Gmina Miasta Toruń z siedzibą w Toruniu, ul. Wały gen. Sikorskiego 8, posiadająca NIP 879-000-10-14, działająca poprzez Toruńskie Centrum Usług Wspólnych, ul. Rydygiera 12a, 87-100 Toruń, zaprasza w formie Zapytania Ofertowego do złożenia oferty w postępowaniu o udzielenie zamówienia o wartości nieprzekraczającej równowartości 30 000 euro. Postępowanie prowadzone jest na podstawie Regulaminu udzielania zamówień o wartości nieprzekraczającej progu stosowania przepisów ustawy „Prawo zamówień publicznych", wprowadzonego przez Dyrektora Toruńskiego Centrum Usług Wspólnych Zarządzeniem nr 3/2017 z dnia 01.03.2017r. na podstawie § 11 Regulaminu Organizacyjnego Toruńskiego Centrum Usług Wspólnych.

**I. Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa usługi informatycznej w modelu PaaS (Platform as a Service) na potrzeby funkcjonowania serwisu www wraz z usługami poczty email i ochroną antywirusową i antyspamową urządzeń końcowych Toruńskiego Centrum Usług Wspólnych.

Wykonawca będzie oferował usługi w oparciu o infrastrukturę technologiczną ośrodka centrum przetwarzania danych zlokalizowanego na terytorium Polski zgodnie z określonymi przez zamawiającego wymaganiami. Ponadto musi zapewnić łącza do sieci Internet, infrastrukturę teletechniczną wraz z niezbędnymi urządzeniami, oprogramowaniem i licencjami potrzebnymi do prawidłowego uruchomienia i działania usługi zgodnie z określonymi parametrami.

Wykonawca musi zapewnić obsługę udostępnionego sprzętu i oprogramowania wraz ze wsparciem administratorów, ochronę przed atakami i instalacją złośliwego oprogramowania.

**II. Termin rozpoczęcia świadczenia usługi**

Od dnia 01.01.2018 przez okres 12 miesięcy.

**III. Miejsce i termin składania ofert**: Wykonawca może złożyć tylko jedną ofertę w jednej z podanych form: w sekretariacie TCUW, ul. Rydygiera 12a, na adres e-mail sekretariat@tcuw.torun.pl lub przesłać na adres Toruńskie Centrum Usług Wspólnych, ul. Rydygiera 12a, 87-100 Toruń. Oferty prosimy składać w terminie **do 18 grudnia 2017r. do godz. 12:00**

**IV. Ofertę stanowi** wypełniony i podpisany Formularz Ofertowy (załącznik nr 1 do Zapytania Ofertowego)

**V. Sposób obliczania ceny**

1. Wykonawca poda cenę brutto oferty w Formularzu Ofertowym, sporządzonym według wzoru stanowiącego Załącznik Nr 1.
2. Wykonawca poda cenę netto za całość usługi w okresie od 01.01.2018 do 31.12.2018.
3. Ceny muszą być wyrażone w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca musi uwzględnić w cenie oferty wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania zamówienia oraz wszelkie opłaty i podatki wynikające z obowiązujących przepisów.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

Mazol

6. Rozliczenia między zamawiającym a wykonawcą będą prowadzone w PLN.

## VI. Badanie ofert

1. W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert.
2. Zamawiający w celu ustalenia, czy oferta zawiera rażąco niską cenę lub części składowe ceny wydają się rażąco niskie w stosunku do przedmiotu zamówienia, zwróci się do wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny.
3. Zamawiający poprawi w ofercie:
   a) oczywiste omyłki pisarskie,
   b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   c) inne omyłki polegające na niezgodności oferty z SIWZ, niepowodujące istotnych zmian w treści oferty,

   niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
4. Zamawiający zastrzega sobie, że może najpierw dokonać oceny ofert, a następnie zbadać, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

## VII. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty i sposobu oceny.

1. Zamawiający dokona oceny ofert, które nie zostały odrzucone, na podstawie następujących kryteriów oceny ofert:

| Lp. | Nazwa kryterium | Waga kryterium (w %) |
|---|---|---|
| 1 | Cena netto za całość usługi | 50 |
| 2 | Ośrodek przetwarzania danych | 40 |
| 3 | Dostępność usługi - SLA | 5 |
| 4 | Przepustowość łącza do sieci Internet | 5 |

2. Zamawiający dokona oceny ofert, przyznając punkty w ramach kryterium „Cena netto za całość usługi" przyjmując zasadę, że 1% = 1 punkt.
3. Punkty za kryterium **„Cena netto za całość usługi"** zostaną obliczone według wzoru:

$$\frac{\text{oferty najtańszej}}{\text{oferty badanej}} \times 50 = LP$$

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.

Mazol

4. Punkty za kryterium „**Ośrodek przetwarzania danych**" zostaną przyznane w skali punktowej od 0 do 40 pkt, wg poniższej zasady:
   a. Posiadany aktualny certyfikat ISO 27001 na usługi cloud computing: 10 pkt
   b. Posiadany aktualny certyfikat ISO 22301 na usługi cloud computing: 10 pkt
   c. Posiadany certyfikat TIER III dokumentacji centrum przetwarzania danych: 10 pkt
   d. Posiadany crtyfikat TIER III infrastruktury centrum przetwarzania danych: 10 pkt

5. Punkty za kryterium „**Dostępność usługi – SLA**" zostaną przyznane w skali punktowej do 5 pkt. wg poniższej zasady ramach:
   a. do 99,98% SLA w skali roku – 0 pkt
   b. od 99,99% SLA w skali roku – 5 pkt

6. Punkty za kryterium „**Przepustowość łącza do sieci Internet**" zostaną przyznane w skali punktowej do 5 pkt wg poniższej zasady:
   a. przepustowość łącza symetrycznego bez limitu transferu poniżej 100 Mbps – 0 pkt
   b. przepustowość łącza symetrycznego bez limitu transferu powyżej 100 Mbps – 5 pkt

7. Liczby punktów, o których mowa w pkt 3 do 6 po zsumowaniu stanowić będą końcową ocenę oferty.

8. Za najkorzystniejszą zostanie uznana oferta z największą liczbą punktów, tj. przedstawiająca najkorzystniejszy bilans kryteriów oceny ofert.

9. Zamawiający nie dopuszcza składania ofert wariantowych.

## VIII. Wymagania dla ośrodka przetwarzania danych w ramach którego oferowane będą usługi.

| OBIEKT I LOKALIZACJA | | |
|---|---|---|
| L.p. | Parametr lub kryterium | Wyeliminowanie zagrożenia |
| 1 | Ogrodzony teren | Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka |
| 2 | Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie | Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury |
| 3 | Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej | Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych. |
| 4 | Minimum 500 m od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, łatwopalne również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych | Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko) |
| 5 | Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i | Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego |

Mazol

| | | |
|---|---|---|
| | obiekty sportowe, miejsc organizacji imprez masowych na minimum 10 tys. osób). | zachowania tłumów, ryzyko zamieszek, zniszczeń. |
| 6 | Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni | Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw. |
| 7 | Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi w ośrodku | Zagrożenie zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności). |
| 8 | Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Klientowi (Zamawiającemu) od źródeł pól zakłócających (transformatory SN i WN). | Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pól zakłócających pracę urządzeń elektrycznych i magnetycznych. |
| 9 | Wysokość technologiczna wewnątrz pomieszczenia serwerowni: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu | Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. |
| 10 | Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m | Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych. |
| 11 | Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1. | Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych. |
| 12 | Ośrodek spełnia wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej. | Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej. |
| 13 | Ośrodek zlokalizowany na terenie Polski. Wszystkie dane będą gromadzone i przechowywane na terenie Polski. | Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium Polski. |
| | WĘZŁY TELEKOMUNIKACYJNE | |
| 1 | Ośrodek podłączony w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym | Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora. |
| 2 | Dojścia połączeń do ośrodka wykonane dwoma niezależnymi | Zagrożenie utraty ciągłości komunikacji danych z |

Nazol

| | | |
|---|---|---|
| | trasami kablowymi. | ośrodkiem. |
| 3 | Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP Przepustowość udostępniona Zamawiającemu minimum 24Mbps | Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet. |
| 4 | Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,98% | Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet. |
| 5 | Węzeł telekomunikacyjny wyposażony w redundantny system firewall | Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej. |
| 6 | Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci. | Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy. |
| | ZASILANIE | |
| 1 | Dostępność roczna systemu zasilania 99,9% | Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń. |
| 2 | Minimum dwie zewnętrzne linie zasilania | Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania. |
| 3 | System zasilania awaryjnego UPS osobno na każdą linię zasilającą | Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego. |
| 4 | Agregat prądotwórczy | Zagrożenie braku zachowania zasilania |
| 5 | System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Klienta (Zamawiającego) przez przynajmniej15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną | Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów. |
| 6 | Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy. | Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów. |
| | BEZPIECZEŃSTWO | |
| 1 | Ośrodek wyposażony w: system telewizji przemysłowej (CCTV),okres archiwizacji min. 7 dni, system kontroli dostępu (SKD). | Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń. |

Maxol

| | | |
|---|---|---|
| 2 | Ośrodek wyposażony w: System sygnalizacji włamania i napadu, System wykrywania wody i zalania. | Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu. |
| 3 | Ośrodek chroniony przez zewnętrzną licencjonowaną firmę. | Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej. |
| 4 | System CCTV zapewnia ciągły365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne. | Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób. |
| 5 | System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 7 dni. | Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń. |
| 6 | System SKD dzieli ośrodek wraz z terenem na 4 strefy dostępu dla ośrodka z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku. |
| 7 | Dostęp do strefy I uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów). | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 8 | Dostęp do strefy II (obiekt uwarunkowany identyfikacją na podstawie dokumentu tożsamości. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 9 | Dostęp do strefy III (Data center) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 10 | Dostęp do strefy IV (Pomieszczenia ze sprzętem komputerowym Klienta (Zamawiającego)) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 11 | System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego. | Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia. |
| 12 | Ściany, stropy Data center o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do | Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia |

Mazd

| | | |
|---|---|---|
| | pomieszczeń data center o odporności ogniowej 60 minutowej. | rozprzestrzeniania się pożaru. |
| MONITOROWANIE | | |
| 1 | System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7 | Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej. |
| 2 | Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Klientowi (Zamawiającemu). Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności. | Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń. |
| 3 | Gromadzenie logów zdarzeń z pracy urządzeń komputerowych udostępnionych Klientowi (Zamawiającemu) | Zagrożenie braku kontroli nad użytkowanymi urządzeniami komputerowymi i historii dowodowej pracy urządzeń. |

**IX. Minimalne wymagania sprzętowo-programowe wraz z usługami**

W ramach realizacji usługi Wykonawca musi udostępnić maszyny wirtualne oraz oprogramowanie systemowe i narzędziowe o parametrach nie gorszych niż obecnie wykorzystywane przez Zamawiającego określone w tabeli poniżej.

**1. Specyfikacja serwera bazy danych – 1 szt.**

| Lp. | Zakres | Minimalne wymagania |
|---|---|---|
| 1 | Architektura | x86-64 |
| 2 | Pamięć podstawowa | 8 GB DDR3 1333MHz |
| 3 | Procesor/Procesory | 4 vCPU 2,40GHz min. 600 punktów w teście PECint_rate_2006 |
| 4 | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| 5 | Interfejsy sieciowe | 2 x 1Gb |
| 6 | Moduł zarządzania | Wymagany |
| 7 | System operacyjny | Windows server 2016 z możliwością upgrade do nowszej wersji lub równoważny |
| 8 | Silnik bazy danych | MS SQL Express Server 2014 z |
| 9 | Przestrzeń dyskowa | 150 GB wydajność 30.000 IOPS |

**2. Specyfikacja serwera portalu - 1 szt.**

| Lp. | Zakres | Minimalne wymagania |
|---|---|---|
| 1 | Architektura | x86-64 |

Mazol

| | | |
|---|---|---|
| 2 | Pamięć podstawowa | 1 GB DDR3 1333MHz |
| 3 | Procesor/Procesory | 1 vCPU 2,40GHz min. 600 punktów w teście PECint_rate_2006 |
| 4 | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% |
| 5 | Interfejsy sieciowe | 2 x 1Gb |
| 6 | Moduł zarządzania | Wymagany |
| 7 | System operacyjny | Windows server 2016 z możliwością upgrade do nowszej wersji lub równoważny |
| 8 | Przestrzeń dyskowa | 50 GB wydajność 5.000 IOPS |

**3. Specyfikacja usługi poczty email Exchange – 87 użytkowników**

| Lp. | Minimalne wymagania |
|---|---|
| 1 | Powierzchnia dysku pojedynczego użytkownika 10 GB |
| 2 | Maksymalny rozmiar załącznika w jednej wiadomości email 40 MB |
| 3 | Środowisko MS Exchange 2016 |
| 4 | Dostęp do OWA (Outlook Web Aplication) |
| 5 | ActiveSync dla smartfonów i tabletów |
| 6 | Dostęp przez IMAP |
| 7 | Integracja z firmowym Active Directory |
| 8 | Podstawowa ochrona antyspamowa i antywirusowa |

**4. Specyfikacja usługi poczty email Exchange – 13 użytkowników**

| Lp. | Minimalne wymagania |
|---|---|
| 1 | Powierzchnia dysku pojedynczego użytkownika 15 GB |
| 2 | Maksymalny rozmiar załącznika w jednej wiadomości email 40 MB |
| 3 | Środowisko MS Exchange 2016 |
| 4 | Dostęp do OWA (Outlook Web Aplication) |
| 5 | ActiveSync dla smartfonów i tabletów |
| 6 | Dostęp przez IMAP |
| 7 | Integracja z firmowym Active Directory |
| 8 | Podstawowa ochrona antyspamowa i antywirusowa |
| 9 | Własna domena firmowa |
| 10 | MS Outlook 2016 |
| 11 | Prywatny i współdzielony kalendarz |

**5. Specyfikacji ochrona stacji roboczych z zabezpieczeniem skrzynek pocztowych Exchange – 90 szt.**

Mozol

| Lp. | Minimalne wymagania |
|---|---|
| 1 | Systemy Operacyjne Komputerów<br>• Windows 10 Anniversary Update "Redstone"<br>• Windows 10 TH2<br>• Windows 10<br>• Windows 8.1<br>• Windows 8<br>• Windows 7<br>• Windows Vista z dodatkiem Service Pack 1<br>• Windows XP z Service Pack 2 64 bit<br>• Windows XP z Service Pack 3<br>Tablety i Wbudowane Systemy Operacyjne<br>• Windows Embedded 8.1 Industry<br>• Windows Embedded 8 Standard<br>• Windows Embedded Standard 7<br>• Windows Embedded Compact 7<br>• Windows Embedded POSReady 7<br>• Windows Embedded Enterprise 7<br>• Windows Embedded POSReady 2009<br>• Windows Embedded Standard 2009<br>• Windows XP z wbudowanym Service Pack 2<br>• Windows XP Tablet PC Edition |
| 2 | Systemy Operacyjne Mac OS X<br>• Mac OS X Sierra (10.12.x)<br>• Mac OS X El Capitan (10.11.x)<br>• Mac OS X Yosemite (10.10.5)<br>• Mac OS X Mavericks (10.9.5)<br>• Mac OS X Mountain Lion (10.8.5) |
| 3 | Wymagania Ochrony Mobile<br>• Apple iPhone i tablety iPad (iOS 5.1+)<br>• Smartfony i tablety z Google Android (2.3+) |
| 4 | Obsługiwane Środowiska Microsoft Exchange<br>• Exchange Server 2016 z rolą Edge Transport lub Mailbox<br>• Exchange Server 2013 z rolą Edge Transport lub Mailbox<br>• Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox<br>• Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox |
| 5 | Wymagania funkcjonalno-użytkowe:<br>1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.<br>2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.<br>3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.<br>4. Wbudowana technologia do ochrony przed rootkitami.<br>5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.<br>6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików |

Mazol

| | |
|---|---|
| | "na żądanie".<br>7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.<br>8. Możliwość skanowania dysków sieciowych i dysków przenośnych.<br>9. Skanowanie plików spakowanych i skompresowanych.<br>10. Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.<br>11. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.<br>12. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).<br>13. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.<br>14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.<br>15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.<br>16. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.<br>17. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.<br>18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.<br>19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.<br>20. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.<br>21. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.<br>22. Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze.<br>23. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.<br>24. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.<br>25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.<br>26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.<br>27. Praca programu musi być niezauważalna dla użytkownika.<br>28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.<br>29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.<br>30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.<br>31. Możliwość odblokowania ustawień programu po wpisaniu hasła<br>32. Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika<br>33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)<br>34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy |

Mazol

| | |
|---|---|
| | danych urządzeń podłączanych przez użytkowników do komputerów.<br>35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.<br>36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.<br>37. Jedna wersja instalacyjna na stacje robocze i serwery plików.<br>38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.<br>39. Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa.<br>40. Możliwość tworzenia list sieci zaufanych.<br>41. Możliwość dezaktywacji funkcji zapory sieciowej.<br>42. Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików.<br>43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.<br>44. Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware |
| 6 | Urządzenia Mobilne<br>1. Dla systemu Android możliwość blokowania stron internetowych.<br>2. Możliwość szyfrowania urządzenia opartego o system android.<br>3. Możliwość pobrania wersji instalacyjnej ze sklepu iOS oraz Android<br>4. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android<br>5. Posiadać możliwość szyfrowania urządzenia dla systemu Android<br>6. Ochrona stron internetowych dla androida pod kontem malware, exploit, phishing<br>7. Możliwość blokowania ekranu głównego hasłem.<br>8. Możliwość definiowania i zabezpieczania połączeń WiFi<br>9. Dla systemu Android moduł odpowiedzialny za blokowanie stron.<br>10. Kontrola przeglądarki Safari dla urządzeń z systemem iOS |

**X. O wyborze najkorzystniejszej oferty** Zamawiający powiadomi niezwłocznie Oferentów oraz zamieści informację o wyborze na swojej stronie internetowej (www.tcuw.torun.pl zakładka BIP, „Zamówienia publiczne").

**XI. Osoba wyznaczona do kontaktowania się z Oferentami:**

*Karolina Ostrowska, tel. 56 611-89-91, sekretariat@tcuw.torun.pl*

**XII.** Zamawiający zastrzega sobie prawo do rezygnacji z realizacji zadania bez wyboru którejkolwiek ze złożonych ofert bez podania przyczyny.

Zatwierdzam

Dyrektor

*Paweł Modrzyński*

Załączniki do Zapytania ofertowego:

1. formularz ofertowy

**Załącznik nr 1. Formularz ofertowy**

**1. Informacje o Wykonawcy**

| | |
|---|---|
| **Nazwa Wykonawcy** | |
| **Adres siedziby** | |
| **NIP** | |
| **Osoba do kontaktu** | |
| **Nr telefonu** | |
| **Adres e-mail** | |

**2. Informacje o ofercie**

| | |
|---|---|
| **Opis przedmiotu zamówienia/zakres oferty** | |
| **Kod CPV** | |
| **Cena netto całości zamówienia w PLN** | |
| **Cena brutto całości zamówienia w PLN** | |

**3. Informacja o spełnieniu warunków udziału w postępowaniu - wymagania dla ośrodka w ramach którego oferowane będą usługi.**

| OBIEKT I LOKALIZACJA | | | |
|---|---|---|---|
| L.p. | Parametr lub kryterium | Wyeliminowanie zagrożenia | Wykonawca spełnia (TAK / NIE) |
| 1 | Ogrodzony teren | Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka | |
| 2 | Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie | Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury | |
| 3 | Teren powinien być położony co najmniej 5 metrów powyżej | Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność | |

| | | | |
|---|---|---|---|
| | poziomu wody stuletniej | oddziaływania sytuacji krytycznych. | |
| 4 | Minimum 500 m od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, łatwopalne również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych | Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko) | |
| 5 | Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, miejsc organizacji imprez masowych na minimum 10 tys. osób). | Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń. | |
| 6 | Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni | Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw. | |
| 7 | Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi w ośrodku | Zagrożenie zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności). | |
| 8 | Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Klientowi (Zamawiającemu) od źródeł pól zakłócających (transformatory SN i WN). | Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych. | |
| 9 | Wysokość technologiczna wewnątrz pomieszczenia serwerowni: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu | Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. | |
| 10 | Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m | Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych. | |
| 11 | Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1. | Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych. | |

| | | | |
|---|---|---|---|
| 12 | Ośrodek spełnia wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej. | Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej. | |
| 13 | Ośrodek zlokalizowany na terenie Polski. Wszystkie dane będą gromadzone i przechowywane na terenie Polski. | Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium Polski. | |
| | WĘZŁY TELEKOMUNIKACYJNE | | |
| 1 | Ośrodek podłączony w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym | Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora. | |
| 2 | Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi. | Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem. | |
| 3 | Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP Przepustowość udostępniona Zamawiającemu minimum 24Mbps | Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet. | |
| 4 | Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,98% | Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet. | |
| 5 | Węzeł telekomunikacyjny wyposażony w redundantny system firewall | Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej. | |
| 6 | Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci. | Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy. | |
| | ZASILANIE | | |
| 1 | Dostępność roczna systemu zasilania 99,9% | Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń. | |
| 2 | Minimum dwie zewnętrzne linie zasilania | Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego | |

| | | | |
|---|---|---|---|
| | | przywracania ciągłości zasilania. | |
| 3 | System zasilania awaryjnego UPS osobno na każdą linię zasilającą | Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego. | |
| 4 | Agregat prądotwórczy | Zagrożenie braku zachowania zasilania | |
| 5 | System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Klienta (Zamawiającego) przez przynajmniej15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną | Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów. | |
| 6 | Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy. | Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów. | |
| | | BEZPIECZEŃSTWO | |
| 1 | Ośrodek wyposażony w: system telewizji przemysłowej (CCTV),okres archiwizacji min. 7 dni, system kontroli dostępu (SKD). | Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń. | |
| 2 | Ośrodek wyposażony w: System sygnalizacji włamania i napadu, System wykrywania wody i zalania. | Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu. | |
| 3 | Ośrodek chroniony przez zewnętrzną licencjonowaną firmę. | Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej. | |
| 4 | System CCTV zapewnia ciągły365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne. | Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób. | |
| 5 | System CCTV powinien | Element zapewniający możliwość | |

| | | | |
|---|---|---|---|
| | zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 7 dni. | określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń. | |
| 6 | System SKD dzieli ośrodek wraz z terenem na 4 strefy dostępu dla ośrodka z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku. | |
| 7 | Dostęp do strefy I uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów). | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. | |
| 8 | Dostęp do strefy II (obiekt uwarunkowany identyfikacją na podstawie dokumentu tożsamości. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. | |
| 9 | Dostęp do strefy III (Data center) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. | |
| 10 | Dostęp do strefy IV (Pomieszczenia ze sprzętem komputerowym Klienta (Zamawiającego)) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. | |
| 11 | System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego. | Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia. | |
| 12 | Ściany, stropy Data center o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń data center o odporności ogniowej 60 minutowej. | Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru. | |
| | MONITOROWANIE | | |
| 1 | System przyjmowania zgłoszeń dotyczących awarii | Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne | |

| | | | |
|---|---|---|---|
| | działający w trybie 365/24/7 | przypadające poza godzinami pracy biurowej. | |
| 2 | Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Klientowi (Zamawiającemu). Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności. | Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń. | |
| 3 | Gromadzenie logów zdarzeń z pracy urządzeń komputerowych udostępnionych Klientowi (Zamawiającemu) | Zagrożenie braku kontroli nad użytkowanymi urządzeniami komputerowymi i historii dowodowej pracy urządzeń. | |

**4. Minimalne wymagania sprzętowo-programowe wraz z usługami**

Specyfikacja serwera bazy danych – 1 szt.

| Lp. | Zakres | Minimalne wymagania | Oferowane rozwiązanie |
|---|---|---|---|
| 1 | Architektura | x86-64 | |
| 2 | Pamięć podstawowa | 8 GB DDR3 1333MHz | |
| 3 | Procesor/Procesory | 4 vCPU 2,40GHz min. 600 punktów w teście PECint_rate_2006 | |
| 4 | Skalowalność | Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50% | |
| 5 | Interfejsy sieciowe | 2 x 1Gb | |
| 6 | Moduł zarządzania | Wymagany | |
| 7 | System operacyjny | Windows server 2016 z możliwością upgrade do nowszej wersji lub równoważny | |
| 8 | Silnik bazy danych | MS SQL Express Server 2014 z | |
| 9 | Przestrzeń dyskowa | 150 GB wydajność 30.000 IOPS | |

Specyfikacja serwera portalu - 1 szt.

| Lp. | Zakres | Minimalne wymagania | Oferowane rozwiązanie |
|---|---|---|---|
| 1 | Architektura | x86-64 | |
| 2 | Pamięć podstawowa | 1 GB DDR3 1333MHz | |
| 3 | Procesor/Procesory | 1 vCPU 2,40GHz min. 600 punktów w teście PECint_rate_2006 | |
| 4 | Skalowalność | Możliwość zwiększenia pamięci | |

| | | | |
|---|---|---|---|
| | | operacyjnej i wydajności obliczeniowej procesorów min. o 50% | |
| 5 | Interfejsy sieciowe | 2 x 1Gb | |
| 6 | Moduł zarządzania | Wymagany | |
| 7 | System operacyjny | Windows server 2016 z możliwością upgrade do nowszej wersji lub równoważny | |
| 8 | Przestrzeń dyskowa | 50 GB wydajność 5.000 IOPS | |

**5. Posiadane certyfikaty:**

a. _____

b. _____

c. _____

d. _____

**6. Dostępność usługi – SLA w skali roku wyrażona w %**

_____

**7. Przepustowość łącza symetrycznego bez limitów do sieci Internet Mbps**

_____