, itp. składa pełnomocnik Wykonawców w imieniu wszystkich Wykonawców składających ofertę wspólną,**
3. **kopie dokumentów dotyczących każdego z Wykonawców składających ofertę wspólną muszą być poświadczone za zgodność z oryginałem przez osobę lub osoby upoważnione do reprezentowania tych Wykonawców.**

3) Wspólnicy spółki cywilnej są traktowani jak Wykonawcy składający ofertę wspólną i mają do nich zastosowanie zasady określone w pkt 1 – 4 niniejszego rozdziału.

4) Przed podpisaniem umowy (w przypadku wygrania postępowania) Wykonawcy składający ofertę wspólną będą mieli obowiązek przedstawić Zamawiającemu umowę konsorcjum, zawierającą, co najmniej:

1. **zobowiązanie do realizacji wspólnego przedsięwzięcia gospodarczego obejmującego swoim zakresem realizację przedmiotu zamówienia,**
2. **określenie zakresu działania poszczególnych stron umowy,**
3. **czas obowiązywania umowy, który nie może być krótszy, niż okres obejmujący realizację zamówienia.**

**XII. POROZUMIEWANIE SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA**

 **OŚWIADCZEŃ I DOKUMENTÓW,**

1. Postępowanie o udzielenie zamówienia prowadzone jest w języku polskim, z zachowaniem formy pisemnej.
2. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pisemnie, faksem lub drogą elektroniczną z zastrzeżeniem ust. 3.
3. Oferta może być złożona wyłącznie w formie pisemnej.
4. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
5. Do kontaktowania się z Wykonawcami upoważniony jest pracownik Muzeum Narodowego w Szczecinie:

Rafał Piątkowski, tel. 797 705 227

Monika Skowrońska tel. 797 705 262

**X. WYJAŚNIENIE TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA**

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści niniejszej specyfikacji istotnych warunków zamówienia. Zamawiający udzieli wyjaśnień niezwłocznie wszystkim wykonawcom, którym przekazał specyfikację istotnych warunków zamówienia nie później niż **na 2 dni** przed upływem terminu składania ofert, z zastrzeżeniem pkt. 2.
2. Jeżeli wniosek o wyjaśnienie treści specyfikacji wpłynie do zamawiającego później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert lub dotyczy udzielonych wyjaśnień, zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpoznania.
3. Ewentualna zmiana terminu składania ofert nie powoduje przesunięcia terminu, o którym mowa w pkt. 2, po upłynięciu, którego zamawiający może pozostawić wniosek o wyjaśnienie treści specyfikacji bez rozpoznania.
4. Treść zapytań oraz udzielone wyjaśnienia zostaną jednocześnie przekazane wszystkim wykonawcom, którym przekazano specyfikację istotnych warunków zamówienia, bez ujawniania źródła zapytania oraz zamieszczone na stronie internetowej Zamawiającego.
5. Nie udziela się żadnych ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane do zamawiającego zapytania w sprawach wymagających zachowania pisemności postępowania.
6. Zamawiający nie przewiduje zorganizowania zebrania wszystkich wykonawców.

**XI. MODYFIKACJA TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA**

1. W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmodyfikować treść specyfikacji istotnych warunków zamówienia.
2. Wprowadzone w ten sposób modyfikacje, uzupełnienia i ustalenia lub zmiany, w tym zmiany terminów zamieszczone zostaną na stronie internetowej Zamawiającego.
3. Wszelkie modyfikacje, uzupełnienia i ustalenia oraz zmiany, w tym zmiany terminów, jak również pytania wykonawców wraz z wyjaśnieniami stają się integralną częścią specyfikacji istotnych warunków zamówienia i będą wiążące przy składaniu ofert. Wszelkie prawa i zobowiązania wykonawcy odnośnie wcześniej ustalonych terminów będą podlegały nowemu terminowi.
4. Jeżeli wprowadzona modyfikacja treści specyfikacji nie prowadzi do zmiany treści ogłoszenia zamawiający może przedłużyć termin składania ofert o czas niezbędny na wprowadzenie zmian w ofertach, jeżeli będzie to niezbędne.
5. Jeżeli wprowadzona modyfikacja treści specyfikacji prowadzi do zmiany treści ogłoszenia zamawiający zamieści w Biuletynie Zamówień Publicznych "ogłoszenie o zmianie głoszenia zamieszczonego w Biuletynie Zamówień Publicznych", przedłużając jednocześnie termin składania ofert o czas niezbędny na wprowadzenie zmian w ofertach, jeżeli spełnione zostaną przesłanki określone w art. 12a ust. 1 Ustawy Pzp.
6. Niezwłocznie po zamieszczeniu w Biuletynie Zamówień Publicznych "ogłoszenia o zmianie głoszenia” zamieszczonego w Biuletynie Zamówień Publicznych zamawiający zamieści informację o zmianach na stronie internetowej Zamawiającego.

**XII. WYMAGANIA DOTYCZĄCE WADIUM**

1) Wysokość wadium ustala się w wysokości 7000 zł.

2) Wadium wnoszone w formie pieniężnej należy wnieść przelewem na rachunek bankowy Zamawiającego:

**Bank Gospodarstwa Krajowego, Oddział Szczecin, ul. Tkacka 4 , 70-556 Szczecin**

**Nr rachunku : 68 1130 1176 0022 2063 6520 0004**

z dopiskiem na blankiecie przelewu: wadium na zabezpieczenie oferty przetargowej z nazwą i symbolem zamówienia. Kserokopię dowodu przelewu potwierdzoną za zgodność z oryginałem należy dołączyć do oferty.

3) Wadium może być wnoszone w formie: pieniężnej, poręczenia bankowego, lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, gwarancji bankowej, gwarancji ubezpieczeniowej lub poręczeń udzielanych przez podmioty, o których mowa w art. 6b ust 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2007 r. Nr 42, poz.275).

4) Z treści gwarancji powinno wynikać bezwarunkowe i nieodwołalne, na pierwsze pisemne żądanie zgłoszone przez Zamawiającego w okresie związania ofertą, zobowiązanie gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a i 5 ustawy.

5) Treść gwarancji wadialnej musi zawierać następujące informacje:

* + 1. nazwa i adres Zamawiającego wraz z symbolem zamówienia;
		2. nazwę przedmiotu zamówienia wraz ze znakiem sprawy (SIWZ rozdz. I)
		3. nazwę i adres Wykonawcy;
		4. termin ważności gwarancji;

6)Wadium musi być wniesione nie później niż do wyznaczonego terminu składania ofert.

7) Wniesienie wadium w pieniądzu będzie skuteczne, jeżeli w podanym terminie rachunek bankowy Zamawiającego zostanie uznany pełną kwotą wymaganego wadium.

8) Zamawiający zwróci niezwłocznie wadium wszystkim Wykonawcom po wyborze oferty najkorzystniejszej, z wyjątkiem wykonawcy, którego oferta została wybrana, jako najkorzystniejsza.

9) Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, Zamawiający zwraca wadium niezwłocznie po zawarciu umowy w sprawie Zamówienia publicznego oraz wniesieniu zabezpieczenia należytego wykonania umowy.

10) Zamawiający zwróci niezwłocznie wadium na wniosek Wykonawcy, który wycofał ofertę przed terminem składania ofert.

11) Zamawiający będzie żądał ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium niezwłocznie po wyborze oferty najkorzystniejszej, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wniesie wadium w terminie określonym przez Zamawiającego.

12) W przypadku wniesienia odwołania, Zamawiający nie później niż na 7 dni przed upływem ważności wadium, wezwie Wykonawców, pod rygorem wykluczenia z postępowania, do przedłużenia ważności wadium albo wniesienia nowego wadium na okres niezbędny do zabezpieczenia postępowania do zawarcia umowy. Jeżeli odwołanie wniesiono po wyborze oferty najkorzystniejszej, wezwanie skieruje jedynie do Wykonawcy, którego ofertę wybrano jako najkorzystniejszą.

13) Zamawiający zatrzyma wadium wraz z odsetkami, jeżeli :

* 1. wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1, oświadczenia, o którym mowa w art. 25a ust. 1, pełnomocnictw lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3, co spowodowało brak możliwości wybrania oferty złożonej przez wykonawcę jako najkorzystniejszej.
	2. Wykonawca odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie,
	3. Wykonawca nie wniósł wymaganego zabezpieczenia należytego wykonania umowy,
	4. Zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

**XIII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY**

1. Wykonawca może złożyć tylko jedną ofertę.

Treść oferty musi odpowiadać treści specyfikacji istotnych warunków zamówienia.

Opis sposobu przygotowania ofert:

1. Oferta powinna być sporządzona w formie pisemnej, w języku polskim; zaleca się, aby oferta została sporządzona na formularzu załączonym do niniejszej specyfikacji istotnych warunków zamówienia;
2. Załącznikami do oferty, stanowiącymi jej integralną część, są oświadczenia i dokumenty wymienione w SIWZ;
3. Oferta i każdy z załączników powinny zostać podpisane przez Wykonawcę lub osobę upoważnioną do jego reprezentowania i składania w jego imieniu oświadczenia woli;
4. W przypadku, gdy Wykonawcę reprezentuje pełnomocnik, do oferty musi być załączone pełnomocnictwo (w oryginale lub kopii potwierdzonej notarialnie) z określeniem jego zakresu;
5. Ewentualne poprawki w treści oferty powinny być naniesione czytelnie i sygnowane podpisem Wykonawcy;
6. Wszystkie strony oferty powinny być spięte (zszyte) w sposób trwały, zapobiegający możliwości dekompletacji zawartości oferty.
7. Wykonawca może zastrzec w ofercie informacje stanowiące tajemnice przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Wykonawca w takim przypadku zobowiązany jest wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa, a także wydzielić je w wybrany przez siebie sposób, zapewniający zachowanie tajemnicy przedsiębiorstwa. Tak wydzielonych informacji Zamawiający nie będzie ujawniał. Wykonawca nie może zastrzec informacji i dokumentów, których jawność wynika z innych aktów prawnych w tym m.in. z zapisu art. 86 ust. 4 Ustawy Pzp.
8. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór jego oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując jednocześnie nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania tego obowiązku, oraz wskazując ich wartość bez kwoty podatku.
9. Oferta powinna zostać zapakowana w sposób uniemożliwiający jej przypadkowe otwarcie oraz opisana w sposób jednoznacznie wskazujący jej charakter i przeznaczenie. Koperta zewnętrzna (zawierająca kopertę z ofertą) opatrzona napisem:

**Oferta na:**

|  |
| --- |
| **Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie** **symbol zamówienia:****AZ.2710.15.2019.MS** |

Wykonawca może, przed upływem terminu składania ofert zmienić, uzupełnić lub wycofać ofertę. Zmiana, uzupełnienie lub wycofanie oferty odbywa się w taki sam sposób jak złożenie oferty, tj. w zamkniętej kopercie z odpowiednim dopiskiem, np. Zmiana oferty przetargowej.

Ofertę złożoną po terminie zwraca się w terminie określonym w art. 84 ust. 2 Ustawy Pzp.

Wykonawca ponosi koszty związane z przygotowaniem i złożeniem oferty. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, której wykonanie zamierza powierzyć podwykonawcy.

Postanowienia dotyczące wnoszenia oferty wspólnej przez dwa lub więcej podmioty gospodarcze (konsorcja/spółki cywilne):

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
2. Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy, a pełnomocnictwo/ upoważnienie do pełnienia takiej funkcji wystawione zgodnie z wymogami ustawowymi, podpisane przez prawnie upoważnionych przedstawicieli każdego z wykonawców występujących wspólnie należy załączyć do oferty.
3. Oferta winna być podpisana przez każdego z wykonawców występujących wspólnie lub przez upoważnionego przedstawiciela.

**XIV. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT**

1. Składanie ofert.
2. Miejscem składania ofert jest siedziba Zamawiającego.
3. Oferty należy składać we wskazanym powyżej miejscu lub przesłać pocztą na adres Zamawiającego z wyraźnym oznaczeniem postępowania.
4. Termin składania ofert upływa dnia **22.10.2019 roku o godz. 10:00**
5. Termin związania ofertą wynosi 30 dni licząc od upływu terminu składania ofert.
6. Otwarcie ofert.
7. Oferty zostaną otwarte w dniu **22.10. 2019 roku o godz. 10:30** w budynku Zamawiającego przy ul. Staromłyńskiej 1 w Szczecinie, pok. 18.
8. Otwarcie ofert jest jawne.

**XV. OPIS SPOSOBU OBLICZENIA CENY**

1. Cena oferty musi być wyrażona w złotych polskich (PLN).
2. Zamawiający wymaga, aby Wykonawca wypełnił formularz ofertowy - załącznik nr 2 do SIWZ i Załącznik nr 3 do SIWZ: formularz cenowo - przedmiotowy.
3. Cenę oferty należy skalkulować (obliczyć) odrębnie
4. Przy obliczaniu ceny należy zastosować wzór:

wartość netto + kwota podatku VAT = wartość brutto.

1. Cena oferty musi zawierać należny podatek VAT zgodnie z ustawą z dnia 11 marca 2004r. o podatku od towarów i usług (tekst jednolity Dz. U. z 2011r. Nr 177, poz. 1054 z późn. zm.) z zastrzeżeniem pkt 5 niniejszego rozdziału, wszystkie przewidywane koszty kompletnego wykonania przedmiotu zamówienia, musi uwzględniać wymagania SIWZ oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia. Skutki finansowe jakichkolwiek błędów obciążają Wykonawcę, który musi przewidzieć wszystkie okoliczności mogące mieć wpływ na cenę zamówienia.
2. W sytuacji gdy Wykonawca składa ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając taką ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadził 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, oświadczenie wpisane na druku załącznika nr 2 do SIWZ - formularz ofertowy. W przypadku ubiegania się o udzielnie zamówienia przez wykonawców krajowych i zagranicznych sposób złożenia oferty cenowej uzależniony jest od siedziby lub miejsca zamieszkania pełnomocnika (ustanowionego przez wykonawców wspólnie ubiegających się o udzielenie zamówienia), zobowiązanego do wystawiania faktury należnej z tytułu wykonania umowy (tj. pełnomocnik mający siedzibę lub miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej zgodnie z wymaganiami dla wykonawców krajowych; poza terytorium Rzeczypospolitej Polskiej - zgodnie z wymaganiami dla wykonawców zagranicznych).
3. Wykonawcy zobowiązani są do zaokrąglenia cen do pełnych groszy, czyli do dwóch miejsc po przecinku, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 grosza i wyższe zaokrągla się do 1 grosza.
4. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
5. Wykonawca w przedstawionej ofercie winien zaoferować ceny jednoznaczne. Podanie ceny wariantowej wyrażonej w „widełkach cenowych” lub zawierającej warunki i zastrzeżenia spowoduje odrzucenie oferty.
6. Cena oferty nie podlega negocjacjom.
7. Wszystkie poprawki w obliczeniach, dokonane ręcznie (niedopuszczalne jest użycie korektora) poprzez przekreślenie poprzedniego zapisu w sposób umożliwiający jego odczytanie winny być parafowane własnoręcznie zgodnie ze statusem prawnym Wykonawcy, czyli przez osobę(y) podpisującą(e) ofertę.

**XVI. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY,**

1. Złożone oferty niepodlegające odrzuceniu na podstawie art. 89 Ustawy Pzp oraz złożone przez Wykonawców niewykluczonych z postępowania na podstawie art. 24 Ustawy Pzp, będą oceniane przez Zamawiającego przy zastosowaniu następujących kryteriów:

1) cena – 60 %

2) termin wykonania zamówienia – 10%

2) deklaracja wykonawcy o posiadaniu autoryzacji producenta dostarczonych przełączników sieciowych jeżeli wykonawca posiada – 30 %

Ad.1) **Cena wykonania zamówienia** – obejmuje cenę brutto wykonania przedmiotu zamówienia określonego w niniejszej SIWZ. Oferta z najniższą ceną otrzyma maksymalną ilość punktów = 60 pkt, oferty następne będą oceniane na zasadzie proporcji w stosunku do oferty najtańszej wg wzoru:

 najniższa cena ofertowa

 C = ------------------------------------------------ x 100 pkt x 60%

 cena ofertowa w ofercie ocenianej

Uzyskana z wyliczenia ilość punktów zostanie ostatecznie ustalona z dokładnością do drugiego miejsca po przecinku z zachowaniem zasady zaokrągleń matematycznych.

Ad.2) **Termin wykonania zamówienia (T)** - W niniejszym kryterium można zdobyć maksymalnie 10 pkt. Oceniany będzie okres skrócenia czasu wykonania zamówienia. Wykonawcy w treści formularza ofertowego wskazują termin, w jakim zrealizują niniejsze zamówienie. Zamawiający obliczy ilość dni, o jakie został skrócony termin wykonania zamówienia i przyzna punkty według następującego wzoru.

 najkrótszy zaoferowany termin dostawy spośród ofert nieodrzuconych

 T = ----------------------------------------------------------------------------------------------- x 100 pkt x 10%

 termin dostawy oferty badanej

gdzie:

T - wartość punktowa w kryterium „termin dostawy”

Termin - najkrótszy zaoferowany termin dostawy spośród ofert nie odrzuconych

Tb - termin dostawy oferty badanej

Wykonawca zobowiązany jest do wyrażenia terminu dostawy w dniach. Jednak termin dostawy nie może być krótszy niż 25 dni oraz nie dłuższy niż 35 dni od daty podpisania umowy. W przypadku zaoferowania terminu krótszego niż 25 dni od daty podpisania umowy, Zamawiający do wyliczenia punktów w niniejszym kryterium przyjmie termin 25 dni, w przypadku terminu dłuższego niż 35 dni nastąpi odrzucenie oferty.

Ad.3) **Deklaracja wykonawcy o posiadaniu autoryzacji producenta dostarczonych przełączników sieciowych jeżeli wykonawca posiada (D)** – w niniejszym kryterium można zdobyć 30 pkt. Ocenie podlegać będzie czy do oferty Wykonawca dołączy pisemne oświadczenie o posiadaniu autoryzacji producenta dostarczanych przełączników sieciowych. Oświadczenie winno być podpisane przez osobę która podpisała ofertę.

 Wykonawca który do oferty dołączy w/w pisemne oświadczenie otrzyma 30 pkt.

 Wykonawca który do oferty nie dołączy w/w oświadczenia otrzyma 0 pkt

Każdy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku. Jako najkorzystniejsza wybrana zostanie oferta, która uzyska łącznie najwyższą liczbę punktów.

**Końcowa liczba otrzymanych punktów będzie sumą punktów otrzymanych przez ofertę zgodnie ze wzorem:**

**Suma punktów = C+D**

1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom przedstawionym w Ustawie Pzp oraz w SIWZ i została oceniona jako najkorzystniejsza, tj. uzyskała największą ilość punktów na podstawie przyjętych kryteriów oceny ofert (art.91 ust.1 Ustawy Pzp).

**XVII. ZAWIADOMIENIE O WYBORZE NAJKORZYSTNIEJSZEJ OFERTY**

1. Niezwłocznie, po wyborze najkorzystniejszej oferty Zamawiający jednocześnie zawiadamia Wykonawców, którzy złożyli oferty o:
2. wyborze najkorzystniejszej oferty, podając nazwę (firmę) albo imię i nazwisko, siedzibę albo miejsce zamieszkania adres Wykonawcy, którego ofertę wybrano, uzasadnienie jej wyboru, a także nazwy (firmy) albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy Wykonawców, którzy złożyli oferty a także punktację przyznaną ofertom podczas oceny,
3. wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne,
4. wykonawcach, którzy zostali wykluczeni z postępowania o udzielenie zamówienia, podając uzasadnienie faktyczne i prawne,
5. terminie, określonym zgodnie z art. 94 ust. 1 lub 2 Ustawy Pzp, po którego upływie umowa w sprawie zamówienia publicznego będzie zawarta.
6. Informacje o których mowa powyżej, zostaną zamieszczone również na stronie internetowej Zamawiającego oraz na tablicy ogłoszeń w siedzibie Zamawiającego.

**XVIII. UNIEWAŻNIENIE POSTĘPOWANIA**

1. Zamawiający może unieważnić postępowanie w przypadkach określonych w art. 93 Ustawy Pzp.
2. W zawiadomieniu o unieważnieniu postępowania Zamawiający poda przyczyny faktyczne i prawne unieważnienia. Zawiadomienie zostanie przesłane wszystkim Wykonawcom, którzy ubiegali się o udzielenie zamówienia lub złożyli oferty oraz umieszczone na stronie internetowej Zamawiającego.

**XIX. INFORMACJE O FORMALNOSCIACH JAKIE NALEŻY DOPEŁNIĆ PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY.**

1. Zamawiający udzieli zamówienia Wykonawcy, który wykazał spełnianie warunków udziału w postępowaniu i przedstawił najkorzystniejszą ofertę zgodnie z kryterium oceny ofert,
2. wyborze oferty Zamawiający zawiadomi niezwłocznie Wykonawców, którzy ubiegali się o udzielenie zamówienia oraz informacje o powyższym zamieści na stronie internetowej,
3. Zamawiający poinformuje Wykonawcę, którego oferta zostanie uznana za najkorzystniejszą o miejscu i terminie podpisania umowy. Termin ten nie może być krótszy niż 5 dni od dnia przekazania zawiadomienia o wyborze oferty. – z zastrzeżeniem art. 94 Ustawy Pzp,
4. W przypadku, gdy zostanie wybrana jako najkorzystniejsza oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Wykonawca przed podpisaniem umowy na wezwanie Zamawiającego przedłoży umowę regulującą współpracę Wykonawców, w której m.in. zostanie określony pełnomocnik uprawniony do kontaktów z Zamawiającym oraz do wystawiania dokumentów związanych z płatnościami.
5. terminie złożenia dokumentu, o którym mowa w pkt 4. Zamawiający powiadomi Wykonawcę odrębnym pismem.
6. Osoby reprezentujące Wykonawcę przy podpisaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
7. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.
8. Przed zawarciem umowy Wykonawca zobowiązany jest wnieść kwotę zabezpieczenia należytego wykonania umowy.

 **XX. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY**

1. Zamawiający ustala zabezpieczenie należytego wykonania umowy w wysokości 10% ceny całkowitej oferty brutto. Należną kwotę zabezpieczenia Wykonawca zobowiązany będzie wnieść w całości przed zawarciem umowy.
2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy oraz roszczeń z tytułu rękojmi za wady.
3. Zabezpieczenie może być wnoszone według wyboru wykonawcy w jednej lub w kilku następujących formach:
4. pieniądzu;
5. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
6. gwarancjach bankowych;
7. gwarancjach ubezpieczeniowych;
8. poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
9. Zabezpieczenie wnoszone w pieniądzu Wykonawca wpłaci przelewem na rachunek bankowy Zamawiającego: Bank Gospodarstwa Krajowego, oddział Szczecin:

 68 1130 1176 0022 2063 6520 0004

1. Jeżeli zabezpieczenie wniesiono w pieniądzu, Zamawiający przechowa je na oprocentowanym rachunku bankowym. Zamawiający zwróci zabezpieczenie wniesione w pieniądzu wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.
2. W trakcie realizacji umowy Wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w pkt. 3.
3. Zamawiający zwróci 70% wniesionego zabezpieczenia w terminie 30 dni od dnia wykonania całości zamówienia i uznania przez Zamawiającego wszystkich prac za należycie wykonane.
4. Kwota pozostawiona na zabezpieczenie roszczeń z tytułu udzielonej gwarancji wynosić będzie 30% wysokości zabezpieczenia i zostanie zwrócona Wykonawcy nie później niż w 15 dniu po upływie okresu gwarancji jednak nie później niż 60 miesięcy po odbiorze całego zadania.
5. Jeżeli zabezpieczenie zostanie wniesione w formie niepieniężnej, to celowym będzie aby Wykonawca ustanowił zabezpieczenie w jednym dokumencie gwarancyjnym następująco (zabezpieczenie redukowalne) :
6. kwota zabezpieczenia podzielona na dwie części odpowiednio dla terminu zakończenia realizacji zamówienia plus 30 dni oraz dla terminu udzielonej w ramach niniejszego zamówienia gwarancji + 15 dni:
7. pierwsza część w wysokości 100 % kwoty wymienionej w pkt. 1 na okres od dnia zawarcia umowy do zakończenia realizacji zamówienia + 30 dni,
8. druga część w wysokości 30 % (po pomniejszeniu o 70 % zgodnie z pkt. 9 niniejszego rozdziału) kwoty wymienionej w pkt. 1 na okres od dnia zawarcia umowy do końca okresu odpowiedzialności wykonawcy z tytułu gwarancji plus 15 dni.
9. W przypadku dokonania zmiany terminu wykonania zamówienia, Wykonawca będzie zobowiązany do przedłużenia ważności odpowiednich części zabezpieczenia o okres, o jaki przedłużono termin wykonania zamówienia,
10. W przypadku niewykonania czynności przewidzianych w pkt. 10 Zamawiający będzie uprawniony do zatrzymania należnego Wykonawcy wynagrodzenia równego kwocie zabezpieczenia na pokrycie ewentualnych roszczeń z tytułu niewykonania lub nienależytego wykonania zobowiązania.

**XXI. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA**

1) Środki ochrony prawnej (Odwołanie, Skarga do Sądu) w niniejszym postępowaniu przysługują wykonawcom, a także innym podmiotom, jeżeli mają lub miały interes w uzyskaniu niniejszego zamówienia lub poniosły lub mogą ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy Prawo zamówień publicznych.

2) Wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia środki ochrony prawnej przysługują również organizacjom wpisanym na listę organizacji uprawnionych do wnoszenia środków ochrony prawnej prowadzoną przez Prezesa Urzędu Zamówień Publicznych.

3) Odwołanie przysługuje wyłącznie wobec czynności:

1. wyboru trybu negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę;
2. określenia warunków udziału w postępowaniu;
3. wykluczenia odwołującego z postępowania o udzielenie zamówienia;
4. odrzucenia oferty odwołującego;
5. opisu przedmiotu zamówienia;
6. wyboru najkorzystniejszej oferty.

4) W przypadku:

1. **niezgodnej z przepisami ustawy czynności podjętej przez zamawiającego w postępowaniu o udzielenie zamówienia, lub**
2. **zaniechania czynności, do której zamawiający jest zobowiązany na podstawie ustawy, na które nie przysługuje w niniejszym postępowaniu odwołanie**

wykonawca może w terminie przewidzianym do wniesienia odwołania poinformować o nich zamawiającego. W przypadku uznania zasadności przekazanej informacji zamawiający powtórzy czynność albo dokona czynności zaniechanej, informując o tym wykonawców.

5) Odwołanie powinno wskazywać czynność lub zaniechanie czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.

6) Odwołanie wnosi się w terminie:

1. **5 dni od dnia przesłania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli zostało ono przesłane przy użyciu środków komunikacji elektronicznej, lub**
2. **10 dni od dnia przesłania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli zostało ono przesłane winny sposób niż określono w ppkt. 1),**

7) Odwołanie wobec treści ogłoszenia o zamówieniu lub wobec postanowień specyfikacji istotnych warunków zamówienia, wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub specyfikacji istotnych warunków zamówienia na stronie internetowej zamawiającego.

8) Odwołanie wobec czynności innych niż określone w pkt. 6, 7 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

9) Jeżeli zamawiający mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze oferty najkorzystniejszej odwołanie wnosi się nie później niż w terminie:

1. 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych**.**
2. 1 miesiąca od dnia zawarcia umowy, jeżeli zamawiający:
* nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o udzieleniu zamówienia; albo
* zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o udzieleniu zamówienia, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia, zamówienia z wolnej ręki albo zapytania o cen

10) Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo elektronicznej podpisane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocą ważnego kwalifikowanego certyfikatu lub równoważnego środka, spełniającego wymagania dla tego rodzaju podpisu.

11) Odwołujący przesyła kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Przesłanie kopii odwołania może nastąpić pisemnie, faksem lub drogą elektroniczną.

12) Brak przekazania zamawiającemu kopii odwołania, w sposób oraz w terminie określonym powyżej, stanowi jedną z przesłanek odrzucenia odwołania przez Krajową Izbę Odwoławczą.

13) W przypadku wniesienia odwołania wobec treści ogłoszenia o zamówieniu lub postanowień specyfikacji istotnych warunków zamówienia zamawiający może przedłużyć termin składania ofert.

14) W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.

15) Jeżeli koniec terminu do wykonania czynności przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następnego po dniu lub dniach wolnych od pracy

16) Kopię odwołania zamawiający:

1. **przekaże niezwłocznie innym wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia,**
2. **zamieści również na stronie internetowej, jeżeli odwołanie dotyczy treści ogłoszenia o zamówieniu lub postanowień specyfikacji istotnych warunków zamówienia, wzywając wykonawców do przystąpienia do postępowania odwoławczego.**

17) Odwołanie podlegać będzie rozpoznaniu przez Krajową Izbę Odwoławczą, jeżeli nie zawiera braków formalnych oraz uiszczono wpis od odwołania.

18) Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do Sądu.

1. Pozostałe informacje dotyczące środków ochrony prawnej znajdują się w Dziale VI. "Środki ochrony prawnej", art. od 179 do 198 ustawy Pzp.

**XXII. POSTANOWIENIA KOŃCOWE**

1. Uczestnicy postępowania mają prawo wglądu do treści protokołu postępowania, ofert od chwili ich otwarcia, w trakcie prowadzonego postępowania, za wyjątkiem dokumentów stanowiących załączniki do protokołu (jawne po zakończeniu postępowania) oraz stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji zastrzeżonych przez uczestników postępowania.

2. Załącznikami do protokołu postępowania są w szczególności: oferty, opinie biegłych, oświadczenia, zawiadomienia, wnioski, inne dokumenty i informacje składane przez zamawiającego i wykonawców oraz umowa w sprawie zamówienia publicznego.

3. Udostępnienie dokumentów odbywać się będzie wg poniższych zasad:

1. zamawiający udostępnia wskazane dokumenty na wniosek,
2. przekazanie protokołu lub załączników następuje przy użyciu środków komunikacji elektronicznej.

4. W przypadku protokołu lub załączników sporządzonych w postaci papierowej, jeżeli z przyczyn technicznych znacząco utrudnione jest udostępnienie tych dokumentów przy użyciu środków komunikacji elektronicznej, w szczególności z uwagi na ilość żądanych do udostępnienia dokumentów, zamawiający wskaże inny sposób, w jaki mogą być one udostępnione.

5. W sprawach nieuregulowanych zastosowanie mają przepisy Ustawy Prawo zamówień publicznych oraz Rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie protokołu postępowania o udzielenie zamówienia publicznego (Dz. U. z 2016 poz. 1128).

6. E-faktury. W przypadku przesyłania przez wykonawcę ustrukturyzowanych faktur elektronicznych, Zamawiający będzie je odbierał za pomocą adresu, przekazanego Wykonawcy najpóźniej do dnia odbioru końcowego niniejszego zamówienia.

7. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

1. administratorem Pani/Pana danych osobowych jest Muzeum Narodowe w Szczecinie z siedzibą przy ul. Staromłyńskiej 27 w Szczecinie, wpisanym do rejestru Instytucji Kultury Województwa Zachodniopomorskiego pod nr. 2/99/WZ, dla której organizatorem jest Samorząd Województwa Zachodniopomorskiego oraz Minister Kultury i Dziedzictwa Narodowego.
2. inspektorem ochrony danych osobowych w Muzeum Narodowym w Szczecinie jest Pan: Michał Dłużak, m.dluzak@muzeum.szczecin.pl;
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego.
4. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp”.
5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy.
6. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp.
7. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8. posiada Pani/Pan:
9. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
10. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych.
11. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO.
12. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
13. nie przysługuje Pani/Panu:
	1. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych, prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
	2. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

**XXIII. KATALOG ZMIAN UMOWY**

1. Zmiana postanowień umowy może nastąpić wyłącznie za zgodą obu Stron oraz w przypadkach określonych w pkt 2, wyrażoną w formie pisemnego aneksu pod rygorem nieważności, z zastrzeżeniem zawartym w pkt 4.

2. Zmiany umowy mogą zostać dokonane w następujących okolicznościach i w następującym zakresie:

1. Zmian ogólnie obowiązujących przepisów prawa powszechnego i/lub miejscowego oraz wymogów dotyczących zamawiającego bezpośrednio odnoszących się do praw i obowiązków stron umowy; zmiany umowy z tego tytułu dokonane mogą być tylko w zakresie niezbędnym do stosowania zapisów umowy do wprowadzonych przepisów,
2. Zmian w terminie realizacji przedmiotu umowy, jeżeli ulegnie on przesunięciu o czas występowania przeszkód o obiektywnym, nadzwyczajnym i niemożliwym do przewidzenia charakterze, w szczególności takim jak niedobory rynkowe, przedłużający się czas dostawy u producenta, itp.
3. Zmian w terminie realizacji przedmiotu umowy, z przyczyn leżących po stronie Zamawiającego, w szczególności wstrzymania terminu dostawy bądź niemożliwości realizacji umowy w wyniku działań osób trzecich.
4. Zmian w zakresie poszczególnych elementów zamówienia, jeżeli w okresie realizacji zamówienia, na rynku pojawi się nowy produkt o parametrach lepszych od zaoferowanego elementu, a zmiana taka zostanie uzgodniona z Zamawiającym i nie wpłynie ona na wartość zamówienia. W takim przypadku ulec może również zmianie termin dostawy.
5. aktualizacji rozwiązań ze względu na postęp techniczny lub technologiczny (np. wycofanie z obrotu urządzeń lub podzespołów), zmiana nie może spowodować podwyższenia ceny oraz obniżenia parametrów technicznych, jakościowych i innych wynikających z oferty. W takim przypadku ulec może również zmianie termin dostawy.
6. Rezygnacji z części zamówienia w przypadku, gdy uzyskanie określonego elementu nie leży już w interesie Zamawiającego bądź występują problemy na rynku z uzyskaniem tego elementu. W takim przypadku wynagrodzenie wykonawcy zostanie odpowiednio pomniejszone o wartość tego elementu.
7. zmiany związane ze zmianami prawa dotyczącego ochrony danych osobowych

Ustała się, iż nie stanowi zmiany umowy w rozumieniu art. 144 ustawy:

1. zmiana nr rachunku bankowego,
2. zmiana osób wyznaczonych do nadzoru nad realizacją umowy,
3. zmiana danych teleadresowych,

Zaistnienie okoliczności, o których mowa w niniejszym punkcie wymaga jedynie niezwłocznego pisemnego zawiadomienia drugiej strony.

**Załącznik nr 1 – Opis przedmiotu zamówienia - OPZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

* + - 1. **PRZEDMIOT ZAMÓWIENIA:**

Przedmiotem zamówienia jest **Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie** a w szczególności:

|  |  |
| --- | --- |
| **Nazwa** | **ilość** |
| Serwer typu RACK | 2  |
| Macierz dyskowa  | 1  |
| Napęd taśmowy LTO | 1  |
| UTM | 1  |
| Oprogramowanie do backupu | 1 |
| System operacyjny serwera | 2  |
| Szafa dystrybucyjna  | 1 |
| Zasilacz awaryjny do szafy serwerowej | 1 |
| Przełacznik sieciowy dystrybucyjny z funkcją PoE | 1 |
| KVM | 1 |
| Listwa PDU | 2 |
| Przełącznik sieciowy szkieletowy | 1 |
| Taśmy LTO  | 20 |

**2.** **OPIS ISTNIEJĄCEJ INFRASTRUKTURY W MUZEUM NARODOWYM W SZCZECINIE**

Sieć w systemie teleinformatycznym pomiędzy główną serwerownią a budynkami zależnymi oparta jest na szyfrowanych połączeniach na rozwiązaniach firmy Fortinet. Wszystkie serwery zadaniowe są zwirtualizowane i działają na hostach opartych o środowisko Microsoft Windows Hyper-V w klastrach HA.

Serwery wirtualne działają w środowisku Windows Serwer, pod kontrolą środowiska Active Directory, które jest odpowiedzialne za autoryzację elementów systemu i użytkowników, dostęp do zasobów oraz dostarcza spójnej polityki bezpieczeństwa serwerom i pozostałym urządzeniom w sieci.

Stacje robocze są ustandaryzowane, co oznacza, iż na wszystkich jest utrzymywana jednolita wersja systemu operacyjnego Windows 10 Professional, co zapewnia spójną politykę zarządzania systemami, jednolity pakiet biurowy MS Office w wersji 2016, co zapewnia pełną zgodność przy przenoszeniu dokumentów pomiędzy elementami systemu, jednolite zarządzane środowisko antywirusowe oparte o rozwiązanie Eset, co zapewnia odpowiednią, scentralizowaną kontrolę nad systemem, system Musnet do katalogowania i zarządzania zbiorami Muzeum, potrafiący pracować tylko w środowisku Windows.

W celu utrzymania spójnego i jednolitego środowiska dla wszystkich aplikacji posiadanych przez Muzeum Narodowe w Szczecinie wymaga się pełnej kompatybilności oferowanego sprzętu z infrastrukturą już posiadaną.

**2. WYMAGANIA OGÓLNE**

 W ramach zakupu wymaga się od Wykonawcy następująco:

1. Wszystkie urządzenia winny być fabrycznie nowe, nieużywane, kompletne, gotowe do pracy oraz wyprodukowane nie wcześniej niż w 2018 r.;
2. Dostarczone poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.
3. Licencje udzielane przez producenta powinny być nieograniczone czasowo, niewyłączne, , do wykorzystania na terenie Polski w tym obejmować co najmniej następujące pola eksploatacji: utrwalanie na dowolnym nośniku, zwielokrotniania dowolną techniką, wprowadzania do pamięci urządzenia, udostępniania w sieci Internet i innych sieciach komputerowych (publiczne udostępnianie Oprogramowania w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym)
4. Wszystkie urządzenia winny być dostarczone w oryginalnych opakowaniach producenta;
5. Zamawiający zastrzega prawo usunięcia opakowań. Opakowania nie będą wymagane do utrzymania warunków gwarancji;
6. Sprzęt winien być dopuszczony do obrotu i użytkowania na terenie UE, czego potwierdzeniem winna być deklaracja zgodności producenta, oraz oznakowanie CE,
7. Sprzęt winien być identyfikowalny poprzez unikalny numer seryjny lub w inny sposób przewidziany przez producenta,
8. Wszystkie zamówione urządzenia należy dostarczyć do siedziby Zamawiającego tj. ul. Staromłyńska 27 lub Wały Chrobrego 3 – do ustalenia przy dostawie;
9. Wykonawca powiadomi o godzinie dostawy Zamawiającego co najmniej 1 dzień przed dostawą w formie pisemnej na adres mailowy r.piatkowski@muzeum.szczecin.pl
10. Dostawa urządzeń odbędzie się w dni robocze pomiędzy godziną 9:00 a 14:00;
11. Podczas dostarczania i odbioru urządzeń do siedziby Zamawiającego winien być obecny przedstawiciel Wykonawcy upoważniony do podpisania protokołu odbioru;
12. Zamawiający po dostawie przed podpisaniem odbioru ma zagwarantowane prawo do włączenia każdego urządzenia, sprawdzenia jego parametrów, sprawdzenia sterowników oraz funkcjonalności i wersji oprogramowania układowego;
13. Przed podpisaniem protokołu odbioru Wykonawca dostarczy:
14. licencje wymagane w OPZ przy danym urządzeniu
15. instrukcje obsługi w języku polskim,
16. dokumenty potwierdzające udzielenie gwarancji
17. certyfikaty CE
18. oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – dotyczy serwera typu RACK oraz macierzy dyskowej
19. Oświadczeń Wykonawcy potwierdzonego, że naprawy gwarancyjne będą realizowane przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta – dotyczy serwerów, UTM oraz macierzy
20. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzacje producenta w zakresie sprzedaży oferowanych rozwiązań- dotyczy UTM
21. Oświadczenie producenta oferowanego urządzenia potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta – serwer typu Rack, macierz dyskowa, przełączniki sieciowe
22. Wykonawca dostarczy wydruk ze strony www.cpubenchmark.net z datą pomiędzy podpisaniem umowy a dostawą urządzeń, świadczący o osiągach dostarczonych procesorów.
23. Dostarczone urządzenia winny mieć wgrane najnowsze dostępne sterowniki producentów komponentów urządzenia;
24. Dostarczone urządzenia winny mieć wgraną najnowszą dostępną wersją oprogramowania układowego;
25. Dostarczane urządzenia winny mieć najnowszą wersję systemu operacyjnego, z zainstalowanymi wszystkimi poprawkami wydanymi do daty co najwyżej trzech miesięcy wstecz od daty dostawy urządzeń;
26. Poza standardowymi składnikami systemu operacyjnego oraz oprogramowaniem producenta do aktualizacji sterowników i diagnostyki urządzenia zabrania się instalacji jakiegokolwiek oprogramowania dodatkowego, w tym oprogramowania antywirusowego firm trzecich w jakiejkolwiek wersji, instalacji pakietów biurowych oraz instalatorów pakietów biurowych, wszelakiego typu gier;
27. Otwarcie obudowy urządzenia nie ma wpływu na gwarancje;
28. Montaż rozszerzenia urządzeń przez Zamawiającego, takiego jak dodatkowa pamięć RAM, dodatkowy dysk czy standardowa karta rozszerzeń nie powoduje utraty gwarancji na urządzenie;
29. Za uszkodzoną matrycę podlegającą naprawie gwarancyjnej przyjmuje się uszkodzenie co najmniej jednego piksela (tak zwanego martwego piksela) w urządzeniu KVM oraz w panelach LCD urządzeń
30. Dostarczone licencje muszą być zgodnie z polityką producenta w taki sposób, aby Muzeum mogło legalnie korzystać z danego oprogramowania;
31. Zamawiający zobowiązuje Wykonawcę do przeprowadzenia instruktażu w zakresie konfiguracji i użytkowania danych urządzeń w ciągu 12 miesięcy od realizacji zamówienia w terminie obustronnie uzgodnionym
32. Jeżeli gdziekolwiek w opisie przedmiotu wystąpiło jakiekolwiek odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, nazw marek czy technologii, należy to traktować jako informację na temat oczekiwanego standardu i poziomu jakości, a nie ściśle jako wyrób konieczny do użycia. Zamawiający dopuszcza rozwiązania równoważne, co oznacza, iż możliwe jest zastosowanie innych równoważnych wyrobów i technologii, których zastosowanie zagwarantuje spełnienie warunków podstawowych;
33. Wykonawca zobowiązany jest do jednoznacznego określenia zaoferowanego w ofercie produktu, charakteryzując go poprzez wskazanie na konkretny wyrób (producent, model).
34. Wymagany okres udzielonej gwarancji i szczegóły dotyczące warunków gwarancji i świadczeń gwarancyjnych zawarte są w poszczególnych Specyfikacjach technicznych ( Załącznik nr 1 opis przedmiotu zamówienia).

3. Wymagania szczegółowe – wg Specyfikacji technicznych:

 **Specyfikacja techniczna nr 1 – Serwer typu RACK – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Utrzymanie wirtualnych serwerów (system oparty na bazie danych MySQL z zawartością 500 000 rekordów, pomocniczy kontroler domeny, DNS, dysk sieciowy) w środowisku Microsoft Windows Hyper-V na potrzeby procesów digitalizacyjnych opartych na klastrze utworzonym na podstawie systemu Windows DataCenter. Każdy z serwerów będzie podłączony za pomocą dwóch przyłączy światłowodowych do oferowanego szkieletowego przełącznika sieciowego oraz za pomocą dwóch kabli FC do oferowanej macierzy dyskowej. |
|  | Obudowa | Maksymalnie 2U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack) |
|  | Płyta Głowna | Dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera, oznaczona jego znakiem firmowym z możliwością zainstalowania dwóch procesorów.Co najmniej 3 sloty generacji 3 o prędkości x8 oraz 2 sloty generacji 3 o prędkości x16 |
|  | Chipset | Dedykowany przez producenta procesora do pracy w serwerach co najmniej dwuprocesorowych. |
|  | Procesor | Zainstalowane dwa procesory ośmio-rdzeniowe x86 – 64 bity, dedykowane do pracy z zaoferowanym serwerem, każdy osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 11500 punktów. Wynik testu musi być opublikowany na stronie www.cpubenchmark.netSuma rdzeni fizycznych obu procesorów nie może być większa niż 16. |
|  | Pamięć RAM |  128 GB RDIMM DDR4 2666 MT/s.Minimum 15 wolnych slotów na rozbudowę pamięć.Możliwość rozbudowy pamięci do co najmniej 1TB. |
|  | Interfejsy sieciowe/FC/SAS | Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz co najmniej 2 interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+ lub BaseT wraz z dwoma modułami nadawczo-odbiorczymi 10GbE SFP+ SR. Zainstalowana co najmniej jedna karta dwuportowa FC 16Gb/s. |
|  | Napęd optyczny | Wbudowany napęd co najmniej DVD. |
|  | Dysk | Co najmniej 2 dyski w technologii SSD minimum 120 GB Hot Plug montowane z przodu obudowy,Co najmniej 4 wolne zatoki do instalacji kolejnych dysków typu: Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy |
|  | Kontroler RAID | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów co najmniej RAID: 0, 1, 5, 10, 50. |
|  | Porty | Co najmniej 1 x VGA,Co najmniej 3 porty USB co najmniej 3.0,Co najmniej 2 porty USB co najmniej 2.0, |
|  | Karta Graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1280x1024. |
|  | Wentylatory | Zestaw wentylatorów redundantnych typu hot-plug. |
|  | Zasilacze | Co najmniej 2 szt., typu Hot-plug, redundantne, każdy o mocy wystarczającej do zasilania oferowanego sprzętu. |
|  | Karta Zarządzania | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe
* Możliwość zdalnego włączenia / wyłączenia oraz restartu serwera
* wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
* dostęp do karty zarządzającej poprzez
	+ dedykowany port RJ45 z tyłu serwera

 dostęp do karty możliwy * + z poziomu przeglądarki webowej (GUI)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer
* zdalna aktualizacja oprogramowania (firmware)
* możliwość równoczesnej obsługi przez co najmniej 2 administratorów
* wsparcie dla autoryzacji elementów systemu i użytkowników oraz dostępu do zasobów stosowanego w Muzeum Narodowym w Szczecinie systemu opisanego w załączniku nr 1
* obsługa SSL i SSH
* wsparcie dla co najmniej IPv4
 |
|  | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-14001. Serwer musi posiadać deklaracja CE.Z uwagi na opisaną w załączniku nr 1 infrastrukturę istniejącą i stosowaną w Muzeum Narodowym w Szczecinie oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów co najmniej Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016. |
| 1. 10.
 | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Z uwagi na opisaną w załączniku nr 1 infrastrukturę istniejącą i stosowaną w Muzeum Narodowym w Szczecinie : Microsoft Windows Server 2012 R2, 2016, 2019Microsoft Hyper-V Server 2012 R2, 2016, 2019 |
| 1. 11.
 | Inne | Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski. |
| 1. 12.
 | Gwarancja | Co najmniej 3 lata. Wsparcie serwisowe producenta serwera, w miejscu instalacji, z czasem reakcji w następnym dniu roboczym, okno zgłoszeniowe 9/5 świadczony przez polski oddział serwisowy producenta serwera.Wszystkie dyski uszkodzone w okresie trwania wsparcia serwisowego nie wymagają zwrotu po wymianie na sprawne.Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania układowego oraz sterowników.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wadyOświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisie – **przed podpisaniem protokołu odbioru** |
|  | Akcesoria | Zestaw kabli umożliwiających podłączenie urządzenia do listw PDU,Patchcord do podłączenia sieci monitoringu do sieci LAN co najmniej 5 metrów, Komplet śrub i akcesoriów wymagany do instalacji urządzenia w szafie RACK,Kable FC wymagane do redundantnego podłączenia serwera do macierzy.  |

 **Specyfikacja techniczna nr 2 – Macierz dyskowa – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Obsługa dysków wirtualnych serwerów w istniejącym w Muzeum Narodowym w Szczecinie systemie opisanym w załączniku nr 1 dla maszyn wirtualnych oraz przestrzeń na dane robocze i archiwalne. |
|  | Obudowa | Obudowa umożliwiająca zamontowanie macierzy w systemie RACK w dostarczonej szafie serwerowej, o maksymalnej wysokości 5U. Załączone wszystkie elementy montażowe konieczne do prawidłowego zamocowania macierzy zgodnie z wytycznymi producenta. W obudowie winny być zainstalowane co najmniej dwa kontrolery macierzowe redundantne |
|  | Przestrzeń dyskowa | Macierz musi być wyposażona w co najmniej 1920GB powierzchni w technologii SSD w systemie raid 1-0 oraz 78TB powierzchni w technologii co najmniej NLSASPowierzchnia jest podana jako surowa - RAW przed formatowaniem. |
|  | Pamięć podręczna | Pamięć podręczna (cache) – co najmniej 16 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie co najmniej 32 GB).  Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. |
|  | Interfejsy zewnętrzne | Macierz musi być wyposażona w co najmniej: 8 portów FC 16Gb/s oraz 8 portów 10 GbE SFP+, 2 porty zarządzające 1GbE Base-T, każdy kontroler macierzy w trybie Active-Active. |
|  | Dostępność | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).Możliwość łączenia w macierzy różnych poziomów RAID, co najmniej: - możliwość zastosowania RAID10- możliwość zastosowania RAID5,- możliwość zastosowania RAID6- możliwość zastosowania RAID0- możliwość zastosowania RAID1Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych.Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).Możliwość zdefiniowania co najmniej 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa.Możliwość obsługi wirtualnych portów (NPIV) w taki sposób, aby awaria fizycznego portu nie powodowała konieczności przełączania ścieżek poprzez oprogramowanie do multipathing |
|  | Wspierane systemy operacyjne | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej MS Windows oraz Linux, Vmware,Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server, HACMP, HP Serviceguard.Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych co najmniej: AIX, HP-UX, MS Windows, Vmware, Linux.Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning |
|  | Skalowalność | Wykonywanie rozbudowy sprzętowej w trybie online.Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash.Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej.Macierz musi umożliwiać rozbudowę o moduły co najmniej 12 dysków 3,5” , co najmniej 24 dyski 2,5”Obsługa ci najmniej 200 dysków SAS/NLSAS lub SSD |
|  | Zarządzanie | Oprogramowanie do zarządzania macierzą przez administratora klienta winno posiadać graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).Stałe monitorowanie macierzy przez zdalne centrum serwisowe, bez konieczności instalacji dodatkowych urządzeń lub serwerów wirtualnych u ZamawiającegoMonitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów. Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych.Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej co najmniej 500TB.Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
|  | Możliwość migracji danych w obrębie macierzy (Jeśli opisane funkcjonalności wymagają dostarczenia licencji, należy uwzględnić w ofercie). | Zamawiający oczekuje funkcjonalności auto-tiering lub inna która pozwoli bez interwencji człowieka na akcelerację operacji na dyskach mechanicznych poprzez dyski SSD. Przyspieszanie może się odbywać poprzez automatyczne przemieszczanie danych między różnymi typami dysków w zależności od stopnia obciążenia lub poprzez akcelerację operacji zapis i odczyt dzięki przestrzeni SSD.Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC. |
| 1. 10.
 | Lokalna replikacja danych | Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.Możliwość tworzenia i utrzymywania jednocześnie co najmniej ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora.Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej.Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot.  Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write)Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |
| 1. 11.
 | Redukcja danych | Macierz powinna zapewniać metody redukcji ilości danych blokowych za pomocą kompresji. Kompresja powinna odbywać się po fakcie zapisu na urządzenia dyskowe wewnątrz macierzy (dane spoczynkowe). |
| 1. 12.
 | Kontrola przepływu danych | Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie. |
| 1. 13.
 | Współpraca z aplikacjami | Możliwość integracji środowiska VMware,  Microsoft SQL z mechanizmem lokalnej replikacji danych, zgodnie z opisem istniejącej infrastruktury opisanej w załączniku nr 1 |
| 1. 14.
 | Gwarancja | Co najmniej trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego. Należy podąć rodzaj oferowanej gwarancji producenta.Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania oraz sterowników.Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisie – **przed podpisaniem protokołu odbioru**Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady |
| 1. 15
 | Wymiana dysków | Wymiana dysków może być dokonywana przez Zamawiającego. Uszkodzone dyski zostają u Zamawiającego |
|  | Akcesoria | Komplet okablowania wymagany do podłączenia urządzenia do redundantnego zasilania, Komplet okablowania do podłączenia macierzy do oferowanych serwerów za pomocą kabli FC, Patchcordy do podłączenia sieci LAN co najmniej 5 metrów, Komplet śrub i akcesoriów wymagany do instalacji urządzenia w szafie RACK. |

 **Specyfikacja techniczna nr 3 – Napęd taśmowy LTO – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Sporządzanie kopii bezpieczeństwa oraz kopii archiwalnych na taśmy LTO z wirtualnych dysków serwerów oraz ze zdigitalizowanych obiektów. |
|  | Obudowa | Oferowane urządzenie musi być przystosowane do montażu w standardowej szafie typu rack 19” Urządzenie należy dostarczyć z niezbędnymi elementami do zamontowania w szafie typu rack 19” oraz okablowanie do podłączenia za pomocą złącza FC oraz do prąduWysokość oferowanego rozwiązania nie więcej niż 2U |
|  | Liczba slotów na taśmy | Możliwością instalacji co najmniej 8 taśm jednocześnie, co najmniej 1 slot mail |
|  | Ilość zainstalowanych napędów | Co najmniej jeden zainstalowany napęd taśmowy |
|  | Rodzaj napędu | Co najmniej LTO 7  |
|  | Interfejs napędu | FC co najmniej 8Gb/s |
|  | Zarządzanie | - Poprzez przeglądarkę WWW (przez wbudowany port Ethernet), - Obsługa za pomocą panelu umieszczonego z przodu biblioteki |
|  | Akcesoria | taśma czyszcząca – 1 sztuka,Okablowanie wymagane do podłączenia zasilania z oferowanej listwy PDU |
|  | Okres gwarancji | Minimum 3-letnie wsparcie serwisowe producenta urządzenia, w miejscu instalacji, z czasem reakcji w następnym dniu roboczym, okno zgłoszeniowe 9/5 świadczony przez polski oddział serwisowy producenta urządzenia. Wszystkie uszkodzone nośniki magnetyczne w okresie trwania wsparcia serwisowego nie wymagają zwrotu po wymianie na sprawne.Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania oraz sterowników.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady |
|  | Aktualizacje oprogramowania | W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania układowego oraz sterowników |

 **Specyfikacja techniczna nr 4 – UTM – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Zapewnienie bezpieczeństwa i łączności z internetem, zapewnienie szyfrowanej łączności z wewnętrzną siecią WAN i LAN Muzeum Narodowego w Szczecinie opartą na rozwiązaniach Fortinet, natywna obsługa posiadanych, używanych punktów dostępu FortiAP zgodnie z opisem posiadanej infrastruktury sieciowej opisanej w załączniku nr 1 |
|  | Wymagania Ogólne | * Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Zamawiający nie dopuszcza aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.
* System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
* W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.
* System musi wspierać IPv4 oraz IPv6 w zakresie:
1. Firewall,
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
 |
|  | Redundancja, monitoring i wykrywanie awarii | * W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
* Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
* Monitoring stanu realizowanych połączeń VPN.
 |
|  | Interfejsy, Dysk, Zasilanie | * System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45.
* System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
* W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
* System musi być wyposażony w zasilanie AC.
 |
|  | Parametry wydajnościowe: | * W zakresie Firewall’a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
* Przepustowość Stateful Firewall: nie mniej niż 3 Gbps.
* Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps.
* Wydajność szyfrowania IPSec VPN: nie mniej niż 2 Gbps.
* Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps.
* Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps.
* Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 135 Mbps.
 |
|  | Funkcje Systemu Bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Nie mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:* Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
* Kontrola Aplikacji.
* Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
* Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
* Ochrona przed atakami - Intrusion Prevention System.
* Kontrola stron WWW.
* Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
* Zarządzanie pasmem (QoS, Traffic shaping).
* Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
* Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
* Analiza ruchu szyfrowanego protokołem SSL.
 |
|  | Polityki, Firewall | * Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
* System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
* W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 |
|  | Połączenia VPN | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: Wsparcie dla IKE v1 oraz v2.* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

Mechanizm „Split tunneling” dla połączeń Client-to-Site.System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
|  | Routing i obsługa łączy WAN | * W zakresie routingu rozwiązanie powinno zapewniać obsługę:
1. Routingu statycznego.
2. Policy Based Routingu.
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
* System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
 |
|  | Zarządzanie pasmem | * System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
* Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
* System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
 |
| 1. 10.
 | Kontrola Antywirusowa | * Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
* System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
* System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
* System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
 |
| 1. 11.
 | Ochrona przed atakami | * Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
* System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
* Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
* System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS
* Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
* Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |
| 1. 12.
 | Kontrola aplikacji | * Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
* Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
* Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
* Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |
| 1. 13.
 | Kontrola WWW | * Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
* W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
* Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
* Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
* Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
 |
| 1. 14.
 | Uwierzytelnianie użytkowników w ramach sesji | * System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
* Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
* Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
 |
| 1. 15
 | Zarządzanie | * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
* Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
* Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
* System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
* System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
* Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
 |
| 1. 16
 | Logowanie | * Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
* Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
* Musi istnieć możliwość logowania do serwera SYSLOG.
 |
| 1. 18.
 | Certyfikaty | * Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
1. ICSA lub EAL4 dla funkcji Firewall.
2. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
3. ICSA dla funkcji SSL VPN.
 |
| 1. 19.
 | Serwisy i licencje | * W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy
 |
|  | Gwarancja oraz wsparcie | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5. |
|  | Rozszerzone wsparcie serwisowe AHB/SOS | * System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta 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. rozwiązania lub autoryzowanego dystrybutora przez okres minimum 36 miesięcy.
* oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań – **przed podpisaniem protokołu odbioru**
* Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady
 |

 **Specyfikacja techniczna nr 5 – Oprogramowanie do backupu – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Wykonywanie kopii bezpieczeństwa i archiwizacji plików z dwóch oferowanych serwerów i załączonej macierzy dyskowej bez konieczności przerywania pracy na czas wykonywania kopii. Kopii będą podlegać całe wirtualne serwery oraz pojedyncze cyfrowe odwzorowania, czyli zdigitalizowane obiekty. |
|  | Wymagania ogólne | * Oferowana licencja musi obejmować wszystkie serwery z maksymalną możliwą liczbą zainstalowanych procesorów wyszczególnionych w ramach postępowania.
* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji co najmniej 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V.
 |
|  | Całkowite koszty posiadania | * Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.
* Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
* Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie.
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
* Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
* Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza.
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
 |
|  | Wymagania RPO | * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
* Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server.
* Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V.
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere.
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).
 |
|  | Wymagania RTO | * Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2,
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V zgodnie z istniejącą i używaną w Muzeum Narodowym w Szczecinie infrastrukturą.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	+ **Linux:** ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
	+ **BSD:** UFS, UFS2
	+ **Mac:** HFS, HFS+
	+ **Windows:** NTFS, FAT, FAT32, ReFS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
* Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
* Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
* Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
* Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows.
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
 |
|  | Ograniczenie ryzyka | * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.
* Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
* Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
 |
|  | Monitoring | * System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez Vmware.
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
* System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x.
 |
|  | Raportowanie | * System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.x vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019.
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez VMware i posiadać status „VMware Ready”.
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
 |
|  | Gwarancja | Oferowane oprogramowanie musi być objęte 3 letnią gwarancją producenta wraz ze wsparciem technicznym świadczonym telefonicznie lub email uprawniającym zamawiającego do uzyskiwania porad lub instruktażu w zakresie zakupionego oprogramowania.  |
|  | Licencja | Licencja winna umożliwić wykorzystanie w pełnym zakresie możliwości każdego z oferowanych serwerów, macierzy oraz napędu LTO Funkcjonalność oprogramowania po okresie wsparcia winna zostać co najmniej taka jak w ostatnim dniu świadczonego wsparcia wraz z dostępnością wykonywania oraz odtwarzania kopii bezpieczeństwa. |

 **Specyfikacja techniczna nr 6 – System operacyjny serwera – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Uruchomienie istniejących wirtualnych maszyn w klastrze serwerowym, integracja klastra z obecnie posiadaną infrastrukturą, instalacja nowych wirtualnych serwerów do zastosowań digitalizacyjnych wraz z oprogramowaniem opartym o strukturę Windows, instalacja serwerów pomocniczych, takich jak system DNS oraz dodatkowy kontroler domeny Active Directory, zgodnie z istniejącą w Muzeum Narodowym w Szczecinie infrastrukturą opisaną w załączniku nr 1. |
|  | System | MS Windows Data Center zgodnie z opisem istniejącej infrastruktury IT, z którą system musi tworzyć jednolitą strukturę i być w pełni zgodnym. |
|  | Licencje dostępowe | 90 licencji dostępowych na użytkownika do oferowanych systemów. |
|  | Rodzaj | Rozbudowa posiadanych licencji MOLP. |
|  | Gwarancja | Wykonawca zagwarantuje dostępność bezpłatnych aktualizacji przez okres co najmniej 36 miesięcy. |

 **Specyfikacja techniczna nr 7 – Szafa dystrybucyjna – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | W szafie dystrybucyjnej będą zainstalowane serwery, macierze, zasilacze awaryjne, pionowe listwy PDU oraz urządzenia sieciowe przeznaczone do realizacji procesów digitalizacyjnych. |
|  | Obudowa | Rama spawana, stabilna o nośności do 2000kg, otworowana wraz z pionowymi otworami umożliwiającymi montaż elementów do organizacji okablowania oraz listew zasilających. Rama szafy wykonana z profili ocynkowanych, zabezpieczonej przed korozją. |
|  | Wymiary | Szerokość szafy 800mm, głębokość szafy 1200mm, wysokość szafy od 42U do 48U |
|  | Drzwi przednie | jednoczęściowe wyposażone z zamek 3 punktowy, |
|  | Drzwi tylne | Drzwi tylne dwuczęściowe(dzielone w pionie) wyposażone z zamek 3 punktowy, |
|  | Ściany boczne | wykonane z blachy stalowej, dzielone w poziomie na 2 lub 3 sekcje, demontowane oraz mocowane przy pomocy zamków, |
|  | Kolor | Szafy oraz drzwi jednolity  |
|  | Inne | * Szafa przystosowana pod montaż elementów RACK typu: organizatory, panele, urządzenia aktywne,
* Konstrukcja szafy ma umożliwiać swobodną eksploatację szafy
* Szafa musi mieć możliwość dowolnej konfiguracji przepustów kablowych,
* Szafa wyposażona w co najmniej 4 belki montażowe,
* Profile montażowe 19” z trwale oznaczoną wysokością U (numeryczny opis),
* Możliwość otwarcia drzwi przednich i tylnych co najmniej 180 stopni,
* Drzwi przednie oraz tylne z perforacją od 80% do 85%, oraz powierzchnią perforacji od 65% do 70%,
* Szafa wyposażona w listwę uziemiającą,
* Zapewniona możliwość prowadzenia okablowania po dachu,
* Dowolnej konfiguracji przepustów kablowych,
* Szafa musi być dostarczona złożona,
 |
| 1. 10.
 | Gwarancja | Gwarancja producenta na okres co najmniej 36 miesięcy. Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 21 dni kalendarzowych od daty zgłoszenia wady |

 **Specyfikacja techniczna nr 8 – Zasilacz awaryjny do szafy serwerowej – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Podtrzymanie napięcia w przypadku utraty zasilania dla wszystkich urządzeń znajdujących się w zamawianej szafie serwerowej |
|  | Obudowa | Obudowa w standardzie RACK wraz z niezbędnymi śrubami i elementami do instalacji w szafie.Wymiary urządzenia winny umożliwić montaż w szafie serwerowej z rozstawem 19 cali |
|  | Sprawność | Urządzenie po utracie zasilania umożliwi nieprzerwaną pracę urządzeń wymienionych w powyższym przetargu z przeznaczeniem do szafy na co najmniej 30 minut. |
|  | Moc | Co najmniej 6000VA, nie mniej jednak niż wymagana moc do zasilenia oferowanych urządzeń w przetargu |
|  | Akcesoria | Do zestawu winien być dołączony kabel umożliwiający podłączenie urządzenia do prądu, oraz kable umożliwiające wyłączenie serwerów oraz macierzy dyskowej z powyższych specyfikacji, patchcord LAN umożliwiający podłączenie systemu monitoringu zasilacza do przełącznika sieciowego o długości 5 metrów. |
|  | System monitoringu | Urządzenie winno być wyposażone w system monitoringu przez sieć LAN o co najmniej możliwościach:- Wyświetlenia przewidywanego czasu działania urządzenia po utracie prądu- Wyświetlenia faktycznego stanu pracy (prąd stały/ praca na bateriach)- Urządzenie winno być w stanie wysłać powiadomienie na adres e-mail o konieczności zmiany baterii- Podać nazwę oraz numer seryjny urządzenia- Posiadać interface www umożliwiający podgląd i konfigurację poprzez przeglądarkę www- Posiadać zabezpieczenie w postaci loginu i hasła w celu zmiany parametrów urządzenia- Posiadać rejestr zdarzeń, o zdarzeniach co najmniej: utrata zasilania, przywrócenie zasilania |
|  | Ekran LCD na urządzeniu | Urządzenie winno być wyposażone w ekran LCD o co najmniej możliwościach:- Wyświetlenia przewidywanego czasu działania urządzenia po utracie prądu- Wyświetlenia faktycznego stanu pracy (prąd stały/ praca na bateriach)- Wyświetlenie monitu o awarii urządzenia- Wyświetlanie parametrów prądu otrzymywanego na wejściu |
|  | Gwarancja | Wykonawca udzieli gwarancji co najmniej 36 miesięcy na urządzenie oraz 6 miesięcy na akumulatory. Samodzielna wymiana akumulatorów nie powoduje utraty gwarancji na urządzenie. Czynności serwisowe będą wykonywane na miejscu u Zamawiającego.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady |

 **Specyfikacja techniczna nr 9 – Przełącznik sieciowy dystrybucyjny z funkcją PoE**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Zapewnienie łączności urządzeniom sieciowym podłączanym do sieci LAN, zapewnienie zasilania urządzeniom PoE |
|  | Obudowa | * Typu RACK.
* Wysokość urządzenia 1U.
 |
|  | Porty | * Co najmniej 48 porty 10/100/1000BASE-T POE+.
* Co najmniej 4 porty 10GbE SFP+ w tym dwa z obsługą modułów optycznych LRM.
* Co najmniej Dwa porty SFP+ z obsługą modułów optycznych LRM.
* Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
 |
|  | POE | * Budżet POE do podziału dla urządzeń co najmniej 370W.
* Dostępność POE na wszystkich 48 portach RJ45.
 |
|  | Obsługa SSH | * RFC 4252: SSH authentication protocol
* RFC 4253: SSH transport layer protocol
* RFC 4254: SSH connection protocol
* RFC 4251: SSH protocol architecture
* RFC 4716: SECSH public key file format
* RFC 4419: Diffie-Hellman group exchange
 |
|  | Obsługa SSL 3.0 oraz TLS 1.0 | * RFC 2246: Protokół TLS, wersja 1.0
* RFC 2818: HTTP over TLS
* RFC 3268: AES
 |
|  | Routing | * Obsługa Routingu statycznego.
* Obsługa statycznego routingu IPv6, co najmniej 60 tras.
* Obsługa dynamicznego routing IPv4 (RFC 2453 RIP v2).
 |
|  | VLAN | * Obsługa Multicast VLAN Registration (MVR).
* Obsługa Independent VLAN Learning (IVL).
 |
|  | ACL | * Obsługa Listy kontroli dostępu ACL co najmniej 9 na port.
 |
|  | Obsługa list kontroli dostępu dla ruchu przychodzącego na podstawie | * Czasu.
* Źródłowego i docelowego adresu IP.
* TCP/UDP źródłowy i docelowy.
* Rodzaju protokołu IP.
* EtherType.
* IEE 802.1p.
* Źródłowy i docelowy adres MAC.
* Vlan id.
 |
|  | Warunki pracy. | * Zakres temperatury pracy Co najmniej od 0-50 °C
* Zakres wilgotności od 10% do 95%.
 |
|  | Inne | * Nieblokująca architektura o wydajności przełączania co najmniej 176 Gb/s.
* Szybkość przełączania co najmniej 130.9 Milionów pakietów na sekundę.
* Tablica MAC adresów co najmniej 16k.
* Wsparcie dla ramek Jumbo Frames.
* Obsługa Quality of Service, IEEE 802.1p.
* Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
* Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
* Obsługa CDPv2.
* Obsługa Remote Switch Port Analyzer (RSPAN).
* Możliwość zarządzania przełącznikiem za pomocą systemu zarządzania z poziomu chmury obsługującego polityki oraz mechanizmy kontroli dostępu NAC.
* Obsługa mechanizmu Zero-touch provisioning z poziomu chmury oraz lokalnego systemu zarządzania.
* Możliwość monitoringu pakietów.
* Obsługa TACACS+ (RFC 1492).
* Obsługa klienta RADIUS RFC 2865.
* Obsługa IEEE 802.3x —Flow control.
* Obsługa minimum 4 instancji MSTP.
* Obsługa RFC 4541 (IGMP).
* Możliwość tworzenia stosu urządzeń. Stos zarządzany za pomocą jednego adresu IP.
* Obsługa Policy-Based Routing.
* Obsługa skryptów CLI.
 |
|  | Zasilanie | * Wbudowany port pozwalający na podłączenie zewnętrznego redundantnego zasilacza RPS.
* Urządzenie wyposażone w oryginalny kabel zasilania.
 |
|  | Zarzadzanie | * WEB
* GUI
* Możliwość utworzenia co najmniej 5 kont dostępu z różnicowanymi uprawnieniami
 |
|  | Dodatkowe wyposażenie | * Kabel połączeniowy RJ45 kat.6 o długości 50 cm – 25 Sztuk
* Kabel połączeniowy RJ45 kat.6 o długości 100 cm – 20 Sztuk
* Moduł SPF+ - 4 sztuki
 |
|  | Gwarancja | Gwarancja producenta Lifetime realizowana przez pięć lat po zakończeniu produkcji urządzenia. Wymiana urządzenia na sprawne na drugi dzień roboczy od momentu zgłoszenia.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady |

 **Specyfikacja techniczna nr 10 – KVM – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | KVM przeznaczony do sterowania serwerami. Urządzenie winno współpracować z oferowanymi serwerami. |
|  | Połączenia | Co najmniej 8 z możliwością połącznia kaskadowego do co najmniej 128 urządzeń |
|  | Porty | * 8 x SPHD-17 żeńskie (żółte)
 |
|  | Ekran | * Co najmniej 17”
* Co najmniej 16,7 mln kolorów
* Czas reakcji co najmniej 5 ms
* Kąt widzenia co najmniej 170° (w poziomie), co najmniej 160° (w pionie)
* Rozdzielczość co najmniej 1280 x 1024
 |
|  | Przewody | Komplet okablowania do podłączenia wszystkich serwerów oferowanych w ramach niniejszego postępowania oraz kable umożliwiające przyłączenie urządzenia do prądu |
| 1. 11.
 | Gwarancja | Gwarancja na okres minimum 36 miesięcy wraz w wszystkimi akcesoriami i okablowaniem. Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady |
|  | Obudowa | Przystosowana do montażu w oferowanej szafie RACK, nie wyższa niż 1U.Do zestawu dołączone będą wszystkie akcesoria i śruby umożliwiające montaż, złożenie i schowanie urządzenia w szafie RACK  |
|  | Klawiatura | W układzie qwerty, prawidłowo obsługująca układ klawiatury polski - programisty. Nie dopuszcza się przystosowania klawiatury poprzez różnego rodzaju nalepki na guziki. |
|  | Touchpad | Wbudowany, z co najmniej dwoma przyciskami symulującymi prawy i lewy przycisk myszy. |
|  | Energia | Urządzenie będzie automatycznie wyłączać ekran podczas składania go celem schowania w szafie, oraz wznawiać automatycznie po otworzeniu urządzenia. |

 **Specyfikacja techniczna nr 11 – Listwa PDU – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1 | Zastosowanie | Dystrybucja zasilania do urządzeń w szafie serwerowej z oferowanego zasilacza awaryjnego oraz z sieci elektrycznej, monitoring warunków klimatycznych  |
| 2 | Obudowa  | Listwa przeznaczona do montażu w szafie serwerowej w pozycji pionowej |
| 3 | Gniazda zasilające | Minimum 20 gniazd typu C13Minimum 4 gniazda typu C19 |
| 4 | Minimalna obciążalność listwy  | Minimum 16A |
| 5 | Wyposażenie  | Czujnik temperatury i wilgotności |
| 6 | Obsługa | Obsługa i zarządzanie listwą odbywa się poprzez protokół http lub https, oprogramowanie ma być zaimplementowane w listwie |
| 7 | Port komunikacyjny  | Co najmniej Ethernet  |
| 8 | Wyświetlacz | Informacja co najmniej o: Bieżący stan urządzeniaObciążenie prądu, Temperaturze, Wilgotności |
| 9 | Monity | W przypadku przekroczenia dopuszczalnych wartości temperatury, wilgotności zostanie wysłane powiadomienie pocztą elektroniczną za pośrednictwem systemu MS Office 365 |
| 10 | Monitoring www umożliwi | Kontrolę Całkowitego obciążenieObciążenie dla indywidualnych portówStan pojedynczego portu, Bieżący stan listwyTemperatura i wilgotnośćObecność dymu, Obecność wody czy innych płynów |
| 11 | Kontrola poprzez www umożliwi | WŁ/WYŁ wszystkich portów WŁ/WYŁ indywidualnych portów |
| 12 | Podłączenie | Dołączony kabel umożliwiający podłączenie do oferowanego UPS  |
| 13 | Gwarancja | Co najmniej 3 lata, jednak nie krócej niż gwarancja producentaWady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady |

 **Specyfikacja techniczna nr 12 – Przełącznik sieciowy szkieletowy – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Zapewnienie łączności pomiędzy segmentami sieci a szafą dystrybucyjną, zapewnienie łączności pomiędzy serwerami a resztą sieci. |
|  | Porty | Przełącznik posiadający co najmniej 16 portów 10Gigabit Ethernet SFP+, mogących pracować co najmniej z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+Wraz z przełącznikiem należy dostarczyć co najmniej 4 wkładki SFP+ wraz okablowaniem (każdy o długości 2m) niezbędnym do podłączenia oferowanego przełącznika z oferowanymi serwerami |
|  | Obudowa | Umożliwiająca montaż w szafie RACK z rozstawem 19 cali, o maksymalnej wysokości 1U. |
|  | Przepustowość | Nieblokująca architektura o wydajności przełączania co najmniej 320 Gb/s |
|  | Łączenie przełączników | Możliwość łączenia co najmniej 8 przełączników w stos za pomocą portów 10G |
|  | Tablica MAC | Tablica MAC adresów min. 16k |
|  | Pamięć flash | Pamięć flash: min. 4 GB pamięci Flash |
|  | Obsługa vLAN | Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094Obsługa sieci wirtualnych protokołowych IEEE 802.1vObsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci |
|  | Obsługa Jumbo Frames | Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) |
|  | Obsługa podwójnie tagowanych ramek | Q-in-Q IEEE 802.1ad |
| 1. 10.
 | Obsługa QoS | - IEEE 802.1p- DiffServ- kolejek priorytetów na każdym porcie wyjściowym |
| 1. 11.
 | Obsługa Link Layer Discovery | Co najmniej protokół LLDP IEEE 802.1AB, Media Endpoint Discovery (LLDP-MED) |
| 1. 12.
 | Pamięć | Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora |
| 1. 13.
 | Redundancja zasilaczy | Przełącznik musi posiadać możliwość instalacji dwóch zasilaczy, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika. Zainstalowany co najmniej jeden zasilacz |
| 1. 14.
 | Zabezpieczenie oprogramowania układowego | Możliwość instalacji co najmniej dwóch wersji oprogramowania – firmware, oraz cofnięcia oprogramowania do poprzedniej wersjiMożliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash |
| 1. 15
 | Monitoring urządzenia | Co najmniej możliwość monitorowania zajętości CPU,Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring) |
| 1. 16
 | Obsługa wirtualnych routerów | możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach |
| 1. 18.
 | Port do zarządzania | Co najmniej wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem |
| 1. 19.
 | Protokół CDP | Co najmniej w wersji 2 |
| 1. 20.
 | Obsługa routingu IPv4 | Co najmniej:Sprzętowa obsługa routingu IPv4 – forwardingRouting statycznyObsługa routingu dynamicznego IPv4 co najmniej RIPv1/v2, OSPFv2 |
|  | Obsługa routingu IPv6 | Co najmniejSprzętowa obsługa routingu IPv6 – forwardingRouting statycznyObsługa routingu dynamicznego dla IPv6 co najmniej: RIPng, OSPF v3Telnet Serwer/Klient dla IPv6SSH2 Serwer/Klient dla IPv6Ping dla IPv6Tracert dla IPv6Obsługa MLDv1 (Multicast Listener Discovery version 1) |
|  | Obsługa multicastów | Co najmniej:Filtrowanie IGMPObsługa Multicast VLAN Registration – MVRObsługa IGMP v1/v2/v3 snooping |
|  | Bezpieczeństwo | Obsługa Network Login co najmniej: EEE 802.1x - RFC 3580, Web-based Network Login, MAC based Network LoginObsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)Możliwość integracji funkcjonalności Network Login z Microsoft NAPObsługa Guest VLAN dla IEEE 802.1xPrzydział sieci VLAN, ACL/QoS podczas logowania Network LoginMożliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authenticationObsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu KerberosObsługa Identity ManagementWbudowana obrona procesora urządzenia przed atakami DoSObsługa TACACS+Obsługa RADIUS AuthenticationObsługa RADIUS AccountingRADIUS and TACACS+ per-command AuthenticationBezpieczeństwo MAC adresów co najmniej: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresu na porcie, możliwość wpisania statycznych MAC adresów na port/vlanMożliwość wyłączenia MAC learningObsługa SNMPv1/v2/v3Klient SSH2Wysłanie informacji do serwera SyslogObsługa IP Security - Gratuitous ARP ProtectionObsługa IP Security – Trusted DHCP ServerObsługa IP Security – DHCP Secured ARP/ARP ValidationObsługa IP Security – IP Source guardOgraniczanie przepustowości (rate limiting) na portach wyjściowych |
|  | Bezpieczeństwo sieci | Co najmniej:Możliwość konfiguracji portu głównego i zapasowegoObsługa redundancji routingu VRRP - RFC 2338Obsługa STP (Spinning Tree Protocol) IEEE 802.1DObsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1wObsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1sObsługa PVST+Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619Obsługa G.8032Obsługa Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portówObsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników |
|  | Administrowanie | Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)Obsługa synchronizacji czasu NTPZarządzanie przez SNMP v1/v2/v3Zarządzanie przez przeglądarkę WWW – protokół http i httpsMożliwość zarządzania przez protokół XMLSSH2 Serwer/Klient dla IPv4 / IPv6Ping dla IPv4 / IPv6Traceroute dla IPv4 / IPv6Obsługa SYSLOG z możliwością definiowania wielu serwerówSprzętowa obsługa sFlowObsługa RMON min. 4 grupy: Status, History, Alarms, EventsObsługa RMON2Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) |
|  | Gwarancja | Gwarancja producenta Lifetime realizowana przez pięć lat po zakończeniu produkcji urządzenia. Wymiana urządzenia na sprawne na drugi dzień roboczy od momentu zgłoszeniaWady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady |
|  | Zarządzanie | Dołączona aplikacja, która musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera Windows. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.Aplikacja musi być wyprodukowana i wspierana przez producenta oferowanych przełączników.Aplikacja zarządzająca musi obsługiwać co najmniej 10 urządzeń (adresów IP)Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego.Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub RadiusAplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AESAplikacja 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 systemówAplikacja 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 skryptuAplikacja musi posiadać wbudowany Syslog serwerAplikacja musi posiadać wbudowany BootP serwerAplikacja musi wspierać protokół IPv4 oraz IPv6Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratoraAplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniachAplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości, stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów, konfiguracji sieci VLAN, konfiguracji protokołu routingu OSPFAplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/httpsAplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane: adres IP urządzenia, adresu MAC urządzenia, nazwy urządzenia, wersji oprogramowania, wersji bootrom, lokalizacji urządzenia, 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 producentówAplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasieAplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniachAplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na kontrolę dostępu do sieci dla urządzeń końcowych (NAC)System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.System zarządzania musi być objęty co najmniej pięcioletnim wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7. |

 **Specyfikacja techniczna nr 13 – Taśmy LTO – 20 sztuk**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** |
| 1. 1.
 | Zastosowanie | Nośniki danych do oferowanego napędu LTO |
|  | Rodzaj taśm | Co najmniej LTO7, jednak pasujące do oferowanego napędu ze specyfikacji nr 3  |
|  | Oznaczenie taśm | Załączone identyfikatory taśm używana w oferowanym napędzie ze specyfikacji nr 3 dla co najmniej wszystkich taśm  |
|  | Opakowanie | Do każdej taśmy winno być dołączone opakowanie zabezpieczające |
|  | Gwarancja | Gwarancja na 6 miesięcy jednak nie krócej niż gwarancja producenta.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady |

**Załącznik nr 2 – Formularz ofertowy**

(Wykonawca)

(pieczęć Wykonawcy)

**(pieczęć wykonawcy)**

**FORMULARZ OFERTOWY**

*………………………………………………………………………………………………………………*...*………*

*nazwa firmy*

*………………………………………………………………………………………………………………*...*………*

*adres*

*………………………………………………………………………………………………………………*...*………*

*Nr KRS/CEiDG*

*………………………………………………………………………………………………………………*...*………*

*telefon, faks, e-mail*

W odpowiedzi na ogłoszenie o przetargu nieograniczonym na:

**„Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie”**

1. **Oferuję** realizację całości przedmiotu zamówienia za cenę całkowitą:

 Cena netto: ……………………………………... zł

 Kwota podatku VAT ……. % ………………. zł

 Cena brutto: ........................................ zł

**2. Oferuję** termin wykonania zamówienia …………….. dni od dnia zawarcia umowy.

3. **Kryterium oceny ofert jest** **Deklaracja wykonawcy o posiadaniu autoryzacji producenta dostarczonych przełączników sieciowych jeżeli wykonawca posiada**  – w niniejszym kryterium można zdobyć 30 pkt. Ocenie podlegać będzie czy do oferty Wykonawca dołączy pisemne oświadczenie o posiadaniu autoryzacji producenta dostarczanych przełączników sieciowych. Oświadczenie winno być podpisane przez osobę która podpisała ofertę.

 Wykonawca który do oferty dołączy w/w pisemne oświadczenie otrzyma 30 pkt.

 Wykonawca który do oferty nie dołączy w/w oświadczenia otrzyma 0 pkt

3. Oświadczam, że podana wyżej cena obejmuje wszelkie koszty związane z realizacją zamówienia.

4. Informuję/informujemy, iż: wybór oferty będzie/ nie będzie\* prowadzić do powstania u Zamawiającego obowiązku podatkowego. W związku z powyższym wskazujemy nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazujemy ich wartość bez kwoty podatku: ………………………………………………………………………………………………………………………………………………………

5. Akceptuję Projekt umowy stanowiący Załącznik nr 10 (odpowiednio dla danego zadania) do SIWZ, w tym warunki i termin płatności w nim określone, zapoznałem się z treścią SIWZ, nie wnoszę do niej zastrzeżeń, w pełni akceptuję jej warunki oraz zdobyłem konieczne informacje do przygotowania oferty.

6. Zobowiązuję się, w przypadku wybrania mojej oferty, do zawarcia umowy, zgodnie z Projektem umowy stanowiącym Załącznik nr 10 do SIWZ (odpowiednio dla danego zadania), w wyznaczonym przez Zamawiającego miejscu i terminie.

7. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

 *W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

8. Oświadczam/oświadczamy, że zamówienie wykonamy samodzielnie\*/przy pomocy podwykonawców\*, którym zamierzamy powierzyć wykonanie następującej części zamówienia:

|  |  |
| --- | --- |
| **Nazwa i adres podwykonawcy** | **Część ( zakres) zamówienia** |
|  |  |

 W przypadku nie wypełnienia tego punktu w całości, bądź nie wymienienia części, które zostaną powierzone podwykonawcom, Zamawiający uzna, że Wykonawca wykona zamówienie samodzielnie.

9. Oświadczam/oświadczamy, że jestem związany ofertą do upływu terminu wskazanego w specyfikacji istotnych warunków zamówienia, tj. 30 dni

10. Na potwierdzenie powyższego wnieśliśmy wadium w wysokości ……………………. zł. złotych w formie/formach ……………………………………………………………………………………………………………………………. Wadium wniesione w pieniądzu należy zwrócić na konto nr……………………………………………………………. W banku…………………………………………………………………………………………………………………………………………

11. \*Oświadczam/y, że oferta **nie zawiera informacji** stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

\*Oświadczam/y, że oferta **zawiera informacje** stanowiące tajemnicę przedsiębiorstwa
w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach : ……………………………….………………………..

\* **Niewłaściwe skreślić**

 ………………………………………………… …………………………………………

 miejscowość i data podpis osoby/osób uprawnionej do reprezentowania Wykonawcy

 **Załącznik nr 3 – Formularz cenowo – przedmiotowy**

|  |
| --- |
|  (wykonawca) |

**FORMULARZ CENOWO PRZEDMIOTOWY**

**Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie**

**\*- wykonawca wypełnia pola kolumny 4 - *Potwierdzenie zgodności parametró*w.**

**Wykonawca zobowiązany jest do wypełnienia każdego pola w kolumnie 4 tabeli poprzez wpis TAK lub NIE (potwierdza lub nie potwierdza zgodność parametrów oferowanego sprzętu z określonymi w odpowiednim polu w kolumnach 2 i 3**

|  |
| --- |
| **SERWER TYPU RACK – 2 SZTUKI** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** | **4** |
| 1 | Zastosowanie | Utrzymanie wirtualnych serwerów (system oparty na bazie danych MySQL z zawartością 500 000 rekordów, pomocniczy kontroler domeny, DNS, dysk sieciowy) w środowisku Microsoft Windows Hyper-V na potrzeby procesów digitalizacyjnych opartych na klastrze utworzonym na podstawie systemu Windows DataCenter. Każdy z serwerów będzie podłączony za pomocą dwóch przyłączy światłowodowych do oferowanego szkieletowego przełącznika sieciowego oraz za pomocą dwóch kabli FC do oferowanej macierzy dyskowej. |  |
| 2 | Obudowa | Maksymalnie 2U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack) |  |
| 3 | Płyta Głowna | Dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera, oznaczona jego znakiem firmowym z możliwością zainstalowania dwóch procesorów.Co najmniej 3 sloty generacji 3 o prędkości x8 oraz 2 sloty generacji 3 o prędkości x16 |  |
| 4 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach co najmniej dwuprocesorowych. |  |
| 5 | Procesor | Zainstalowane dwa procesory ośmio-rdzeniowe x86 – 64 bity, dedykowane do pracy z zaoferowanym serwerem, każdy osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 11500 punktów. Wynik testu musi być opublikowany na stronie www.cpubenchmark.netSuma rdzeni fizycznych obu procesorów nie może być większa niż 16. | Nazwa procesora………………………………………………………..Taktowanie………………………………….. |
| 6 | Pamięć RAM | 128 GB RDIMM DDR4 2666 MT/s.Minimum 15 wolnych slotów na rozbudowę pamięć.Możliwość rozbudowy pamięci do co najmniej 1TB. |  |
| 7 | Interfejsy sieciowe/FC/SAS | Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz co najmniej 2 interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+ lub BaseT wraz z dwoma modułami nadawczo-odbiorczymi 10GbE SFP+ SR. Zainstalowana co najmniej jedna karta dwuportowa FC 16Gb/s. |  |
| 8 | Napęd optyczny | Wbudowany napęd co najmniej DVD. |  |
| 9 | Dysk | Co najmniej 2 dyski w technologii SSD minimum 120 GB Hot Plug montowane z przodu obudowy,Co najmniej 4 wolne zatoki do instalacji kolejnych dysków typu: Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy |  |
| 10 | Kontroler RAID | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów co najmniej RAID: 0, 1, 5, 10, 50. |  |
| 11 | Porty | Co najmniej 1 x VGA,Co najmniej 3 porty USB co najmniej 3.0,Co najmniej 2 porty USB co najmniej 2.0, |  |
| 12 | Karta Graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1280x1024. |  |
| 13 | Wentylatory | Zestaw wentylatorów redundantnych typu hot-plug. |  |
| 14 | Zasilacze | Co najmniej 2 szt., typu Hot-plug, redundantne, każdy o mocy wystarczającej do zasilania oferowanego sprzętu. |  |
| 15 | Karta Zarządzania | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe
* Możliwość zdalnego włączenia / wyłączenia oraz restartu serwera
* wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
* dostęp do karty zarządzającej poprzez
	+ dedykowany port RJ45 z tyłu serwera

 dostęp do karty możliwy * + z poziomu przeglądarki webowej (GUI)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer
* zdalna aktualizacja oprogramowania (firmware)
* możliwość równoczesnej obsługi przez co najmniej 2 administratorów
* wsparcie dla autoryzacji elementów systemu i użytkowników oraz dostępu do zasobów stosowanego w Muzeum Narodowym w Szczecinie systemu opisanego w załączniku nr 1
* obsługa SSL i SSH
* wsparcie dla co najmniej IPv4
 |  |
| 16 | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-14001. Serwer musi posiadać deklaracja CE.Z uwagi na opisaną w załączniku nr 1 infrastrukturę istniejącą i stosowaną w Muzeum Narodowym w Szczecinie oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów co najmniej Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016. |  |
| 17 | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Z uwagi na opisaną w załączniku nr 1 infrastrukturę istniejącą i stosowaną w Muzeum Narodowym w Szczecinie : Microsoft Windows Server 2012 R2, 2016, 2019Microsoft Hyper-V Server 2012 R2, 2016, 2019 |  |
| 18 | Inne | Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski. |  |
| 19 | Gwarancja | Co najmniej 3 lata. Wsparcie serwisowe producenta serwera, w miejscu instalacji, z czasem reakcji w następnym dniu roboczym, okno zgłoszeniowe 9/5 świadczony przez polski oddział serwisowy producenta serwera.Wszystkie dyski uszkodzone w okresie trwania wsparcia serwisowego nie wymagają zwrotu po wymianie na sprawne.Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania układowego oraz sterowników.Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisie - – **przed podpisaniem protokołu odbioru** Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji ……………………….. |
| 20 | Akcesoria | Zestaw kabli umożliwiających podłączenie urządzenia do listw PDU,Patchcord do podłączenia sieci monitoringu do sieci LAN co najmniej 5 metrów, Komplet śrub i akcesoriów wymagany do instalacji urządzenia w szafie RACK,Kable FC wymagane do redundantnego podłączenia serwera do macierzy.  |  |
| 21 |  | Nazwa producenta komputera |  |
| 22 |  | Model oferowanego komputera |  |

|  |
| --- |
| **MACIERZ DYSKOWA – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
|  **1** | **2** | **3** | **4** |
| 1 | Zastosowanie | Obsługa dysków wirtualnych serwerów w istniejącym w Muzeum Narodowym w Szczecinie systemie opisanym w załączniku nr 1 dla maszyn wirtualnych oraz przestrzeń na dane robocze i archiwalne. |  |
| 2 | Obudowa | Obudowa umożliwiająca zamontowanie macierzy w systemie RACK w dostarczonej szafie serwerowej, o maksymalnej wysokości 5U. Załączone wszystkie elementy montażowe konieczne do prawidłowego zamocowania macierzy zgodnie z wytycznymi producenta. W obudowie winny być zainstalowane co najmniej dwa kontrolery macierzowe redundantne |  |
| 3 | Przestrzeń dyskowa | Macierz musi być wyposażona w co najmniej 1920GB powierzchni w technologii SSD w systemie raid 1-0 oraz 78TB powierzchni w technologii co najmniej NLSASPowierzchnia jest podana jako surowa - RAW przed formatowaniem. |  |
| 4 | Pamięć podręczna | Pamięć podręczna (cache) – co najmniej 16 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie co najmniej 32 GB).  Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. |  |
| 5 | Interfejsy zewnętrzne | Macierz musi być wyposażona w co najmniej: 8 portów FC 16Gb/s oraz 8 portów 10 GbE SFP+, 2 porty zarządzające 1GbE Base-T, każdy kontroler macierzy w trybie Active-Active. |  |
| 6 | Dostępność | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).Możliwość łączenia w macierzy różnych poziomów RAID, co najmniej: - możliwość zastosowania RAID10- możliwość zastosowania RAID5,- możliwość zastosowania RAID6- możliwość zastosowania RAID0- możliwość zastosowania RAID1Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych.Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).Możliwość zdefiniowania co najmniej 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa.Możliwość obsługi wirtualnych portów (NPIV) w taki sposób, aby awaria fizycznego portu nie powodowała konieczności przełączania ścieżek poprzez oprogramowanie do multipathing |  |
| 7 | Wspierane systemy operacyjne | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej MS Windows oraz Linux, Vmware,Wymagane wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server, HACMP, HP Serviceguard.Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych co najmniej: AIX, HP-UX, MS Windows, Vmware, Linux.Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning |  |
| 8 | Skalowalność | Wykonywanie rozbudowy sprzętowej w trybie online.Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash.Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej.Macierz musi umożliwiać rozbudowę o moduły co najmniej 12 dysków 3,5” , co najmniej 24 dyski 2,5”Obsługa ci najmniej 200 dysków SAS/NLSAS lub SSD |  |
| 9 | Zarządzanie | Oprogramowanie do zarządzania macierzą przez administratora klienta winno posiadać graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).Stałe monitorowanie macierzy przez zdalne centrum serwisowe, bez konieczności instalacji dodatkowych urządzeń lub serwerów wirtualnych u ZamawiającegoMonitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów. Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych.Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej co najmniej 500TB.Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |  |
| 10 | Możliwość migracji danych w obrębie macierzy (Jeśli opisane funkcjonalności wymagają dostarczenia licencji, należy uwzględnić w ofercie). | Zamawiający oczekuje funkcjonalności auto-tiering lub inna która pozwoli bez interwencji człowieka na akcelerację operacji na dyskach mechanicznych poprzez dyski SSD. Przyspieszanie może się odbywać poprzez automatyczne przemieszczanie danych między różnymi typami dysków w zależności od stopnia obciążenia lub poprzez akcelerację operacji zapis i odczyt dzięki przestrzeni SSD.Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC. |  |
| 11 | Lokalna replikacja danych | Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.Możliwość tworzenia i utrzymywania jednocześnie co najmniej ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora.Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej.Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot.  Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write)Kopie migawkowe muszą mieć możliwość prezentacji, jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |  |
| 12 | Redukcja danych | Macierz powinna zapewniać metody redukcji ilości danych blokowych za pomocą kompresji. Kompresja powinna odbywać się po fakcie zapisu na urządzenia dyskowe wewnątrz macierzy (dane spoczynkowe). |  |
| 13 | Kontrola przepływu danych | Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie. |  |
| 14 | Współpraca z aplikacjami | Możliwość integracji środowiska VMware,  Microsoft SQL z mechanizmem lokalnej replikacji danych, zgodnie z opisem istniejącej infrastruktury opisanej w załączniku nr 1 |  |
| 15 | Gwarancja | Co najmniej trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego. Należy podąć rodzaj oferowanej gwarancji producenta.Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania oraz sterowników.Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisie -– **przed podpisaniem protokołu odbioru** Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji ………………………. |
| 16 | Wymiana dysków | Wymiana dysków może być dokonywana przez Zamawiającego. Uszkodzone dyski zostają u Zamawiającego |  |
| 17 | Akcesoria | Komplet okablowania wymagany do podłączenia urządzenia do redundantnego zasilania, Komplet okablowania do podłączenia macierzy do oferowanych serwerów za pomocą kabli FC, Patchcordy do podłączenia sieci LAN co najmniej 5 metrów, Komplet śrub i akcesoriów wymagany do instalacji urządzenia w szafie RACK. |  |
| 18 |  | Nazwa producenta komputera |  |
| 19 |  | Model oferowanego komputera |  |

|  |
| --- |
| **NAPĘD TAŚMOWY LTO – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** | **4** |
| 1 | Zastosowanie | Sporządzanie kopii bezpieczeństwa oraz kopii archiwalnych na taśmy LTO z wirtualnych dysków serwerów oraz ze zdigitalizowanych obiektów. |  |
| 2 | Obudowa | Oferowane urządzenie musi być przystosowane do montażu w standardowej szafie typu rack 19” Urządzenie należy dostarczyć z niezbędnymi elementami do zamontowania w szafie typu rack 19” oraz okablowanie do podłączenia za pomocą złącza FC oraz do prąduWysokość oferowanego rozwiązania nie więcej niż 2U |  |
| 3 | Liczba slotów na taśmy | Możliwością instalacji co najmniej 8 taśm jednocześnie, co najmniej 1 slot mail |  |
| 4 | Ilość zainstalowanych napędów | Co najmniej jeden zainstalowany napęd taśmowy |  |
| 5 | Rodzaj napędu | Co najmniej LTO 7  |  |
| 6 | Interfejs napędu | FC co najmniej 8Gb/s |  |
| 7 | Zarządzanie | - Poprzez przeglądarkę WWW (przez wbudowany port Ethernet), - Obsługa za pomocą panelu umieszczonego z przodu biblioteki |  |
| 8 | Akcesoria | taśma czyszcząca – 1 sztuka,Okablowanie wymagane do podłączenia zasilania z oferowanej listwy PDU |  |
| 9 | Okres gwarancji | Minimum 3-letnie wsparcie serwisowe producenta urządzenia, w miejscu instalacji, z czasem reakcji w następnym dniu roboczym, okno zgłoszeniowe 9/5 świadczony przez polski oddział serwisowy producenta urządzenia. Wszystkie uszkodzone nośniki magnetyczne w okresie trwania wsparcia serwisowego nie wymagają zwrotu po wymianie na sprawne.Dostarczone urządzenie musi być produktem fabrycznie nowym, nieużywanym, dostarczonym poprzez autoryzowany kanał sprzedaży producenta na terenie Polski.W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania oraz sterowników.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji ……………………….. |
| 10 | Aktualizacje oprogramowania | W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania układowego oraz sterowników |  |
| 11 |  | Nazwa producenta komputera |  |
| 12 |  | Model oferowanego komputera |  |

|  |
| --- |
| **UTM – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
|  **1** | **2** | **3** |  **4** |
| 1 | Zastosowanie | Zapewnienie bezpieczeństwa i łączności z internetem, zapewnienie szyfrowanej łączności z wewnętrzną siecią WAN i LAN Muzeum Narodowego w Szczecinie opartą na rozwiązaniach Fortinet, natywna obsługa posiadanych, używanych punktów dostępu FortiAP zgodnie z opisem posiadanej infrastruktury sieciowej opisanej w załączniku nr 1 |  |
| 2 | Wymagania Ogólne | * Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Zamawiający nie dopuszcza aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.
* System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
* W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.
* System musi wspierać IPv4 oraz IPv6 w zakresie:
1. Firewall,
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
 |  |
| 3 | Redundancja, monitoring i wykrywanie awarii | * W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
* Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
* Monitoring stanu realizowanych połączeń VPN.
 |  |
| 4 | Interfejsy, Dysk, Zasilanie | * System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45.
* System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
* W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
* System musi być wyposażony w zasilanie AC.
 |  |
| 5 | Parametry wydajnościowe: | * W zakresie Firewall’a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
* Przepustowość Stateful Firewall: nie mniej niż 3 Gbps.
* Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps.
* Wydajność szyfrowania IPSec VPN: nie mniej niż 2 Gbps.
* Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps.
* Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps.
* Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 135 Mbps.
 |  |
| 6 | Funkcje Systemu Bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Nie mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:* Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
* Kontrola Aplikacji.
* Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
* Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
* Ochrona przed atakami - Intrusion Prevention System.
* Kontrola stron WWW.
* Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
* Zarządzanie pasmem (QoS, Traffic shaping).
* Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
* Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
* Analiza ruchu szyfrowanego protokołem SSL.
 |  |
| 7 | Polityki, Firewall | * Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
* System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
* W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 |  |
| 8 | Połączenia VPN | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: Wsparcie dla IKE v1 oraz v2.* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

Mechanizm „Split tunneling” dla połączeń Client-to-Site.System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |  |
| 9 | Routing i obsługa łączy WAN | * W zakresie routingu rozwiązanie powinno zapewniać obsługę:
1. Routingu statycznego.
2. Policy Based Routingu.
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
* System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
 |  |
| 10 | Zarządzanie pasmem | * System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
* Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
* System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
 |  |
| 11 | Kontrola Antywirusowa | * Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
* System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
* System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
* System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
 |  |
| 12 | Ochrona przed atakami | * Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
* System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
* Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
* System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS
* Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
* Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |  |
| 13 | Kontrola aplikacji | * Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
* Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
* Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
* Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |  |
| 14 | Kontrola WWW | * Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
* W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
* Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
* Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
* Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
 |  |
| 15 | Uwierzytelnianie użytkowników w ramach sesji | * System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
* Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
* Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
 |  |
| 16 | Zarządzanie | * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
* Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
* Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
* System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
* System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
* Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
 |  |
| 17 | Logowanie | * Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
* Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
* Musi istnieć możliwość logowania do serwera SYSLOG.
 |  |
| 18 | Certyfikaty | * Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
1. ICSA lub EAL4 dla funkcji Firewall.
2. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
3. ICSA dla funkcji SSL VPN.
 |  |
| 19 | Serwisy i licencje | * W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy
 |  |
| 20 | Gwarancja oraz wsparcie | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5. | Okres gwarancji ……………………….. |
| 21 | Rozszerzone wsparcie serwisowe AHB/SOS | * System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta 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. rozwiązania lub autoryzowanego dystrybutora przez okres minimum 36 miesięcy.
* oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań - – **przed podpisaniem protokołu odbioru**
* Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady
 |  |
| 22 |  | Nazwa producenta komputera |  |
| 23 |  | Model oferowanego komputera |  |

|  |
| --- |
| **OPROGRAMOWANIE DO BACKUPU – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametr ów** |
| **1** | **2** | **3** | **4** |
| 1 | Zastosowanie | Wykonywanie kopii bezpieczeństwa i archiwizacji plików z dwóch oferowanych serwerów i załączonej macierzy dyskowej bez konieczności przerywania pracy na czas wykonywania kopii. Kopii będą podlegać całe wirtualne serwery oraz pojedyncze cyfrowe odwzorowania, czyli zdigitalizowane obiekty. |  |
|  | Wymagania ogólne | * Oferowana licencja musi obejmować wszystkie serwery z maksymalną możliwą liczbą zainstalowanych procesorów wyszczególnionych w ramach postępowania.
* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji co najmniej 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V.
 |  |
| 2 | Całkowite koszty posiadania | * Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.
* Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
* Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie.
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
* Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
* Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza.
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
 |  |
| 3 | Wymagania RPO | * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
* Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server.
* Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V.
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere.
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).
 |  |
| 4 | Wymagania RTO | * Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2,
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V zgodnie z istniejącą i używaną w Muzeum Narodowym w Szczecinie infrastrukturą.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	+ **Linux:** ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
	+ **BSD:** UFS, UFS2
	+ **Mac:** HFS, HFS+
	+ **Windows:** NTFS, FAT, FAT32, ReFS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
* Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
* Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
* Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
* Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows.
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
 |  |
| 5 | Ograniczenie ryzyka | * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.
* Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
* Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
 |  |
| 6 | Monitoring | * System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez Vmware.
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
* System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x.
 |  |
| 7 | Raportowanie | * System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.x vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019.
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez VMware i posiadać status „VMware Ready”.
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
 |  |
| 8 | Gwarancja | Oferowane oprogramowanie musi być objęte 3 letnią gwarancją producenta wraz ze wsparciem technicznym świadczonym telefonicznie lub email uprawniającym zamawiającego do uzyskiwania porad lub instruktażu w zakresie zakupionego oprogramowania. | Okres gwarancji ………………………. |
| 9 | Licencja | Licencja winna umożliwić wykorzystanie w pełnym zakresie możliwości każdego z oferowanych serwerów, macierzy oraz napędu LTOFunkcjonalność oprogramowania po okresie wsparcia winna zostać co najmniej taka jak w ostatnim dniu świadczonego wsparcia wraz z dostępnością wykonywania oraz odtwarzania kopii bezpieczeństwa. |  |
| 10 |  | Nazwa producenta komputera |  |
| 11 |  | Model oferowanego komputera |  |

|  |
| --- |
| **SYSTEM OPERACYJNY SERWERA – 2 SZTUKI** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** |  **4** |
| 1 | Zastosowanie | Uruchomienie istniejących wirtualnych maszyn w klastrze serwerowym, integracja klastra z obecnie posiadaną infrastrukturą, instalacja nowych wirtualnych serwerów do zastosowań digitalizacyjnych wraz z oprogramowaniem opartym o strukturę Windows, instalacja serwerów pomocniczych, takich jak system DNS oraz dodatkowy kontroler domeny Active Directory, zgodnie z istniejącą w Muzeum Narodowym w Szczecinie infrastrukturą opisaną w załączniku nr 1. |  |
| 2 | System |  MS Windows Data Center zgodnie z opisem istniejącej infrastruktury IT, z którą system musi tworzyć jednolitą strukturę i być w pełni zgodnym. |  |
| 3 | Licencje dostępowe | 90 licencji dostępowych na użytkownika do oferowanych systemów. |  |
| 4 | Rodzaj | Rozbudowa posiadanych licencji MOLP. |  |
| 5 | Gwarancja | Wykonawca zagwarantuje dostępność bezpłatnych aktualizacji przez okres co najmniej 36 miesięcy. | Okres gwarancji ………………………. |
| 6 |  | Nazwa producenta komputera |  |
| 7 |  | Model oferowanego komputera |  |

|  |
| --- |
| **SZAFA DYSTRYBUCYJNA – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** | **4** |
| 1 | Zastosowanie | W szafie dystrybucyjnej będą zainstalowane serwery, macierze, zasilacze awaryjne, pionowe listwy PDU oraz urządzenia sieciowe przeznaczone do realizacji procesów digitalizacyjnych. |  |
| 2 | Obudowa | Rama spawana, stabilna o nośności do 2000kg, otworowana wraz z pionowymi otworami umożliwiającymi montaż elementów do organizacji okablowania oraz listew zasilających. Rama szafy wykonana z profili ocynkowanych, zabezpieczonej przed korozją. |  |
| 3 | Wymiary | Szerokość szafy 800mm, głębokość szafy 1200mm, wysokość szafy od 42U do 48U |  |
| 4 | Drzwi przednie | jednoczęściowe wyposażone z zamek 3 punktowy, |  |
| 5 | Drzwi tylne | Drzwi tylne dwuczęściowe(dzielone w pionie) wyposażone z zamek 3 punktowy, |  |
| 6 | Ściany boczne | wykonane z blachy stalowej, dzielone w poziomie na 2 lub 3 sekcje, demontowane oraz mocowane przy pomocy zamków, |  |
| 7 | Kolor | Szafy oraz drzwi jednolity  |  |
| 8 | Inne | * Szafa przystosowana pod montaż elementów RACK typu: organizatory, panele, urządzenia aktywne,
* Konstrukcja szafy ma umożliwiać swobodną eksploatację szafy
* Szafa musi mieć możliwość dowolnej konfiguracji przepustów kablowych,
* Szafa wyposażona w co najmniej 4 belki montażowe,
* Profile montażowe 19” z trwale oznaczoną wysokością U (numeryczny opis),
* Możliwość otwarcia drzwi przednich i tylnych co najmniej 180 stopni,
* Drzwi przednie oraz tylne z perforacją od 80% do 85%, oraz powierzchnią perforacji od 65% do 70%,
* Szafa wyposażona w listwę uziemiającą,
* Zapewniona możliwość prowadzenia okablowania po dachu,
* Dowolnej konfiguracji przepustów kablowych,
* Szafa musi być dostarczona złożona,
 |  |
| 9 | Gwarancja | Gwarancja producenta na okres co najmniej 36 miesięcy. Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 21 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji……………………… |
| 10 |  | Nazwa producenta komputera |  |
| 11 |  | Model oferowanego komputera |  |

|  |
| --- |
| **ZASILACZ AWARYJNY DO SZAFY SERWEROWEJ – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** |  **4** |
| 1 | Zastosowanie | Podtrzymanie napięcia w przypadku utraty zasilania dla wszystkich urządzeń znajdujących się w zamawianej szafie serwerowej |  |
| 2 | Obudowa | Obudowa w standardzie RACK wraz z niezbędnymi śrubami i elementami do instalacji w szafie.Wymiary urządzenia winny umożliwić montaż w szafie serwerowej z rozstawem 19 cali |  |
| 3 | Sprawność | Urządzenie po utracie zasilania umożliwi nieprzerwaną pracę urządzeń wymienionych w powyższym przetargu z przeznaczeniem do szafy na co najmniej 30 minut. |  |
| 4 | Moc | Co najmniej 6000VA, nie mniej jednak niż wymagana moc do zasilenia oferowanych urządzeń w przetargu |  |
| 5 | Akcesoria | Do zestawu winien być dołączony kabel umożliwiający podłączenie urządzenia do prądu, oraz kable umożliwiające wyłączenie serwerów oraz macierzy dyskowej z powyższych specyfikacji, patchcord LAN umożliwiający podłączenie systemu monitoringu zasilacza do przełącznika sieciowego o długości 5 metrów. |  |
| 6 | System monitoringu | Urządzenie winno być wyposażone w system monitoringu przez sieć LAN o co najmniej możliwościach:- Wyświetlenia przewidywanego czasu działania urządzenia po utracie prądu- Wyświetlenia faktycznego stanu pracy (prąd stały/ praca na bateriach)- Urządzenie winno być w stanie wysłać powiadomienie na adres e-mail o konieczności zmiany baterii- Podać nazwę oraz numer seryjny urządzenia- Posiadać interface www umożliwiający podgląd i konfigurację poprzez przeglądarkę www- Posiadać zabezpieczenie w postaci loginu i hasła w celu zmiany parametrów urządzenia- Posiadać rejestr zdarzeń, o zdarzeniach co najmniej: utrata zasilania, przywrócenie zasilania |  |
| 7 | Ekran LCD na urządzeniu | Urządzenie winno być wyposażone w ekran LCD o co najmniej możliwościach:- Wyświetlenia przewidywanego czasu działania urządzenia po utracie prądu- Wyświetlenia faktycznego stanu pracy (prąd stały/ praca na bateriach)- Wyświetlenie monitu o awarii urządzenia- Wyświetlanie parametrów prądu otrzymywanego na wejściu |  |
| 8 | Gwarancja | Wykonawca udzieli gwarancji co najmniej 36 miesięcy na urządzenie oraz 6 miesięcy na akumulatory. Samodzielna wymiana akumulatorów nie powoduje utraty gwarancji na urządzenie. Gwarantowany czas naprawy 30 dni. Czynności serwisowe będą wykonywane na miejscu u Zamawiającego.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady | 1. Okres gwarancji na urządzenie

…………………1. Okres gwarancji na akumulatory

 ………………… |
| 9 |  | Nazwa producenta komputera |  |
| 10 |  | Model oferowanego komputera |  |

|  |
| --- |
| **PRZEŁĄCZNIK SIECIOWY DYSTRYBUCYJNY Z FUNKCJĄ PoE – 1 SZTUKA**  |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów**  |
| **1** | **2** | **3** |  **4** |
| 1 | Zastosowanie | Zapewnienie łączności urządzeniom sieciowym podłączanym do sieci LAN, zapewnienie zasilania urządzeniom PoE |  |
| 2 | Obudowa | * Typu RACK.
* Wysokość urządzenia 1U.
 |  |
| 3 | Porty | * Co najmniej 48 porty 10/100/1000BASE-T POE+.
* Co najmniej 4 porty 10GbE SFP+ w tym dwa z obsługą modułów optycznych LRM.
* Co najmniej Dwa porty SFP+ z obsługą modułów optycznych LRM.
* Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
 |  |
| 4 | POE | * Budżet POE do podziału dla urządzeń co najmniej 370W.
* Dostępność POE na wszystkich 48 portach RJ45.
 |  |
| 5 | Obsługa SSH | * RFC 4252: SSH authentication protocol
* RFC 4253: SSH transport layer protocol
* RFC 4254: SSH connection protocol
* RFC 4251: SSH protocol architecture
* RFC 4716: SECSH public key file format
* RFC 4419: Diffie-Hellman group exchange
 |  |
| 6 | Obsługa SSL 3.0 oraz TLS 1.0 | * RFC 2246: Protokół TLS, wersja 1.0
* RFC 2818: HTTP over TLS
* RFC 3268: AES
 |  |
| 7 | Routing | * Obsługa Routingu statycznego.
* Obsługa statycznego routingu IPv6, co najmniej 60 tras.
* Obsługa dynamicznego routing IPv4 (RFC 2453 RIP v2).
 |  |
| 8 | VLAN | * Obsługa Multicast VLAN Registration (MVR).
* Obsługa Independent VLAN Learning (IVL).
 |  |
| 9 | ACL | * Obsługa Listy kontroli dostępu ACL co najmniej 9 na port.
 |  |
| 10 | Obsługa list kontroli dostępu dla ruchu przychodzącego na podstawie | * Czasu.
* Źródłowego i docelowego adresu IP.
* TCP/UDP źródłowy i docelowy.
* Rodzaju protokołu IP.
* EtherType.
* IEE 802.1p.
* Źródłowy i docelowy adres MAC.
* Vlan id.
 |  |
| 11 | Warunki pracy. | * Zakres temperatury pracy Co najmniej od 0-50 °C
* Zakres wilgotności od 10% do 95%.
 |  |
| 12 | Inne | * Nieblokująca architektura o wydajności przełączania co najmniej 176 Gb/s.
* Szybkość przełączania co najmniej 130.9 Milionów pakietów na sekundę.
* Tablica MAC adresów co najmniej 16k.
* Wsparcie dla ramek Jumbo Frames.
* Obsługa Quality of Service, IEEE 802.1p.
* Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
* Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
* Obsługa CDPv2.
* Obsługa Remote Switch Port Analyzer (RSPAN).
* Możliwość zarządzania przełącznikiem za pomocą systemu zarządzania z poziomu chmury obsługującego polityki oraz mechanizmy kontroli dostępu NAC.
* Obsługa mechanizmu Zero-touch provisioning z poziomu chmury oraz lokalnego systemu zarządzania.
* Możliwość monitoringu pakietów.
* Obsługa TACACS+ (RFC 1492).
* Obsługa klienta RADIUS RFC 2865.
* Obsługa IEEE 802.3x —Flow control.
* Obsługa minimum 4 instancji MSTP.
* Obsługa RFC 4541 (IGMP).
* Możliwość tworzenia stosu urządzeń. Stos zarządzany za pomocą jednego adresu IP.
* Obsługa Policy-Based Routing.
* Obsługa skryptów CLI.
 |  |
| 13 | Zasilanie | * Wbudowany port pozwalający na podłączenie zewnętrznego redundantnego zasilacza RPS.
* Urządzenie wyposażone w oryginalny kabel zasilania.
 |  |
| 14 | Zarzadzanie | * WEB
* GUI
* Możliwość utworzenia co najmniej 5 kont dostępu z różnicowanymi uprawnieniami
 |  |
| 15 | Dodatkowe wyposażenie | * Kabel połączeniowy RJ45 kat.6 o długości 50 cm – 25 Sztuk
* Kabel połączeniowy RJ45 kat.6 o długości 100 cm – 20 Sztuk
* Moduł SPF+ - 4 sztuki
 |  |
| 16 | Gwarancja | Gwarancja producenta Lifetime realizowana przez pięć lat po zakończeniu produkcji urządzenia. Wymiana urządzenia na sprawne na drugi dzień roboczy od momentu zgłoszenia.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady |  |
| 17 |  | Nazwa producenta komputera |  |
| 18 |  | Model oferowanego komputera |  |

|  |
| --- |
| **KVM – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** | **4** |
| 1 | Zastosowanie | KVM przeznaczony do sterowania serwerami. Urządzenie winno współpracować z oferowanymi serwerami. |  |
| 2 | Połączenia | Co najmniej 8 z możliwością połącznia kaskadowego do co najmniej 128 urządzeń |  |
| 3 | Porty | * 8 x SPHD-17 żeńskie (żółte)
 |  |
| 4 | Ekran | * Co najmniej 17”
* Co najmniej 16,7 mln kolorów
* Czas reakcji co najmniej 5 ms
* Kąt widzenia co najmniej 170° (w poziomie), co najmniej 160° (w pionie)
* Rozdzielczość co najmniej 1280 x 1024
 |  |
| 5 | Przewody | Komplet okablowania do podłączenia wszystkich serwerów oferowanych w ramach niniejszego postępowania oraz kable umożliwiające przyłączenie urządzenia do prądu |  |
| 6 | Gwarancja | Gwarancja na okres minimum 36 miesięcy wraz w wszystkimi akcesoriami i okablowaniem. Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji…………………….. |
| 7 | Obudowa | Przystosowana do montażu w oferowanej szafie RACK, nie wyższa niż 1U.Do zestawu dołączone będą wszystkie akcesoria i śruby umożliwiające montaż, złożenie i schowanie urządzenia w szafie RACK  |  |
| 8 | Klawiatura | W układzie qwerty, prawidłowo obsługująca układ klawiatury polski - programisty. Nie dopuszcza się przystosowania klawiatury poprzez różnego rodzaju nalepki na guziki. |  |
| 9 | Touchpad | Wbudowany, z co najmniej dwoma przyciskami symulującymi prawy i lewy przycisk myszy. |  |
| 10 | Energia | Urządzenie będzie automatycznie wyłączać ekran podczas składania go celem schowania w szafie, oraz wznawiać automatycznie po otworzeniu urządzenia. |  |
| 11 |  | Nazwa producenta komputera |  |
| 12 |  | Model oferowanego komputera |  |

|  |
| --- |
| **LISTWA PDU – 2 SZTUKI** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** |  **4** |
| 1 | Zastosowanie | Dystrybucja zasilania do urządzeń w szafie serwerowej z oferowanego zasilacza awaryjnego oraz z sieci elektrycznej, monitoring warunków klimatycznych  |  |
| 2 | Obudowa  | Listwa przeznaczona do montażu w szafie serwerowej w pozycji pionowej |  |
| 3 | Gniazda zasilające | Minimum 20 gniazd typu C13Minimum 4 gniazda typu C19 |  |
| 4 | Minimalna obciążalność listwy  | Minimum 16A |  |
| 5 | Wyposażenie  | Czujnik temperatury i wilgotności |  |
| 6 | Obsługa | Obsługa i zarządzanie listwą odbywa się poprzez protokół http lub https, oprogramowanie ma być zaimplementowane w listwie |  |
| 7 | Port komunikacyjny  | Co najmniej Ethernet  |  |
| 8 | Wyświetlacz | Informacja co najmniej o: Bieżący stan urządzeniaObciążenie prądu, Temperaturze, Wilgotności |  |
| 9 | Monity | W przypadku przekroczenia dopuszczalnych wartości temperatury, wilgotności zostanie wysłane powiadomienie pocztą elektroniczną za pośrednictwem systemu MS Office 365 |  |
| 10 | Monitoring www umożliwi | Kontrolę Całkowitego obciążenieObciążenie dla indywidualnych portówStan pojedynczego portu, Bieżący stan listwyTemperatura i wilgotnośćObecność dymu, Obecność wody czy innych płynów |  |
| 11 | Kontrola poprzez www umożliwi | WŁ/WYŁ wszystkich portów WŁ/WYŁ indywidualnych portów |  |
| 12 | Podłączenie | Dołączony kabel umożliwiający podłączenie do oferowanego UPS  |  |
| 13 | Gwarancja | Co najmniej 3 lata, jednak nie krócej niż gwarancja producentaWady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji………………………. |
| 14 |  | Nazwa producenta komputera |  |
| 15 |  | Model oferowanego komputera |  |

|  |
| --- |
| **PRZEŁĄCZNIK SIECIOWY SZKIELETOWY – 1 SZTUKA** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** |  **4**  |
| 1 | Zastosowanie | Zapewnienie łączności pomiędzy segmentami sieci a szafą dystrybucyjną, zapewnienie łączności pomiędzy serwerami a resztą sieci. |  |
| 2 | Porty | Przełącznik posiadający co najmniej 16 portów 10Gigabit Ethernet SFP+, mogących pracować co najmniej z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+Wraz z przełącznikiem należy dostarczyć co najmniej 4 wkładki SFP+ wraz okablowaniem (każdy o długości 2m) niezbędnym do podłączenia oferowanego przełącznika z oferowanymi serwerami |  |
| 3 | Obudowa | Umożliwiająca montaż w szafie RACK z rozstawem 19 cali, o maksymalnej wysokości 1U. |  |
| 4 | Przepustowość | Nieblokująca architektura o wydajności przełączania co najmniej 320 Gb/s |  |
| 5 | Łączenie przełączników | Możliwość łączenia co najmniej 8 przełączników w stos za pomocą portów 10G |  |
| 6 | Tablica MAC | Tablica MAC adresów min. 16k |  |
| 7 | Pamięć flash | Pamięć flash: min. 4 GB pamięci Flash |  |
| 8 | Obsługa vLAN | Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094Obsługa sieci wirtualnych protokołowych IEEE 802.1vObsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci |  |
| 9 | Obsługa Jumbo Frames | Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) |  |
| 10 | Obsługa podwójnie tagowanych ramek | Q-in-Q IEEE 802.1ad |  |
| 11 | Obsługa QoS | - IEEE 802.1p- DiffServ- kolejek priorytetów na każdym porcie wyjściowym |  |
| 12 | Obsługa Link Layer Discovery | Co najmniej protokół LLDP IEEE 802.1AB, Media Endpoint Discovery (LLDP-MED) |  |
| 13 | Pamięć | Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora |  |
| 14 | Redundancja zasilaczy | Przełącznik musi posiadać możliwość instalacji dwóch zasilaczy, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika. Zainstalowany co najmniej jeden zasilacz |  |
| 15 | Zabezpieczenie oprogramowania układowego | Możliwość instalacji co najmniej dwóch wersji oprogramowania – firmware, oraz cofnięcia oprogramowania do poprzedniej wersjiMożliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash |  |
| 16 | Monitoring urządzenia | Co najmniej możliwość monitorowania zajętości CPU,Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring) |  |
| 17 | Obsługa wirtualnych routerów | możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach |  |
| 18 | Port do zarządzania | Co najmniej wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem |  |
| 19 | Protokół CDP | Co najmniej w wersji 2 |  |
| 20 | Obsługa routingu IPv4 | Co najmniej:Sprzętowa obsługa routingu IPv4 – forwardingRouting statycznyObsługa routingu dynamicznego IPv4 co najmniej RIPv1/v2, OSPFv2 |  |
| 21 | Obsługa routingu IPv6 | Co najmniejSprzętowa obsługa routingu IPv6 – forwardingRouting statycznyObsługa routingu dynamicznego dla IPv6 co najmniej: RIPng, OSPF v3Telnet Serwer/Klient dla IPv6SSH2 Serwer/Klient dla IPv6Ping dla IPv6Tracert dla IPv6Obsługa MLDv1 (Multicast Listener Discovery version 1) |  |
| 22 | Obsługa multicastów | Co najmniej:Filtrowanie IGMPObsługa Multicast VLAN Registration – MVRObsługa IGMP v1/v2/v3 snooping |  |
| 23 | Bezpieczeństwo | Obsługa Network Login co najmniej: EEE 802.1x - RFC 3580, Web-based Network Login, MAC based Network LoginObsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)Możliwość integracji funkcjonalności Network Login z Microsoft NAPObsługa Guest VLAN dla IEEE 802.1xPrzydział sieci VLAN, ACL/QoS podczas logowania Network LoginMożliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authenticationObsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu KerberosObsługa Identity ManagementWbudowana obrona procesora urządzenia przed atakami DoSObsługa TACACS+Obsługa RADIUS AuthenticationObsługa RADIUS AccountingRADIUS and TACACS+ per-command AuthenticationBezpieczeństwo MAC adresów co najmniej: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresu na porcie, możliwość wpisania statycznych MAC adresów na port/vlanMożliwość wyłączenia MAC learningObsługa SNMPv1/v2/v3Klient SSH2Wysłanie informacji do serwera SyslogObsługa IP Security - Gratuitous ARP ProtectionObsługa IP Security – Trusted DHCP ServerObsługa IP Security – DHCP Secured ARP/ARP ValidationObsługa IP Security – IP Source guardOgraniczanie przepustowości (rate limiting) na portach wyjściowych |  |
| 24 | Bezpieczeństwo sieci | Co najmniej:Możliwość konfiguracji portu głównego i zapasowegoObsługa redundancji routingu VRRP - RFC 2338Obsługa STP (Spinning Tree Protocol) IEEE 802.1DObsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1wObsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1sObsługa PVST+Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619Obsługa G.8032Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portówObsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników |  |
| 25 | Administrowanie | Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)Obsługa synchronizacji czasu NTPZarządzanie przez SNMP v1/v2/v3Zarządzanie przez przeglądarkę WWW – protokół http i httpsMożliwość zarządzania przez protokół XMLSSH2 Serwer/Klient dla IPv4 / IPv6Ping dla IPv4 / IPv6Traceroute dla IPv4 / IPv6Obsługa SYSLOG z możliwością definiowania wielu serwerówSprzętowa obsługa sFlowObsługa RMON min. 4 grupy: Status, History, Alarms, EventsObsługa RMON2Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) |  |
| 26 | Gwarancja | Gwarancja producenta Lifetime realizowana przez pięć lat po zakończeniu produkcji urządzenia. Wymiana urządzenia na sprawne na drugi dzień roboczy od momentu zgłoszeniaWady przedmiotu będą usuwane przez Wykonawcę w ciągu 7 dni kalendarzowych od daty zgłoszenia wady |  |
| 27 | Zarządzanie | Dołączona aplikacja, która musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera Windows. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.Aplikacja musi być wyprodukowana i wspierana przez producenta oferowanych przełączników.Aplikacja zarządzająca musi obsługiwać co najmniej 10 urządzeń (adresów IP)Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego.Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub RadiusAplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AESAplikacja 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 systemówAplikacja 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 skryptuAplikacja musi posiadać wbudowany Syslog serwerAplikacja musi posiadać wbudowany BootP serwerAplikacja musi wspierać protokół IPv4 oraz IPv6Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratoraAplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniachAplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości, stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów, konfiguracji sieci VLAN, konfiguracji protokołu routingu OSPFAplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/httpsAplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane: adres IP urządzenia, adresu MAC urządzenia, nazwy urządzenia, wersji oprogramowania, wersji bootrom, lokalizacji urządzenia, 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 producentówAplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasieAplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniachAplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na kontrolę dostępu do sieci dla urządzeń końcowych (NAC)System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.System zarządzania musi być objęty co najmniej pięcioletnim wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7. |  |
| 28 |  | Nazwa producenta komputera |  |
| 29 |  | Model oferowanego komputera |  |

|  |
| --- |
| **TAŚMY LTO – 20 SZTUK** |
| **L.p.** | **Element konfiguracji** | **Wymagania minimalne** | **Potwierdzenie zgodności parametrów** |
| **1** | **2** | **3** |  **4** |
| 1 | Zastosowanie | Nośniki danych do oferowanego napędu LTO |  |
| 2 | Rodzaj taśm | Co najmniej LTO7, jednak pasujące do oferowanego napędu ze specyfikacji nr 3  |  |
| 3 | Oznaczenie taśm | Załączone identyfikatory taśm używana w oferowanym napędzie ze specyfikacji nr 3 dla co najmniej wszystkich taśm  |  |
| 4 | Opakowanie | Do każdej taśmy winno być dołączone opakowanie zabezpieczające |  |
| 5 | Gwarancja | Gwarancja na 6 miesięcy jednak nie krócej niż gwarancja producenta.Wady przedmiotu będą usuwane przez Wykonawcę w ciągu 30 dni kalendarzowych od daty zgłoszenia wady | Okres gwarancji ……………………… |
| 6 |  | Nazwa producenta komputera |  |
| 7 |  | Model oferowanego komputera |  |

Miejscowość i data podpis osoby/osób uprawnionej

 do reprezentowania Wykonawcy

…………………………… …………………………………………..

**II. Formularz cenowy**

Uwaga! Formularz cenowy Wykonawca sporządza we własnym zakresie, w formie indywidualnej kalkulacji, wyszczególniając w nim wszystkie wymagane elementy przedmiotu zamówienia wyspecyfikowane w części I niniejszego załącznika pn. Specyfikacja techniczna sprzętu, z podziałem na poszczególne pozycje asortymentowe. W cenach poszczególnych pozycji należy uwzględnić wszystkie pozostałe koszty wykonawcy takie jak np. transport, załadunek, montaż, instalacja, itp., w taki sposób aby suma wszystkich wartości brutto była równa z ceną brutto oferty.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Oferowany przedmiot zamówienia (opis, w tym producent, typ, model)** | **Ilość (w szt.)** | **Cena jedn.netto** | **Cena jedn.brutto** | **Łączna wartość netto** | **Stawka VAT** | **Łączna wartość brutto** |
|  **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **1** | **Serwer typu RACK**  | **2 sztuki** |  |  |  |  |  |
| **2** | **Macierz dyskowa**  | **1 sztuka** |  |  |  |  |  |
| **3** | **Napęd taśmowy LTO** | **1 sztuka** |  |  |  |  |  |
| **4** | **UTM** | **1 sztuka** |  |  |  |  |  |
| **5** | **Oprogramowanie do backupu** | **1 sztuka** |  |  |  |  |  |
| **6** | **System operacyjny serwera**  | **2 sztuki** |  |  |  |  |  |
| **7** | **Szafa dystrybucyjna** | **1 sztuka** |  |  |  |  |  |
| **8** | **Zasilacz awaryjny do szafy serwerowej** | **1 sztuka**  |  |  |  |  |  |
| **9** | **Przełącznik sieciowy dystrybucyjny z funkcją PoE** | **1 sztuka** |  |  |  |  |  |
| **10** | **KVM** | **1 sztuka** |  |  |  |  |  |
| **11** | **Listwa PDU** | **2 sztuki** |  |  |  |  |  |
| **12** | **Przełącznik sieciowy szkieletowy** | **1 sztuka** |  |  |  |  |  |
| **13** | **Taśmy LTO** | **20 sztuk** |  |  |  |  |  |

\*\* Tak obliczoną cenę należy przenieść do formularza ofertowego – załącznik nr 2 do SIWZ

Miejscowość i data podpis osoby/osób uprawnionej

 do reprezentowania Wykonawcy

…………………………… …………………………………………..

**Załącznik nr 4 – oświadczenie o spełnieniu warunków udziału w postępowaniu**

|  |
| --- |
| (wykonawca) |

**OŚWIADCZENIE WYKONAWCY O SPEŁNIENIU WARUNKÓW UDZIAŁU WPOSTĘPOWANIU**

**składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych dotyczące spełniania warunków udziału w postępowaniu**

Na potrzeby postępowania o udzielenie zamówienia publicznego na: **Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie**

oświadczam co następuje:

Ja niżej podpisany

działając w imieniu i na rzecz:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

(nazwa i adres Wykonawcy NIP/PESEL, KRS/CEiDG)

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Dziale VI. WARUNKI UDZIAŁU W POSTĘPOWANIU Ogłoszenia o zamówieniu, znak postępowania: **AZ.2710.15.2019.MS**

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

………………………. dnia ………… r. ……………………………..

 (miejscowość) (podpis Wykonawcy

**Załącznik nr 5 do SIWZ - Przykładowy wzór zobowiązania podmiotu trzeciego**

..............................................................

(pieczęć wykonawcy)

**ZOBOWIĄZANIE**

**do oddania do dyspozycji niezbędnych zasobów**

**na potrzeby wykonana zamówienia**

Ja(/My) niżej podpisany(/ni) …………………………….……………..……………… będąc

*(imię i nazwisko składającego oświadczenie)*

upoważnionym(/mi) do reprezentowania:

…………………………….………………………………….………………………………

*(nazwa i adres podmiotu oddającego do dyspozycji zasoby)*

**o ś w i a d c z a m(y)**,

że wyżej wymieniony podmiot, stosownie do art. 22a ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 z późn. zm.), odda wykonawcy:

…………………………………………………………………....………………………………………………………………………………………

*(nazwa i adres wykonawcy składającego ofertę)*

do dyspozycji w trakcie realizacji zamówienia niezbędne zasoby1.

…………………………………………………………………………………………………………………………………………………………….

…………………………………………………………………………………………………………………………………………………………….

*(zakres udostępnianych zasobów)*

na potrzeby wykonania zamówienia: Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie

Sposób wykorzystania ww. zasobów przez wykonawcę przy wykonywaniu zamówienia2: …………........…………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………….

…………………………………………………………………………………………………………………………………………………………….

Charakter stosunku, jaki będzie łączył nas z wykonawcą3: …………………………………………………………………………………………………………………………………………………………….

…………………………………………………………………………………………………………………………………………………………….

……………………………………………………………………………………………………………………………………………………………

………………………………………….. ….……………………………………

*(miejsce i data złożenia oświadczenia) (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli w imieniu podmiotu oddającego do dyspozycji zasoby)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Zakres udostępnianych zasobów niezbędnych do potwierdzenia spełniania warunku:
* zdolności techniczne lub zawodowe
* zdolności finansowe lub ekonomiczne
1. np. podwykonawstwo, konsultacje, doradztwo. W sytuacji gdy przedmiotem udzielenia są zasoby nierozerwalnie związane z podmiotem ich udzielającym, niemożliwe do samodzielnego obrotu i dalszego udzielenia ich bez zaangażowania tego podmiotu w wykonanie zamówienia, taki dokument powinien zawierać wyraźne nawiązanie do uczestnictwa tego podmiotu w wykonaniu zamówienia.
2. np. umowa cywilno-prawna, umowa o współpracy.

**Załącznik nr 6 – Oświadczenie o braku podstaw wykluczenia**

**Wykonawca:**

……………………………………………………………………………………………………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

…………………………………………………………………………………………………………………………………………………………..

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**OŚWIADCZENIE WYKONAWCY DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

**składane na podstawie art. 25a ust. 1 ustawy Pzp**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.: Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie prowadzonego przez Muzeum Narodowe w Szczecinie, oświadczam co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie
art. 24 ust 1 pkt 12-23 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie
art. 24 ust. 5 pkt 1) i 8) ustawy Pzp .

 …………….……………….. *(miejscowość),* dnia ………….…………………. r.

 …………………………………………

 *(podpis)*

1. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …………. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze: ………………………………………………………………………………………………………………..…………………………………………………………………………………………..…………………...........……………………………………………………………

………………….……. *(miejscowość),* dnia ………………………... r.

 ………………………………………………

*(podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:**

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby

powołuję się w niniejszym postępowaniu, tj.: …………………………………………………………………………

…………………………………………………………………………………………………………………………………………………

*(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

 …………….……. *(miejscowość),* dnia …………………. r.

 …………………………………………

 *(podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

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 …………………. r.

 …………………………………………

 *(podpis)*

**Załącznik nr 7 - Informacja Wykonawcy o przynależności do grupy kapitałowej**

|  |
| --- |
| (Wykonawca) |

**Informacja Wykonawcy**

Przystępując do udziału w postępowaniu o zamówienie publiczne na:

 **Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie**

informuję, że

**należę/ nie należę\***

do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), o której mowa w art. 24 ust. 1 pkt. 23 Ustawy Pzp.

Wobec tego, że w niniejszym postępowaniu składa ofertę inny Wykonawca należący do grupy kapitałowej, do której należy Wykonawca składający niniejszą ofertę, poniżej wyjaśniam, że istniejące między nami powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia:

|  |  |
| --- | --- |
| Podmiot składający ofertę należący do grupy kapitałowej wspólnie z Wykonawcą | Uzasadnienie |
|  |  |

………………………………….. …………………………………….

*miejscowość i data podpis osoby/osób uprawnionej do*

 *reprezentowania Wykonawcy*

**Uwaga! *W przypadku gdy Wykonawca należy do grupy kapitałowej wraz z informacją zobowiązany jest złożyć listę podmiotów należących do tej samej grupy kapitałowej.***

*\* niepotrzebne skreślić*

**Załącznik nr 8 – Wykaz zrealizowanych zamówień**

|  |
| --- |
|  (wykonawca) |

**WYKAZ DOSTAW**

W odpowiedzi na ogłoszenie o przetargu nieograniczonym na: **Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie** prowadzonego przez Muzeum Narodowe w Szczecinie, oświadczam co następuje:

ja/ my niżej podpisany/podpisani

…………………………………………………………………………………………………………………………………………………………

działając w imieniu

……………………………………………………………………………………………………………………………………………………………

oświadczam/y że ww. Wykonawca posiada następujące doświadczenie zawodowe:

Wykonawca musi wykazać się doświadczeniem, polegającym na tym, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał przynajmniej 1 zamówienie polegające na dostawie sprzętu serwerowego (wyposażenie szafy serwerowej) o wartości nie mniejszej niż 200 000,00 zł brutto .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Wykonawca** | **Zamawiający** |  **Przedmiot dostawy** | **Wartość zamówienia**  | **Okres realizacji**  |
| **Początek****dzień/miesiąc/rok** | **Koniec****dzień/miesiąc/rok** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**UWAGA!!!**

**Na wezwanie Zamawiającego na potwierdzenie okoliczności, o których mowa w art.25 ust.1 pkt 1 ustawy w celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu dotyczących zdolności technicznej lub zawodowej zamawiający będzie żądał od Wykonawcy złożenia wraz z wykazem dowodów potwierdzających, że wskazane dostawy zostały wykonane lub są wykonywane należycie.**

miejscowość i data podpis osoby/osób uprawnionej do ……………………………. reprezentowania Wykonawcy

 ……………………………………………



**Załącznik nr 9 – wzór umowy**

**Umowa nr ………………..**

Zawarta w dniu ............................

pomiędzy:

Muzeum Narodowym w Szczecinie z siedzibą przy ul. Staromłyńskiej 27 w Szczecinie, wpisanym do rejestru Instytucji Kultury Województwa Zachodniopomorskiego pod nr 2/99/WZ, dla której organizatorem jest Samorząd Województwa Zachodniopomorskiego oraz Minister Kultury i Dziedzictwa Narodowego,

NIP 851-00-13-721, REGON 000276860

zwanym dalej **Zamawiającym** i

reprezentowanym przez :

p. Lecha Karwowskiego – Dyrektora Muzeum

za kontrasygnatą głównej księgowej-

a

…………………………………………, z siedzibą ……………………………………………, wpisaną do Rejestru ……………………………………………., pod numerem KRS: ………………………………, NIP……………………………………, REGON……………………………

zwanym dalej Wykonawcą

reprezentowanym przez :

p. .................

**§1**

**Podstawa prawna**

Umowa niniejsza zawarta została zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych ( Dz.U. z 2018 r poz. 1986 z późn.zm.) w wyniku przeprowadzenia postępowania w trybie przetargu nieograniczonego z zachowaniem zasad określonych ww. ustawą.

**§2**

**Przedmiot umowy**

* 1. Przedmiotem niniejszej umowy jest realizacja przez Wykonawcę zamówienia polegającego na „Dostawie infrastruktury serwerowej do Muzeum Narodowego w Szczecinie
	2. Szczegółowy opis przedmiotu zamówienia zawiera Specyfikacja istotnych warunków zamówienia wraz z załącznikiem nr 1 Opisem przedmiotu zamówienia – załącznik nr 1 do umowy, oferta wykonawcy –załącznik nr 2 do umowy, oraz formularz cenowo –przedmiotowy – załącznik nr 3 do umowy.
	3. Wykonawca gwarantuje, iż przedmiot umowy jest wolny od wad fizycznych i prawnych
	4. Wykonawca gwarantuje że licencje udzielane przez producenta powinny być nieograniczone czasowo, niewyłączne, , do wykorzystania na terenie Polski w tym obejmować co najmniej następujące pola eksploatacji: utrwalanie na dowolnym nośniku, zwielokrotniania dowolną techniką, wprowadzania do pamięci urządzeń, udostępniania w sieci Internet i innych sieciach komputerowych (publiczne udostępnianie Oprogramowania w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym)

**§3**

**Obowiązki Wykonawcy**

* 1. Wykonawca dostarczy do Muzeum Narodowego w Szczecinie ( Staromłyńska 27 lub Wały Chrobrego 3 – do ustalenia przed dostawą), fabrycznie nowy, kompletny, gotowy do pracy sprzęt zgodny z wymienionym na załączonym do oferty formularzu cenowo – przedmiotowym.
	2. Wykonawca zapewni Zamawiającemu przed podpisaniem protokołu odbioru możliwość włączenia każdego urządzenia, sprawdzenia jego parametrów, sprawdzenia sterowników oraz funkcjonalności i wersji oprogramowania układowego.
	3. Wykonawca dostarczy sprzęt z wgranymi najnowszymi dostępnymi sterownikami producentów komponentów urządzenia.
	4. Wykonawca dostarczy sprzęt z wgraną najnowszą dostępną wersją oprogramowania układowego.
	5. Wykonawca dostarczy sprzęt z najnowszą wersją systemu operacyjnego z zainstalowanymi wszystkimi poprawkami wydanymi do daty co najwyżej trzech miesięcy wstecz od daty dostawy urządzeń.
	6. Poza standardowymi składnikami systemu operacyjnego oraz oprogramowaniem producenta do aktualizacji sterowników i diagnostyki urządzenia zabrania się instalacji jakiegokolwiek oprogramowania dodatkowego, w tym oprogramowania antywirusowego firm trzecich w jakiejkolwiek wersji, instalacji pakietów biurowych oraz instalatorów pakietów biurowych, wszelakiego typu gier.
	7. Przed przystąpieniem do odbioru końcowego Wykonawca przekaże Zamawiającemu:

* 1. licencje wymagane w OPZ przy danym urządzeniu
	2. instrukcje obsługi w języku polskim,
	3. dokumenty potwierdzające udzielenie gwarancji
	4. certyfikaty CE
	5. oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – dotyczy serwera typu RACK oraz macierzy dyskowej
	6. Oświadczeń Wykonawcy potwierdzonego, że naprawy gwarancyjne będą realizowane przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta – dotyczy serwerów, UTM oraz macierzy
	7. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzacje producenta w zakresie sprzedaży oferowanych rozwiązań- dotyczy UTM
	8. Oświadczenie producenta oferowanego urządzenia potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta – serwer typu Rack, macierz dyskowa, przełączniki sieciowe
	9. Wykonawca dostarczy wydruk ze strony www.cpubenchmark.net z datą pomiędzy podpisaniem umowy a dostawą urządzeń, świadczący o osiągach dostarczonych procesorów.

8) Zamawiający zobowiązuje Wykonawcę do przeprowadzenia instruktażu w zakresie konfiguracji i użytkowania danych urządzeń w ciągu 12 miesięcy od realizacji zamówienia w terminie obustronnie uzgodnionym.

9) Wykonawca zachowa należytą staranność we wszystkich w/w czynnościach.

**§4**

**Termin wykonania**

Wykonawca zobowiązuje się zrealizować całość przedmiotu zamówienia w terminie ……………………… dni od dnia zawarcia umowy.

**§ 5**

**Odbiór**

1) Wykonawca zobowiązany jest w terminie co najmniej 1 dnia roboczego przed planowaną datą dostawy sprzętu w formie pisemnej na adres email: r.piątkowski@muzeum.szczecin.pl do zawiadomienia i uzgodnienia z Zamawiającym dokładnej godziny oraz miejsca przekazania przedmiotu umowy.

2) Wykonawca po wykonaniu czynności określonych w § 3 pkt. 1) - 7) zgłosi Zamawiającemu gotowość do przystąpienia do odbioru sprzętu. **Zgłoszenie uznaje się za nieskuteczne w przypadku nie dopełnienia którejkolwiek z ww. czynności.**

3) Zamawiający przeprowadzi odbiór zamówienia potwierdzony protokołem odbioru stwierdzającym realizację przez Wykonawcę wszystkich czynności opisanych w § 3.

4) W dniu dostawy sprzętu winien być obecny przedstawiciel Wykonawcy upoważniony do podpisania protokołu odbioru.

6) Protokół odbioru przedmiotu umowy będzie sporządzony przez upoważnionych przedstawicieli stron umowy.

7) Osobą upoważnioną do reprezentowania Zamawiającego w sprawach związanych z realizacją niniejszej umowy, w tym do podpisania protokołu odbioru jest:

 P. Rafał Piątkowski tel. 797 705 227 e-mail: r.piątkowski@muzeum.szczecin.pl;

8) Osobą upoważnioną do reprezentowania Wykonawcy w sprawach związanych z realizacją niniejszej umowy jest:

……………………………………………………………………………………………………………………………………………………….

9) Zamówienie winno być zrealizowane w dni robocze tj. od poniedziałku do piątku w godzinach od 9.00 do 14.00.

**§ 6**

**Wynagrodzenie**

1) Wysokość wynagrodzenia przysługującego Wykonawcy za wykonanie przedmiotu umowy ustalona została na podstawie oferty Wykonawcy.

2) Wynagrodzenie ryczałtowe za prawidłowo wykonany przedmiot umowy ustala się na kwotę netto: ……………….…………...PLN, słownie: (……………………..), co po doliczeniu należnej stawki podatku VAT (wg. stawki .....%) daje kwotę brutto:……………………PLN, słownie: (………………………………..........................................................).

1. Kwota wskazana w ust. 2) obejmuje wszystkie czynności konieczne do wykonania przedmiotu umowy wskazane w § 3.
2. Wykonawca otrzyma wynagrodzenie na podstawie wystawionej faktury VAT po wykonaniu całości przedmiotu umowy.
3. Wynagrodzenie płatne będzie na numer konta Wykonawcy w terminie 30 dni od dnia doręczenia prawidłowo wystawionej faktury wraz z potwierdzającym wykonanie zamówienia protokołem odbioru końcowego.
4. Wynagrodzenie Wykonawcy za wykonanie przedmiotu umowy nie podlega waloryzacji.
5. Dniem zapłaty jest dzień obciążenia rachunku Zamawiającego.
6. Wykonawca wyraża zgodę na potrącenie z wynagrodzenia wszelkich wymagalnych roszczeń przysługujących Zamawiającemu na gruncie niniejszej umowy, w szczególności odszkodowawczych, wykonania zastępczego oraz z tytułu kar umownych.

**§ 7**

**Faktury elektroniczne**

1. Wykonawca może wystawiać ustrukturyzowane faktury elektroniczne w rozumieniu przepisów ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. poz. 2191, dalej – „Ustawa o Fakturowaniu”).
2. W przypadku wystawienia faktury, o której mowa w ust. 1, Wykonawca jest obowiązany do jej ustrukturyzowania wysyłając ją do Zamawiającego za pośrednictwem Platformy Elektronicznego Fakturowania na adres / konto jaki Zamawiający przekaże Wykonawcy najpóźniej do dnia odbioru końcowego.
3. Wystawiona przez Wykonawcę ustrukturyzowana faktura elektroniczna winna zawierać elementy, o których mowa w art. 6 Ustawy o Fakturowaniu, a nadto faktura ta, lub załącznik do niej musi zawierać numer Umowy i zamówienia, których dotyczy.
4. Za chwilę doręczenia ustrukturyzowanej faktury elektronicznej uznawać się będzie chwilę wprowadzenia prawidłowo wystawionej faktury, zawierającej wszystkie elementy, o których mowa w ust. 3 powyżej, do konta Zamawiającego na PEF, w sposób umożliwiający Zamawiającemu zapoznanie się z jej treścią.
5. W przypadku wystawienia faktury w formie pisemnej, prawidłowo wystawiona faktura powinna być doręczona do Sekretariatu Zamawiającego na adres jego siedziby.

**§ 8**

**Gwarancja i rękojmia za wady**

1) Wykonawca oświadcza, że udziela na przedmiot dostawy gwarancji oraz rękojmi za wady na okresy zadeklarowane na załączonym do oferty wykonawcy „Formularzu cenowo – przedmiotowym” –załączniku nr 3 do niniejszej umowy –co potwierdza niniejsza umowa.

2) Wykonawca oświadcza, że udzielona gwarancja obejmuje również gwarancję zgodności dostarczonego systemu operacyjnego z dostarczonym sprzętem – odpowiednio w zakresie jego przeznaczenia .

3) Wykonawca oświadcza, że zapewnia wsparcie techniczne w trybach oraz na warunkach określonych w poszczególnych Specyfikacjach technicznych (Załącznik nr 1 – opis przedmiotu zamówienia).

4) Wykonawca oświadcza, że w okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania układowego oraz sterowników zgodnie z poszczególnymi Specyfikacjami technicznymi (Załącznik nr 1 – opis przedmiotu zamówienia).

5) Otwarcie obudowy urządzenia nie ma wpływu na gwarancję.

6) Montaż rozszerzenia urządzeń przez Zamawiającego, takiego jak dodatkowa pamięć RAM, dodatkowy dysk czy standardowa karta rozszerzeń nie powoduje utraty gwarancji na urządzenia.

7) Za uszkodzoną matrycę podlegającą naprawie gwarancyjnej przyjmuje się uszkodzenie co najmniej jednego piksela (tak zwanego martwego piksela) w urządzeniu KVM oraz w panelach LCD urządzeń.

8) Okres gwarancji oraz rękojmi za wady rozpoczyna się z dniem podpisania protokołu odbioru końcowego.

9) Naprawy gwarancyjne będą realizowane przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta (dotyczy serwerów, macierzy dyskowej, UTM)

10) Naprawy gwarancyjne dotyczące przełączników sieciowych będą realizowane przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta jeżeli wykonawca zadeklarował w formularzu ofertowym posiadanie takiej autoryzacji.

10) Udzielona gwarancja nie wyłącza, nie ogranicza ani nie zawiesza uprawnień Zamawiającego wynikających z niezgodności dostarczonego sprzętu z umową.

11) W ramach udzielonej gwarancji Zamawiający ma prawo żądać dokonania bezpłatnej naprawy lub wymiany rzeczy na nową. W obu przypadkach Wykonawca zobowiązany jest również do wykonania na swój koszt takich czynności jak opakowanie, transport uwzględniający odbiór z siedziby Zamawiającego, załadunek, rozładunek itp.

12) Zgłoszenie wady przez Zamawiającego ma formę pisemną i kierowane jest w formie elektronicznej na adres e-mail:

 …………………………………………………………………………………………………………………………………,

 lub faksem na nr:

 ………………………………………………………………………………………………………………………………… .

13) Wykonawca obowiązany jest przystąpić do usunięcia zgłoszonej przez Zamawiającego wady najpóźniej w ciągu 2 dni kalendarzowych od daty otrzymania zawiadomienia od Zamawiającego.

14) Wady Przedmiotu Umowy będą usuwane przez Wykonawcę w terminie określonym w Specyfikacjach technicznych w ( Załącznik nr 1 do Siwz – Opis przedmiotu zamówienia). Termin ten w szczególnych przypadkach może ulec wydłużeniu, jeżeli Wykonawca uzgodni to (pisemnie – w tym również w drodze elektronicznej ) z Zamawiającym.

15) W przypadku, gdy Wykonawca nie dokona naprawy lub wymiany wadliwego Przedmiotu Umowy, w terminie określonym w ust. 14, Zamawiający ma prawo dokonać naprawy lub zakupu nowego urządzenia (o takich samych parametrach) na koszt i ryzyko Wykonawcy.

16) Zamawiającemu przysługuje prawo do wymiany wadliwej części Przedmiotu Umowy na wolną od wad na koszt Wykonawcy po wykonaniu 2 napraw gwarancyjnych, o ile nadal występują wady uniemożliwiające eksploatację określonej części Przedmiotu Umowy. Żądanie wymiany należy zgłosić na piśmie wg zasad określonych w ust 10.

17) Jeżeli w wykonaniu obowiązku gwarancji następuje wymiana rzeczy wadliwej na rzecz wolną od wad, albo została dokonana istotna naprawa wadliwej rzeczy, termin gwarancji biegnie na nowo, licząc od dnia dostarczenia rzeczy wolnej od wad lub od dnia zwrotu rzeczy naprawionej. W przypadku wymiany części rzeczy, zasady te stosuje się odpowiednio.

18) Usunięcie zgłoszonej wady Wykonawca zgłasza pisemnie, podając przyczynę wystąpienia wady oraz opisując sposób jej usunięcia. Zamawiający potwierdza usunięcie wady – przy czym uprawniony jest do zażądania aby Wykonawca osobiście zademonstrował, iż naprawiony sprzęt działa prawidłowo. Brak potwierdzenia usunięcia zgłoszonej wady ze strony Zamawiającego w ciągu siedmiu dni od zwrotu naprawionej rzeczy jest równoznaczny z jego pozytywnym odbiorem z naprawy.

**§ 9**

**Kary umowne**

1) Za niewykonywanie lub nienależyte wykonywanie przedmiotu umowy strony ponoszą odpowiedzialność w formie kar umownych. Zamawiający ma prawo naliczyć Wykonawcy karę umowną:

a) za niedotrzymanie terminu wykonania całego przedmiotu umowy w wysokości 0,1 % wartości wynagrodzenia brutto, za każdy dzień zwłoki,

b) za niedotrzymanie terminów usunięcia wad w okresie gwarancji i rękojmi w wysokości 0,1 % wartości brutto sprzętu, który podlega naprawie (zgodnie z wartościami określonymi na załączonym do oferty wykonawcy wypełnionym formularzu cenowo – przedmiotowym), za każdy dzień zwłoki,

e) za niedotrzymanie terminów usunięcia wad przy odbiorze w wysokości 0,02% wynagrodzenia brutto za każdy dzień zwłoki,

c) z tytułu odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy w wysokości 20% wynagrodzenia brutto należnego za realizację tej części umowy, od której wykonania odstąpiono.

2) Jeżeli kara umowna nie pokryje poniesionej przez Zamawiającego szkody, może on dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

3) Wykonawca oświadcza, że wyraża zgodę na potrącanie z należnego mu wynagrodzenia lub zabezpieczenia należytego wykonania umowy naliczonych kar umownych.

**§ 10**

**Zabezpieczenie należytego wykonania**

1) W celu zabezpieczenia ewentualnych roszczeń Zamawiającego wynikających z niewykonania lub nienależytego wykonania umowy, Wykonawca wniósł zabezpieczenie należytego wykonania w wysokości 10 % wynagrodzenia brutto tj. na kwotę ……………….. zł (słownie: …………………………………………………………….).

2) Zabezpieczenie zostało wniesione w formie: ……………………………………..

3) Wykonawca zobowiązuje się do utrzymania zabezpieczenia przez cały okres obowiązywania umowy tj. od dnia podpisania umowy do upływu terminu gwarancji plus 15 dni.

4) W przypadku, gdy termin wykonania przedmiotu umowy ulegnie przesunięciu, Wykonawca zobowiązany jest na co najmniej 14 dni przed upływem ważności zabezpieczenia przedłużyć jego ważność lub wnieść nowe zabezpieczenie na przedłużony okres realizacji umowy + gwarancji.

5) Jeżeli Wykonawca nie przedłuży zabezpieczenia zgodnie z ust. 4 to Zamawiający będzie uprawniony do zatrzymania należnego Wykonawcy wynagrodzenia równego kwocie zabezpieczenia na pokrycie ewentualnych roszczeń z tytułu niewykonania lub nienależytego wykonania zobowiązania.

6) Zabezpieczenie zostanie zwrócone Wykonawcy w następujący sposób:

70% kwoty zabezpieczenia w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego wszystkich dostaw za należycie wykonane w protokole odbioru.

30% kwoty zabezpieczenia w terminie 15 dni od dnia upływu okresu udzielonej gwarancji.

7) Zabezpieczenie należytego wykonania umowy służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania przedmiotu umowy, w tym roszczeń z tytułu rękojmi za wady.

**§ 11**

**Odstąpienie od umowy**

1) Zamawiający może odstąpić od umowy w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym.

2) Zamawiający zastrzega sobie prawo odstąpienia od umowy w każdym czasie w przypadku stwierdzenia nienależytego wykonania postanowień umownych przez Wykonawcę, lub występowania okoliczności uzasadniających naliczanie kar umownych.

3) Odstąpienie od umowy w przypadku określonym w ust. 1) oraz ust. 2) nastąpi jeżeli Wykonawca nie dotrzyma swojego zobowiązania pomimo uprzedniego wezwania wraz z informacją o skutku nie dotrzymania zobowiązania w terminie wyznaczonym przez Zamawiającego.

4) W przypadku odstąpienia od umowy, o jakim mowa w ust. 1 Wykonawca może żądać wynagrodzenia jedynie za część umowy wykonaną do daty odstąpienia.

5) W przypadku gdy Wykonawca jako kryterium oceny ofert zadeklaruje posiadanie autoryzacji producenta dostarczonych przełączników sieciowych i nie przekaże jej przed przystąpieniem do odbioru końcowego, Zamawiający może odstąpić od umowy.

6) Prawo do odstąpienia od umowy przysługuje w ciągu 90 dni od dnia powzięcia wiadomości od okoliczności stanowiącej podstawę odstąpienia.

**§ 12**

**Zmiana umowy**

1) Zmiana postanowień umowy może nastąpić wyłącznie za zgodą obu Stron oraz w przypadkach określonych w pkt 2, wyrażoną w formie pisemnego aneksu-pod rygorem nieważności.

2) Zmiany umowy mogą zostać dokonane w następujących okolicznościach i w następującym zakresie:

a) Zmian ogólnie obowiązujących przepisów prawa powszechnego i/lub miejscowego oraz wymogów dotyczących zamawiającego bezpośrednio odnoszących się do praw i obowiązków stron umowy; zmiany umowy z tego tytułu dokonane mogą być tylko w zakresie niezbędnym do stosowania zapisów umowy do wprowadzonych przepisów,

b) Zmian w terminie realizacji przedmiotu umowy, jeżeli ulegnie on przesunięciu o czas występowania przeszkód o obiektywnym, nadzwyczajnym i niemożliwym do przewidzenia charakterze, w szczególności takim jak niedobory rynkowe, przedłużający się czas dostawy u producenta, itp.

c) Zmian w terminie realizacji przedmiotu umowy, z przyczyn leżących po stronie Zamawiającego, w szczególności wstrzymania terminu dostawy bądź niemożliwości realizacji umowy w wyniku działań osób trzecich.

d) Zmian w zakresie poszczególnych elementów zamówienia, jeżeli w okresie realizacji zamówienia, na rynku pojawi się nowy produkt o parametrach lepszych od zaoferowanego elementu, a zmiana taka zostanie uzgodniona z Zamawiającym i nie wpłynie ona na wartość zamówienia. W takim przypadku ulec może również zmianie termin dostawy.

e) aktualizacji rozwiązań ze względu na postęp techniczny lub technologiczny (np. wycofanie z obrotu urządzeń lub podzespołów), zmiana nie może spowodować podwyższenia ceny oraz obniżenia parametrów technicznych, jakościowych i innych wynikających z oferty. W takim przypadku ulec może również zmianie termin dostawy.

f) Rezygnacji z części zamówienia w przypadku, gdy uzyskanie określonego elementu nie leży już w interesie Zamawiającego bądź występują problemy na rynku z uzyskaniem tego elementu. W takim przypadku wynagrodzenie wykonawcy zostanie odpowiednio pomniejszone o wartość tego elementu.

g) zmiany związane ze zmianami prawa dotyczącego ochrony danych osobowych

3) Ustała się, iż nie stanowi zmiany umowy w rozumieniu art. 144 ustawy:

1. zmiana nr rachunku bankowego Wykonawcy,
2. zmiana osób wyznaczonych do nadzoru nad realizacją umowy,
3. zmiana danych teleadresowych,

Zaistnienie okoliczności, o których mowa w niniejszym punkcie wymaga jedynie niezwłocznego pisemnego zawiadomienia drugiej strony.

**§ 13**

**Podwykonawcy**

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.

**§ 14**

 **Ochrona danych osobowych**

1) Realizacja umowy wymaga gromadzenia danych osobowych (informacji i danych objętych wymianą w związku z niniejszą Umową, które są powiązane z jakąkolwiek zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną lub, w zakresie sprzeczności z obowiązującymi przepisami prawa, które podlegają obowiązującym przepisom o ochronie danych osobowych). Zakres danych osobowych obejmuje dane osobowe niezbędne do realizacji przedmiotu umowy, w szczególności mogących dotyczyć pracowników stron umowy, oraz innych osób fizycznych, których dane osobowe są konieczne do realizacji przedmiotu Umowy. Dane osobowe mogą obejmować: imię i nazwisko, służbowy adres email, nr telefonu służbowego, stanowisko pracy, informacje o posiadanych uprawnieniach i szkoleniach.

2) Obydwie strony będą przestrzegać obowiązujących przepisów o ochronie danych osobowych dotyczących danych osobowych przetwarzanych w związku z działalnością na mocy niniejszej Umowy. Strony podejmą wszelkie uzasadnione z handlowego punktu widzenia i prawne kroki w celu ochrony danych osobowych przed niepożądanym ujawnieniem.

3) Jeśli obydwie strony przekazują dane osobowe, zapewnią, że są do tego uprawnione. Strona przekazująca dane osobowe zawiadomi osoby, których dane osobowe dostarczył, o takim przekazaniu przed ich dostarczeniem odbiorcy.

4) Obydwie strony mogą udostępniać dane osobowe swoim dostawcom usług, ale wyłącznie zgodnie z obowiązującymi przepisami o ochronie danych osobowych oraz z odpowiednimi wdrożonymi zabezpieczeniami.

5) W zakresie, w jakim obydwie strony przetwarzają dane osobowe w ramach niniejszej umowy, są uprawnione do przechowywania danych osobowych na czas obowiązywania niniejszej umowy oraz w okresie późniejszym, zgodnie z wymaganiami umowy, w celu ochrony praw obu stron lub spełnienia wymogów prawa i sprawozdawczości. W zakresie, w jakim strona przetwarza dane osobowe do celów odrębnych i niezależnych od niniejszej Umowy, występuje w charakterze administratora danych i przejmuje obowiązki prawne administratora danych, w tym w zakresie określenia odpowiedniego okresu przechowywania danych.

6) Jeśli dane osobowe są związane z incydentem naruszenia ochrony danych (wszelkimi okolicznościami obejmującymi rzeczywistą lub uzasadnioną możliwość uzyskania dostępu do danych osobowych przez osoby nieupoważnione, wejścia przez nie w posiadanie takich danych, ich utratę lub zniszczenie), strona, w której systemie dane były przechowywane, ponosi odpowiedzialność za wszelkie powiadomienia i związane z tym koszty. O ile nie jest to sprzeczne z przepisami prawa lub zakazane przez właściwy dla jednej ze stron organ regulacyjny, strona powiadamiająca dołoży racjonalnie uzasadnionych starań w celu dokonania uzgodnień z drugą stroną, by umożliwić jej wpływ na treść powiadomienia przed jego sporządzeniem.

7) Jeśli podczas wykonywania zobowiązań wynikających z niniejszej umowy jedna ze stron uzyska informacje o: (i) skardze lub zarzucie wskazujących na naruszenie obowiązujących przepisów o ochronie danych osobowych; (ii) wniosku co najmniej jednej osoby ubiegającej się o dostęp do danych osobowych, wprowadzenie do nich poprawek lub ich usunięcie lub (iii) zapytaniu lub skardze co najmniej jednej osoby w związku z przetwarzaniem danych osobowych, wówczas ta strona podejmie wszelkie uzasadnione starania w celu niezwłocznego powiadomienia drugiej ze stron o wyżej wskazanych okolicznościach, z wyjątkiem przypadków, w których jest to niedopuszczalne na mocy prawa, zakazane przez organy ścigania lub przez właściwy organ regulacyjny. Strony zapewnią sobie wzajemne, uzasadnione z handlowego punktu widzenia wsparcie w zakresie weryfikacji powyższych informacji, określania istotnych informacji, przygotowywania odpowiedzi, wdrażania działań naprawczych i/lub współpracy w prowadzeniu wszelkich roszczeń oraz postępowań sądowych lub regulacyjnych i obrony przed takimi roszczeniami oraz postępowaniami.

8) W sprawach nieuregulowanych w niniejszym punkcie, mają zastosowanie odpowiednie przepisy 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

**§ 15**

**Postanowienia końcowe**

1) Zamawiający i Wykonawca podejmą starania w celu polubownego rozstrzygnięcia wszelkich sporów powstałych między nimi, a wynikających z umowy lub pozostających w pośrednim bądź bezpośrednim związku z umową, na drodze bezpośrednich negocjacji.

2) Jeśli Zamawiający i Wykonawca nie są w stanie polubownie rozstrzygnąć sporu, każda ze Stron może poddać spór rozstrzygnięciu sądu powszechnego właściwego dla siedziby Zamawiającego.

3) W sprawach nie uregulowanych niniejszą umową stosuje się przepisy kodeksu cywilnego oraz ustawy Prawo Zamówień Publicznych.

4) Umowę sporządzono w 2 jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Załącznikami do umowy stanowiącymi jej integralną część są:

1) Specyfikacja Istotnych Warunków Zamówienia – Załącznik nr 1 - Opis przedmiotu zamówienia

2) Oferta Wykonawcy.

3) Formularz cenowo przedmiotowy

4) Wzór protokołu odbioru

 Zamawiający : Wykonawca:

……………………………………………. ……………………………………………….

Załącznik nr 4

**PROTOKÓŁ ODBIORU - WZÓR**

Dostawa infrastruktury serwerowej do Muzeum Narodowego w Szczecinie na podstawie Umowy nr…………………. z dnia………………………..

Sporządzony przy udziale:

Osoby reprezentujące Zamawiającego: Osoby reprezentujące Wykonawcę:

…………………………………………………………. ……………………………………………………………

…………………………………………………………. ……………………………………………………………

|  |  |  |
| --- | --- | --- |
| **l. p.**  | **Model, nr seryjny sprzętu**  | **Gwarancja** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Pozostałe uwagi:

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Szczecin, dnia……………………………………………..

 Zamawiający: Wykonawca:

 ………………………………………… …………………………………………

 (imię i nazwisko przedstawiciela (imię i nazwisko przedstawiciela

 zamawiającego, pieczęć firmowa) Wykonawcy, pieczęć firmowa)FF

**Załącznik 10 do formularza ofertowego - Oświadczenie dotyczące posiadania autoryzacji producenta dostarczonych przełączników sieciowych**

|  |
| --- |
|  (wykonawca) |

**DEKLARACJA WYKONAWCY O POSIADANIU AUTORYZACJI PRODUCENTA DOSTARCZONYCH PRZEŁĄCZNIKÓW SIECIOWYCH**

W odpowiedzi na ogłoszenie o przetargu nieograniczonym na: Dostawę infrastruktury serwerowej do Muzeum Narodowego w Szczecinie , deklaruje:

Ja niżej podpisany działając w imieniu i na rzecz: ............................................................................................................................................................................................................................................................................................................................................................................... (nazwa i adres Wykonawcy NIP/PESEL, KRS/CEiDG)

**Deklaruje że**, posiadam autoryzację producenta dostarczonych przełączników sieciowych.

**Uwaga: Deklaracja jest kryterium oceny ofert. Wykonawca który złoży ofertę wraz z deklaracją otrzyma 30 pkt. W przypadku nie złożenia deklaracji Wykonawca otrzyma 0 pkt.**

miejscowość i data podpis osoby/osób uprawnionej do

………………………. reprezentowania Wykonawcy

 ……………………………………..