Zamówienie publiczne 18/2019

Usługi informatyczne w zakresie hostingu. Szczegółowy opis przedmiotu zamówienia

Gmina Miasta Toruń z siedzibą w Toruniu, ul. Wały gen. Sikorskiego 8, posiadająca NIP 879-000-10-14, działająca poprzez Toruńskie Centrum Usług Wspólnych (TCUW), pl. św. Katarzyny 9, 87-100 Toruń, zaprasza w formie Zapytania Ofertowego do złożenia oferty w postępowaniu o udzielenie zamówienia o wartości nieprzekraczającej równowartości 30 000 euro.

KOD CPV:

48800000-6 - Systemy i serwery operacyjne

72415000-2 - Usługi hostingowe dla stron WWW

I. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa usługi informatycznej w modelu IaaS (Infrastructure as a Service) na potrzeby funkcjonowania serwisów www wraz z usługą administrowania serwerami, usługą migracji i usługą poczty email obejmującą ochronę antyspamową i antywirusową urządzeń końcowych dla Toruńskiego Centrum Usług Wspólnych.

Wykonawca będzie oferował usługi w oparciu o infrastrukturę technologiczną ośrodka centrum przetwarzania danych zlokalizowanego na terytorium Unii Europejskiej lub Liechtensteinu, Islandii, Norwegii, zgodnie z określonymi przez Zamawiającego w punktach od **VII** do **XI** poniżej wymaganiami. Ponadto Wykonawca 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 w punktach od **VII** do **XI poniżej**.

Wykonawca musi zapewnić obsługę udostępnionej infrastruktury wraz ze wsparciem administratorów IT w trybie 24/7/365 oraz ochronę przed atakami i instalacją złośliwego oprogramowania.

Szczegółowe wymagania zamówienia zawarte zostały w punktach od **VII** do **XI** niniejszego zapytania.

Wszelkie użyte w niniejszym zapytaniu i załącznikach do niego nazwy własne, normy, aprobaty, specyfikacje techniczne, systemy referencji technicznych, wymagane certyfikaty itp., w tym nazwy handlowe, oznaczenia lub znaki towarowe, patenty, określenia pochodzenia, źródła lub szczególnego procesu charakteryzujące produkt lub usługę dostarczane przez konkretnego wykonawcę, a które mogły pojawić się w zapytaniu i załącznikach do niego, należy rozumieć każdorazowo jak opatrzone dopiskiem „lub równoważne".

II. Termin rozpoczęcia świadczenia usługi

Od dnia zawarcia umowy, nie wcześniej niż od 01.01.2020 r. do dnia 31.12.2021 r.

III. Miejsce i termin składania ofert

Wykonawca może złożyć tylko jedną ofertę w jednej z podanych form: w sekretariacie TCUW, pl. Św. Katarzyny 9, 87-100 Toruń, na adres e-mail sekretariat@tcuw.torun.pl lub przesłać na adres Toruńskie Centrum Usług Wspólnych, pl. św. Katarzyny 9, 87-100 Toruń. Oferty prosimy składać w terminie **do 27.12.2019 r. do godz. 12:00.**

IV. Sposób obliczania ceny

1. Wykonawca poda cenę netto i brutto oferty w Formularzu Ofertowym, sporządzonym według wzoru stanowiącego Załącznik nr 1.
2. Cena ofertowa podana przez wykonawcę w Formularzu Oferty zostanie ustalona jako cena łączna na okres ważności umowy i nie będzie podlegała zmianom.
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. Cena musi zawierać wszystkie koszty przygotowania i złożenia oferty, a także koszty ewentualnego zaplanowania i przeprowadzenia bezprzerwowej migracji wszystkich zasobów Zamawiającego z obecnie wykorzystywanej infrastruktury IT do nowej infrastruktury IT dostarczanej przez Wykonawcę oraz świadczenie usługi przez okres wskazany w przedmiocie zamówienia.
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.
6. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w PLN.
7. Płatność za usługi realizowana będzie w transzach rocznych z terminem płatności:
    a. 50% ceny usługi w terminie do 31.12.2020 r.
    b. 50% ceny usługi w terminie do 31.12.2021 r.

V. Badanie ofert

1. Niespełnienie lub niewykazanie spełnienia któregokolwiek warunku lub braku podstaw do wykluczenia będzie przyczyną wykluczenia Wykonawcy i uznania jego oferty za odrzuconą.
2. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień, dotyczących treści złożonych ofert. Zamawiający zastrzega możliwość weryfikacji i wizytacji wskazanego w ofercie ośrodka centrum przetwarzania danych, w tym złożenia dowodów dotyczących spełnienia wskazanych w zapytaniu wymagań.
3. 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. Zamawiający zwraca się o wyjaśnienia w szczególności w przypadku, gdy cena całkowita oferty jest niższa o co najmniej 30% od:
    a) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania lub średniej arytmetycznej cen wszystkich złożonych ofert, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia.
    b) wartości zamówienia powiększonej o należny podatek od towarów i usług, zaktualizowanej z uwzględnieniem okoliczności, które nastąpiły po wszczęciu postępowania, w szczególności istotnej zmiany cen rynkowych.
4. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na Wykonawcy. Zamawiający odrzuca ofertę Wykonawcy, który nie udzielił wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia. 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 niniejszym zapytaniem, niepowodujące istotnych zmian w treści oferty,

niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

5. 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.
6. Zamawiający oceni i porówna jedynie te oferty, które nie zostaną wykluczone i odrzucone.
7. Postępowanie zostanie rozstrzygnięte w przypadku złożenia co najmniej jednej oferty niepodlegającej odrzuceniu.

VI. 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 brutto za całość usługi	50
2	Ośrodek przetwarzania danych	40
3	Dostępność usługi - SLA	5
4	Łącze	5

2. Zamawiający dokona oceny ofert, przyznając punkty w ramach kryterium „Cena brutto za całość usługi" przyjmując zasadę, że 1% = 1 punkt.

   Punkty za kryterium **„Cena brutto za całość usługi"** zostaną obliczone według wzoru:

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

   gdzie

   LP = liczba uzyskanych punktów

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

3. 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 certyfikat TIER III infrastruktury centrum przetwarzania danych: 10 pkt

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

5. Punkty za kryterium „**Przepustowość łącza do sieci Internet**" zostaną przyznane w skali punktowej do 5 pkt wg poniższej zasady:
   a. łącze symetryczne bez limitu transferu danych, wraz z ochroną DDoS o przepustowości poniżej 1 Gbps – 0 pkt
   b. łącze symetryczne bez limitu transferu danych, wraz z ochroną DDoS o przepustowości od 1 Gbps i więcej – 5 pkt.
6. Liczby punktów, o których mowa w pkt 2 do 5 po zsumowaniu stanowić będą końcową ocenę oferty.
7. Za najkorzystniejszą zostanie uznana oferta z największą liczbą punktów, tj. przedstawiająca najkorzystniejszy bilans kryteriów oceny ofert.
8. Zamawiający nie dopuszcza składania ofert wariantowych ani częściowych.

VII. Wymagania dla ośrodka przetwarzania danych, w ramach którego oferowane będą usługi.

1. Wymagania obligatoryjne dla ośrodka.

OBIEKT I LOKALIZACJA		
L.p.	Parametry lub kryterium	Wyeliminowanie zagrożenia
1	Centrum przetwarzania danych zlokalizowane na terenie UE lub Liechtensteinu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Liechtensteinu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.
3	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.
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, 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).
6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.

7	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.
8	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).
9	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych 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.
10	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.
11	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.
12	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.
13	Spełnienie 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.
WĘZŁY TELEKOMUNIKACYJNE		
1	Podłączenie 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.	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 99,99%	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 99,99%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.	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	Redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.
5	System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 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	Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 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	Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.
3	Ochrona przez zewnętrzną licencjonowaną firmę.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.
4	System CCTV zapewnia ciągły 365/7/24 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 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.
6	System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu 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 (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
8	Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
9	Dostęp do strefy III (strefa technologiczna) 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 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 części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych 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		
	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.
	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej 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.

2. Wymagania obligatoryjne. Ośrodek centrum przetwarzania danych posiada zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Bezpieczeństwo sprzętu informatycznego:

	Zakres
1	Izolacja sprzętu krytycznego
2	Ochrona przed uszkodzeniem
3	Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego
4	Ochrona przed dostępem dla osób nieupoważnionych

3. Wymagania obligatoryjne. Naprawa i konserwacja sprzętu:

	Zakres
1	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.
2	Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka.
3	Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy.
4	Ochrona przed dostępem dla osób nieupoważnionych.
5	Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).
6	Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania.
7	Należy prowadzić rejestr incydentów, awarii i usterek.
8	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.

VIII. Wymagania SLA i czas reakcji

a. SLA dla świadczonej usługi musi wynosić minimum 99,95% w skali roku.

b. Obsługa zarządzania środowiskiem teleinformatycznym musi być realizowana w trybie 24/7/365.

c. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w systemie online Wykonawcy, który umożliwia podgląd wszystkich zgłoszeń, czas ich realizacji oraz bieżący status.

d. Czas reakcji na zgłoszenie musi wynosić do 1h od przyjęcia zgłoszenia.

e. Czas realizacji zgłoszenia musi wynosić:

- dla błędów kategorii „krytyczny", czyli dla całkowitego braku dostępności Usługi w całości lub w części obejmującej pocztę e-mail, w czasie nie dłuższym niż 4 godziny od przyjęcia zgłoszenia;

- dla błędów pozostałych kategorii, czyli dla braku możliwości realizacji zakładanych funkcjonalności lub wystąpienia obniżenia jakości warunków pracy - w czasie nie dłuższym niż 12 godzin od przyjęcia zgłoszenia.

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 środowiska serwerowego w modelu IaaS.

Lp.	Zakres	Minimalne wymagania
1	Architektura	x86-64
2	Pamięć podstawowa	20 GB DDR3 1333MHz
3	Procesor/Procesory	11 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	600 GB wydajność 30.000 IOPS
10	Adres IP	4 x IPv4

2. Specyfikacja usługi poczty podstawowej email Exchange z ochroną – 115 użytkowników

Lp.	Minimalne wymagania
1	Powierzchnia dysku pojedynczego użytkownika 5 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

3. Specyfikacja usługi poczty rozszerzonej email Exchange z ochroną – 15 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

4. Specyfikacji ochrona stacji roboczych i urządzeń przenośnych – 130 szt.

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

	9. Skanowanie plików spakowanych i skompresowanych. 10. Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów. 11. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 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). 13. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. 16. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 17. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 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. 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. 22. Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze. 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. 24. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym. 25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 27. Praca programu musi być niezauważalna dla użytkownika. 28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 31. Możliwość odblokowania ustawień programu po wpisaniu hasła 32. Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika 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) 34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów. 35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 37. Jedna wersja instalacyjna na stacje robocze i serwery plików. 38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 39. Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa. 40. Możliwość tworzenia list sieci zaufanych. 41. Możliwość dezaktywacji funkcji zapory sieciowej. 42. Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików. 43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 44. Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware

6	Urządzenia Mobilne 1. Dla systemu Android możliwość blokowania stron internetowych. 2. Możliwość szyfrowania urządzenia opartego o system android. 3. Możliwość pobrania wersji instalacyjnej ze sklepu iOS oraz Android 4. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android 5. Posiadać możliwość szyfrowania urządzenia dla systemu Android 6. Ochrona stron internetowych dla androida pod kontem malware, exploit, phishing 7. Możliwość blokowania ekranu głównego hasłem. 8. Możliwość definiowania i zabezpieczania połączeń WiFi 9. Dla systemu Android moduł odpowiedzialny za blokowanie stron. 10. Kontrola przeglądarki Safari dla urządzeń z systemem iOS

X. Wsparcie administracyjne

Do zadań realizowanych przez Wykonawcę w ramach usług utrzymaniowych należeć będzie bieżąca obsługa administracyjna zasobów informatycznych (instancji serwerowych) obejmująca nadzór nad posiadaną przez Zamawiającego infrastrukturą IT zlokalizowaną w centrum przetwarzania danych, składającą się w szczególności z zasobów IaaS (Infrastructure as a Service), SaaS (Software as a Service), poprzez świadczenie usług informatycznych w zakresie:

1. migracji usług do infrastruktury cloud i ich utrzymania,
2. instalacji i konfiguracji systemów operacyjnych,
3. instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności (HA),
4. aktualizacji oprogramowania ze względu na błędy bezpieczeństwa,
5. utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa,
6. realizacji bieżących czynności administracyjnych,
7. realizacji polityki kopii zapasowych gromadzonych danych,
8. utrzymania infrastruktury sieciowej (urządzenia sieciowe, punkty AP, połączenia VPN),
9. konsultacji wykonawczych z użytkownikami wewnętrznymi i zewnętrznymi,

Zamawiający wymaga zatrudnienia przez Wykonawcę, jak i ewentualnych podwykonawców, na podstawie umowy o pracę osób wykonujących w zakresie realizacji zamówienia czynności polegające na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz.U. z 2018r. poz. 917 z późn. zm.), tj. osób wykonujących następujące czynności:

1. administrowanie serwerami w środowisku wirtualnym,
2. administrowanie systemami operacyjnymi na serwerach.

XI. Migracja

Z uwagi na fakt, że przedmiotem zamówienia jest utrzymanie wszystkich obecnie funkcjonujących w modelu IaaS, SaaS systemów i usług Zamawiającego (serwisy www, aplikacje, system zgłaszania typu helpdesk), Wykonawca zobowiązany jest do ich bezprzerwowego dalszego utrzymania. Zamawiający oczekuje przygotowania i przedstawienia wraz z ofertą harmonogramu migracji zasobów Zamawiającego z obecnie użytkowanej infrastruktury IaaS i usług SaaS do oferowanych. Zamawiający nie dopuszcza w momencie migracji przerwy w dostępie do usług ani utraty jakichkolwiek danych. Migracja usług musi zostać wykonana bezprzerwowo. Wszystkie systemy i usługi muszą zostać uruchomione produkcyjnie najpóźniej od dnia 01.01.2020 r.

Załączniki:

- Załącznik nr 1 – formularz ofertowy

- Załącznik nr 2 – wzór umowy

p.o. DYREKTORA
TORUŃSKIEGO CENTRUM USŁUG WSPÓLNYCH
Łukasz Nowak (5)

Zamówienie publiczne 18/2019

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	
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.

1. Wymagania obligatoryjne dla ośrodka.

OBIEKT I LOKALIZACJA			
L.p.	Parametry lub kryterium	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1	Centrum przetwarzania danych zlokalizowane na terenie UE lub Liechtensteinu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Liechtensteinu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.	
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.	
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub	Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania,	

	zalanie.	agregaty) w wyniku działań działania sił natury.	
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.	
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, 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).	
6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.	
7	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.	
8	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).	
9	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych 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.	
10	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.	
11	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.	
12	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.	
13	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w	

	zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.	
WĘZŁY TELEKOMUNIKACYJNE			
1	Podłączenie 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.	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 99,99%	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 99,99%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.	
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.	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	Redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.	
5	System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 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	Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 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	Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.	
3	Ochrona przez zewnętrzną licencjonowaną firmę.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.	
4	System CCTV zapewnia ciągły 365/7/24 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 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.	
6	System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu 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 (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
8	Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
9	Dostęp do strefy III (strefa technologiczna) 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 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 części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych 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			
	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.	
	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej 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.	

2. Wymagania obligatoryjne. Ośrodek centrum przetwarzania danych posiada zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Bezpieczeństwo sprzętu informatycznego:

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Izolacja sprzętu krytycznego	
2	Ochrona przed uszkodzeniem	
3	Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego	
4	Ochrona przed dostępem dla osób nieupoważnionych	

3. Wymagania obligatoryjne. Naprawa i konserwacja sprzętu:

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.	
2	Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka.	
3	Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy.	

4	Ochrona przed dostępem dla osób nieupoważnionych.	
5	Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).	
6	Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania.	
7	Należy prowadzić rejestr incydentów, awarii i usterek.	
8	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.	

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	20 GB DDR3 1333MHz	
3	Procesor/Procesory	11 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	
9	Przestrzeń dyskowa	600 GB wydajność 30.000 IOPS	
10	Adres IP	4 x IPv4	

5. Posiadane certyfikaty:

1. _____
2. _____
3. _____
4. _____

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

_____

7. Przepustowość łącza do sieci Internet

_____

Zamówienie publiczne 18/2019

Załącznik nr 2 - wzór umowy

Umowa nr ...../.....

zawarta w dniu ..... r. w Toruniu pomiędzy:

Gminą Miasta Toruń z siedzibą w Toruniu, ul. Wały gen. Sikorskiego 8, 87-100 Toruń, NIP: 879-000-10-14, działającą poprzez Toruńskie Centrum Usług Wspólnych z siedzibą w Toruniu pl. Św. Katarzyny 9,

reprezentowaną przez: .....

zwaną dalej **Zamawiającym**,

a

....., NIP: .....,

reprezentowanym/ą przez: .....

zwaną/-ym dalej **Wykonawcą**,

zwane dalej **Stronami.**

§1
Przedmiot Umowy

1. Przedmiotem Umowy jest świadczenie przez Wykonawcę na rzecz Zamawiającego usługi informatycznej w modelu IaaS (Infrastructure as a Service) na potrzeby funkcjonowania serwisów www wraz z usługą administrowania serwerami, usługą migracji i usługą poczty email obejmującą ochronę antyspamową i antywirusową urządzeń końcowych zwanej dalej **Usługą.** Zamawiającego. Szczegółowy zakres usług został zawarty w zapytaniu ofertowym nr 18/2019 i ofercie Wykonawcy z dnia .....,.
2. Wykonawca gwarantuje udostępnienie zasobów informatycznych na poziomie parametrów podstawowych, tj. w postaci Usługi posiadającej parametry wskazane w Załączniku nr 1 „Parametry środowiska" (dalej jako **Parametry podstawowe**).
3. Zasoby informatyczne w postaci Usługi mogą każdorazowo zostać zwiększone przez Zamawiającego w zakresie i terminie zgodnym ze złożonym drogą elektroniczną zamówieniem (dalej jako **Zamówienie**).
4. Wykonawca udostępni Usługę od dnia zawarcia umowy, nie wcześniej niż od dnia 01.01.2020 r.

§2
Komunikacja

1. Wszelkie komunikaty, zamówienia, informacje i dokumenty związane z realizacją zawartej Umowy, jeżeli Umowa nie wymaga dla nich formy pisemnej lub innej szczególnej, Strony będą przekazywały sobie drogą elektroniczną na adresy email:
   a) Wykonawca wyznacza adres email: .....
   b) Zamawiający wyznacza adresy email: sekretariat@tcuw.torun.pl, l.nowak@tcuw.torun.pl,
2. Każda ze Stron zobowiązana jest do poinformowanie drugiej Strony o zmianie danych kontaktowych, pod rygorem uznania komunikatów, zamówień, informacji i dokumentów przekazanych zgodnie z dotychczasowymi danymi za skutecznie doręczone.

§3
Wynagrodzenie

1. W zamian za świadczenie Usługi na zasadach określonych w niniejszej Umowie, Zamawiający zobowiązuje się do zapłaty na rzecz Wykonawcy wynagrodzenia w wysokości ..... zł brutto (słownie: .....) płatnego w 2 ratach w następujący sposób:
   1) 50% wynagrodzenia w terminie do dnia 31.12.2020 r.;
   2) 50% wynagrodzenia w terminie do dnia 31.12.2021 r..
2. Płatność Wynagrodzenia, o którym mowa w ust.1 nastąpi na podstawie faktury VAT wystawianej przez Wykonawcę i doręczonej Zamawiającemu.
3. Abonent wyraża zgodę na otrzymywanie faktur VAT drogą elektroniczną w formacie PDF, na adres email Zamawiającego, wskazany w paragrafie §2, ust. 1, lit. b).
4. Za dzień dokonania zapłaty Strony uznają dzień, w którym zostanie obciążony rachunek bankowy Zamawiającego.

§4
Prawa i obowiązki Stron

1. Zamawiający na podstawie niniejszej Umowy otrzymuje możliwość korzystania z Usługi w okresie ustalonym w Umowie.
2. Zamawiający zobowiązany jest do korzystania z Usługi wyłącznie w sposób zgodny z obowiązującym prawem, postanowieniami Umowy, dobrymi obyczajami oraz charakterem i przeznaczeniem usług chmury obliczeniowej.
3. Zamawiający w szczególności nie może korzystać z Usługi, a Wykonawca świadczyć jej w celu:
   a) rozpowszechniania treści pornograficznych lub erotycznych, nawołujących do przemocy lub nienawiści rasowej i narodowościowej;
   b) wysyłania masowej niezamawianej poczty elektronicznej (spamming);
   c) prowadzenia lub reklamowania serwisów, zawierających nielegalne produkty komputerowe lub licencje (warez), służących do wymiany plików pomiędzy użytkownikami (p2p) oraz publikowania informacji lub materiałów związanych z piractwem komputerowym (hacking) i łamaniem zabezpieczeń oprogramowania (cracking);
   d) celowego powodowania przeciążenia, przepełniania, blokowania lub natłoku w sieci Internet, innych sieciach transmisji danych lub zasobach drugiej Strony;
   e) naruszania praw osób trzecich, w szczególności dóbr osobistych, praw autorskich i innych praw własności intelektualnej.
4. Wykonawca zobowiązuje się do świadczenia Usługi będącej przedmiotem Umowy z należytą starannością, stosownie do zawodowego charakteru świadczonych usług. W szczególności zobowiązuje się zapewnić ciągłą dostępność Usług w granicach i na warunkach określonych w Zapytaniu, z zastrzeżeniem ust. 6 poniżej.
5. Wykonawca w ramach zapewnienia dostępności Usługi zobowiązuje się do utrzymywania prawidłowego działania i sprawności urządzeń i zasobów sieciowych w ramach sieci wewnętrznej Wykonawcy.
6. Wykonawca zapewnia Zamawiającemu dostępność Usługi na poziomie SLA ..... w skali roku podczas trwania Umowy.
7. Wszelkie przerwy techniczne w dostępności Usługi, niezbędne dla zapewnienia prawidłowości i ciągłości świadczenia Usługi zgodnie z umową, w szczególności w związku z obsługą, konserwacją, rozbudową lub aktualizacją zasobów sieci wewnętrznej Wykonawcy, uniemożliwiające lub ograniczające możliwość korzystania z Usług lub infrastruktury i danych informatycznych Zamawiającego niezbędne dla prawidłowego świadczenia Usługi, nie mogą przekraczać .....min jednorazowo i ..... h w miesiącu. O planowanych przerwach

technicznych Wykonawca poinformuje Zamawiającego nie później niż na 48h przed planowaną przerwą. Informacja zostanie przekazana drogą elektroniczną na adres email Zamawiającego wskazany w paragrafie §2, ust. 1, lit. b) oraz zamieszczona na stronie internetowej Wykonawcy ..... w zakładce ..... .

8. Wykonawca zobowiązuje się do zapewnienia ciągłości funkcjonowania Usługi, w szczególności do usuwania awarii, błędów, ograniczeń w dostępności Usługi. Czas reakcji na zgłoszenie wynosi do 1h od przyjęcia zgłoszenia. Czas realizacji zgłoszenia nastąpi w terminie:
   a) dla błędów kategorii „krytyczny", czyli dla całkowitego braku dostępności Usługi w całości lub w części obejmującej pocztę e-mail, w czasie nie dłuższym niż 4 godziny od przyjęcia zgłoszenia;
   b) dla błędów pozostałych kategorii, czyli dla braku możliwości realizacji zakładanych funkcjonalności lub wystąpienia obniżenia jakości warunków pracy - w czasie nie dłuższym niż 12 godzin od przyjęcia zgłoszenia.
9. Zgłaszanie błędów następować będzie w następujący sposób: .....
10. Wykonawca jest zobowiązany do zapewnienia odpowiednich zabezpieczeń swojej sieci wewnętrznej przed wirusami komputerowymi, atakami hakerskimi lub utratą danych.
11. Zamawiający, w związku z korzystaniem z Usługi, będzie przesyłać, przechowywać lub rozpowszechniać jedynie takie dane, do korzystania z których jest uprawniony i których umieszczenie w zasobach Wykonawcy nie stanowi naruszenia obowiązującego prawa, praw osób trzecich lub zobowiązań umownych Zamawiającego. Wykonawca nie ponosi odpowiedzialności za treść danych przesyłanych, przechowywanych lub rozpowszechnianych przez Zamawiającego w związku z korzystaniem z usług lub za jakiekolwiek naruszenia prawa przez Zamawiającego, jeżeli nie mają one związku z działaniami lub zaniechaniami Wykonawcy. W szczególności Wykonawca nie sprawdza, nie rozpowszechnia ani też w żaden sposób nie wykorzystuje danych przechowywanych lub przesyłanych przez Zamawiającego.
12. W przypadku uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych przesyłanych, przechowywanych lub rozpowszechnianych przez Zamawiającego w związku z korzystaniem z Usługi, Wykonawca podejmie wszelkie środki nakazane przez prawo i przewidziane w Umowie, a ponadto, po uprzednim uzyskaniu wyjaśnień od Zamawiającego, będzie uprawniony do usunięcia danych Zamawiającego naruszających prawo.
13. Wykonawca zobowiązuje się przyznać Zamawiającemu dostęp do indywidualnego konta użytkownika w portalu ..... z narzędziami i dokumentacją dotyczącą Usługi, w szczególności interfejsy opisujące aktualny status infrastruktury serwerowej oraz narzędzia umożliwiające zdalny monitoring i zarzadzanie serwerem, w szczególności jego restartowanie. Dostęp do panelu (login i hasło) zostaną przekazane Zamawiającemu w dniu zawarcia niniejszej Umowy.

§ 5
Odpowiedzialność Stron

1. Wykonawca ponosi pełną odpowiedzialność za zgodny z Umową i przepisami prawa sposób świadczenia Usługi oraz za działania wszelkich osób, którymi posługuje się przy jej świadczeniu, w tym za bezpieczeństwo i integralność danych przechowywanych lub przesyłanych z wykorzystaniem Zasobów udostępnionych przez Wykonawcę
2. Zamawiający jest zobowiązany do należytego zabezpieczenia własnych danych dostępu do indywidualnego Konta Użytkownika w portalu ..... . Zamawiający ponosi pełną odpowiedzialność za skutki świadomego udostępnienia danych dostępu osobom niepowołanym.
3. Wykonawca ponosi na podstawie Umowy odpowiedzialność odszkodowawczą wobec Zamawiającego za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy.
4. Wykonawca nie ponosi odpowiedzialności za ewentualne szkody spowodowane:
   a) okolicznościami powstałymi z wyłącznej winy osób trzecich lub Zamawiającego, w szczególności naruszeniem przez Zamawiającego postanowień Umowy;

b) działaniem nielegalnego oprogramowania zainstalowanego przez Zamawiającego.

§ 6
Prawa autorskie

1. Wykonawca oświadcza i zapewnia, iż posiada majątkowe prawa autorskie lub odpowiednie licencje do korzystania z oprogramowania udostępnianego Zamawiającemu w ramach świadczenia Usługi, a także uprawnienie do sublicencjonowania niniejszego oprogramowania w zakresie niezbędnym do spełnienia zobowiązań objętych niniejszą Umową.
2. O ile jest to konieczne dla prawidłowego świadczenia Usługi, Wykonawca udziela Zamawiającemu niewyłącznej i nieprzenaszalnej licencji/sublicencji na korzystanie z oprogramowania, wskazanego w Załączniku nr 1 do Umowy, w zakresie niezbędnym do korzystania z Usług, zgodnie z ich przeznaczeniem i Umową, w szczególności na następujących polach eksploatacji: trwałe lub czasowe zwielokrotnianie programu komputerowego w całości lub w części jakimkolwiek środkami i w jakiejkolwiek formie, tłumaczenie, przystosowywanie, zmiany układu lub jakiekolwiek inne zmiany w programie komputerowym. Licencja/sublicencja zostaje udzielona na czas trwania Umowy i można z niej korzystać na terytorium Rzeczypospolitej Polski. Wykonawca oświadcza, że Załącznik nr 1 zawiera pełną i kompletną listę oprogramowania, korzystanie z którego przez Zamawiającego jest konieczne do prawidłowego świadczenia Usługi, a jeżeli stan ten ulegnie zmianie - niezwłocznie udzieli Zamawiającemu licencji/ sublicencji na nowe lub zmienione oprogramowanie w zakresie nie węższym, niż określony powyżej.
3. Zamawiający nie jest uprawniony do:
   a) jakichkolwiek poprawek, modyfikacji źródeł i zmian w strukturze przedmiotowego oprogramowania w wersji wynikowej lub jej części;
   b) stosowania przedmiotowego oprogramowania, jego części, fragmentów lub wersji w innym oprogramowaniu;
   c) odsprzedawania, rozpowszechniania, użyczania, dzierżawienia, najmowania, oddawania płatnie i nieodpłatnie osobom trzecim do używania przedmiotowego oprogramowania, jego kopii, wszelkich modyfikacji oraz dokumentacji.

§ 7
Ochrona danych osobowych

1. Zamawiający może w związku z korzystaniem z Usługi przechowywać lub przeprowadzać operacje na danych osobowych.
2. Zamawiający jest administratorem danych osobowych, o których mowa w ust. 1 lub ich procesorem (przetwarzającym powierzone dane osobowe). Wykonawca nie decyduje o celach i środkach przetwarzania tych danych osobowych, a jedynie udostępnia w ramach świadczenia usług zasoby pozwalające na przechowywanie danych. Wykonawca stosuje środki techniczne i organizacyjne zapewniające ochronę danych przechowywanych i przetwarzanych przez Zamawiającego zgodnie z odpowiednimi przepisami ustawy o ochronie danych osobowych oraz 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) – zwane dalej RODO.
3. Wykonawca oświadcza, że serwery fizyczne, za pomocą których świadczone są Usługi, będące przedmiotem Umowy, znajdują się na terenie Unii Europejskiej/EOG, a przechowywane dane w żadnym przypadku w toku świadczenia Usługi nie są przesyłane poza obszar Unii Europejskiej/EOG.
4. O ile będzie to konieczne dla prawidłowego świadczenia Usługi, Strony zobowiązują się do zawarcia odrębnej umowy o powierzeniu przetwarzania danych osobowych, najpóźniej w dniu rozpoczęcia świadczenia usługi będącej przedmiotem niniejszej Umowy.

§ 8
Wymagania techniczne korzystania z Usług

1. Zamawiający przyjmuje do wiadomości, że prawidłowe korzystanie z Usługi może wiązać się z użyciem tzw. plików cookies lub też innych plików posiadających podobną funkcję użytkową.
2. Wykonawca nie ponosi odpowiedzialności za problemy techniczne i ograniczenia techniczne występujące na sprzęcie komputerowym, z którego korzysta Zamawiający, w tym za problemy spowodowane zainstalowaniem lub konfiguracją na sprzęcie komputerowym oprogramowania (firewall'e - blokady, niewłaściwe wersje odtwarzacza plików multimedialnych, programy antywirusowe i inne), które uniemożliwia Zamawiającemu korzystanie z Usług, o ile poinformował uprzednio Zamawiającego o możliwości wystąpienia tego rodzaju problemów związanych z instalacją konkretnego oprogramowania oraz pod warunkiem, że sprzęt lub oprogramowanie nie było dostarczane lub licencjonowane przez Wykonawcę.

§ 9
Wsparcie techniczne

1. Wykonawca zobowiązuje się do usuwania awarii, błędów urządzeń, za prawidłowe działanie, których ponosi odpowiedzialność, zgodnie z postanowieniami Umowy. Za awarię, błąd uważa się nieprawidłowe działanie urządzenia, powodujące przerwę w świadczeniu Usług, trwające dłużej niż 15 minut w ciągu doby.
2. Abonent może zgłaszać awarie, błędy pocztą elektroniczną na adres: ..... . W przypadku otrzymania zgłoszenia awarii, błędu Operator w najkrótszym możliwym czasie nie dłuższym niż 1 godzina dokona analizy zasadności zgłoszenia oraz usunie błąd lub awarię w terminach określonych w § 4 ust. 8 Umowy.
3. Jeżeli w wyniku analizy zasadności zgłoszenia nie zostanie potwierdzone istnienie awarii lub jeśli ustalona przyczyna awarii Wykonawca powiadomi Zamawiającego o braku podstaw do interwencji.
4. Jeżeli w wyniku analizy zasadności zgłoszenia zostanie ustalona przyczyna awarii, mieszcząca się w zakresie odpowiedzialności Wykonawcy, Wykonawca niezwłocznie przystąpi do usuwania awarii i powiadomi Zamawiającego o przewidywanym terminie jej usunięcia, nie dłuższym niż 12 godzin. Wykonawca zobowiązuje się do usuwania awarii w najwcześniejszym możliwym terminie w normalnym toku czynności, z uwzględnieniem charakteru i rozmiaru awarii.
5. W przypadkach wskazanych w niniejszym paragrafie zastosowanie znajdują terminy określone w § 4 ust. 8 Umowy.
6. Czas prowadzenia analizy zasadności zgłoszenia awarii i sposobu usuwania awarii jest wliczany do czasu dostępności Usługi dla Abonenta.
7. Operator może odmówić udzielenia wsparcia technicznego jeżeli:
   a) w systemie operacyjnym maszyn wirtualnych uruchomionych w ramach Usługi nie będzie zainstalowane oprogramowanie VMware Tools.
   b) pojemność pojedynczego dysku wirtualnego przekracza 2 TB.

§ 10
Ochrona Informacji Poufnych

1. Strony zobowiązują się do zachowania ścisłej poufności polegającej na tym, iż nie ujawnią żadnej nieuprawnionej osobie trzeciej informacji poufnych, określonych w ust. 2 i 3 poniżej (dalej jako „**Informacje Poufne**"). Strony nie mogą wykorzystywać Informacji Poufnych inaczej niż do celów określonych w niniejszej Umowie. Uchylenie zobowiązania do zachowania poufności wymaga uprzedniej pisemnej zgody odpowiedniej Strony niniejszej Umowy.
2. Przez Informacje Poufne Strony rozumieją informacje lub materiały odnoszące się do działalności Strony oraz stosunków cywilnoprawnych łączących Strony z podmiotami trzecimi lub wzajemnie oraz informacje wynikające lub związane z takimi stosunkami, a także wszelkie informacje dotyczące Stron i związane z prowadzoną przez Strony działalnością gospodarczą, informacje finansowe, techniczne, naukowe oraz informacje innego rodzaju, włączając w powyższe

specyfikacje, a także informacje dotyczące ich podmiotów zależnych lub podmiotów z nimi trwale powiązanych kontraktami, które zostały ujawnione przez jedną ze Stron („Stronę Ujawniającą") drugiej Stronie („Stronie Otrzymującej") w związku z wykonywaniem Umowy lub przekazane przez osobę trzecią będącą wykonawcą, działającą w imieniu Strony. Informacjami Poufnymi są także dane, które posiadając wartość gospodarczą mogą być uznane za poufne lub zostały udostępnione drugiej z zastrzeżeniem poufności, niezależnie od formy ich udostępnienia w jakiejkolwiek formie oraz na jakimkolwiek nośniku, zarówno materialnym, jak i niematerialnym, w tym ustnie, na piśmie lub drogą elektroniczną.

3. Za Informacje Poufne w rozumieniu niniejszej Umowy uznaje się również treść danych przechowywanych lub przesyłanych przez Zamawiającego z wykorzystaniem zasobów Wykonawcy udostępnionych w związku ze świadczeniem Usług.
4. Strona Otrzymująca zachowa Informacje Poufne Strony Ujawniającej w tajemnicy i w stosunku do nich podejmie co najmniej takie same środki ostrożności, gwarantując tym samym, że zapewniają one odpowiednią ochronę przeciwko nieupoważnionemu ujawnieniu, kopiowaniu lub wykorzystaniu. Strona Otrzymująca zapewni, że ujawnianie Informacji Poufnych ograniczone będzie do tych pracowników, członków władz Strony Otrzymującej, którym wiedza taka jest niezbędna dla realizacji Umowy i którzy będą poinformowani o obowiązkach Stron wynikających z Umowy, i zobowiązani do postępowania zgodnie z zasadami wynikającymi z Umowy. Strony nie będą wykonywać kopii Informacji Poufnych, chyba że będzie to konieczne w zakresie niezbędnym dla realizacji Umowy, a wszelkie wykonane kopie będą zwrócone Stronie Ujawniającej w ciągu trzydziestu dni od otrzymania pisemnego żądania od Strony Ujawniającej lub zostaną usunięte po upływie 14 od dnia rozwiązania lub wygaśnięcia Umowy.
5. Obowiązek zachowania poufności nie dotyczy Informacji Poufnych:
   a) których ujawnienia wymagają bezwzględnie obowiązujące przepisy prawa;
   b) których ujawnienie następuje na żądanie podmiotu uprawnionego na podstawie przepisów prawa do kontroli, pod warunkiem; że podmiot ten został poinformowany o poufnym charakterze informacji;
   c) które są lub staną się publicznie dostępne w jakikolwiek sposób bez naruszenia Umowy przez Stronę Otrzymującą;
   d) które Strona uzyskała lub uzyska od osoby trzeciej, jeżeli przepisy obowiązującego prawa wiążące tę osobę nie zakazują ujawniania przez nią tych informacji i o ile Strona umowy nie zobowiązała się do zachowania poufności;
   e) w których posiadanie Strona weszła zgodnie z obowiązującymi przepisami prawa, przed dniem uzyskania takich informacji na podstawie Umowy;
   f) dotyczących faktu zawarcia Umowy, z wyłączeniem jej postanowień szczególnych, chyba że obowiązek jej ujawnienia wynika z przepisów powszechnie obowiązującego prawa oraz w zakresie wykorzystania tej okoliczności w materiałach marketingowych Strony lub ewentualnie referencji i potwierdzenia posiadanych kompetencji;
   g) dotyczących faktu zawarcia Umowy oraz jej postanowień szczególnych, których ujawnienie następuje na żądanie podmiotu prowadzącego audyt lub świadczącego pomoc prawną pod warunkiem, że podmiot ten został poinformowany o poufnym charakterze informacji i został zobowiązany do zachowania przekazanych informacji w poufności.
6. W wypadku, gdy Strona zostanie zobowiązana nakazem sądu bądź organu administracji państwowej do ujawnienia Informacji Poufnych albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, zobowiązuje się niezwłocznie pisemnie powiadomić o tym fakcie druga Stronę oraz poinformować odbiorcę Informacji Poufnych o ich poufnym charakterze.
7. Obowiązek zachowania poufności wiąże Strony w okresie obowiązywania Umowy jak również przez okres 5 lat po jej wygaśnięciu lub rozwiązaniu w przypadku Zamawiającego, a bezterminowo – w przypadku Wykonawcy.

§ 11
Kary umowne

1. W przypadku wystąpienia przerw bądź utrudnień w dostępności Usługi, których łączny czas spowoduje spadek dostępności Usługi poniżej gwarantowanego poziomu, o którym mowa w §4 ust. 6 umowy Abonent jest uprawniony do naliczenia kary umownej w wysokości:

   rekompensata za każdy rozpoczęty 1% niedostępności Usługi poniżej gwarantowanego w Umowie poziomu , o którym mowa w § 4 ust. 6 wynosi 10% wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy, łącznie nie więcej niż 100% wartości wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy.

2. Strony przewidują zapłatę kar umownych również w następujących przypadkach i wysokościach:

   a) za opóźnienie Wykonawcy w zareagowaniu na awarie (błędy), w stosunku do terminu określonego w § 9 ust. 2 umowy w wysokości 1% 1/12 wynagrodzenia brutto określonego w § 3 ust. 1 za każdą rozpoczętą godzinę opóźnienia.

   b) za opóźnienie Wykonawcyw usunięciu awarii, w stosunku do terminu określonego w § 4 ust. 8 Wykonawca zapłaci karę umowną w wysokości 1% 1/12 wynagrodzenia brutto określonego w § 3 ust. 1 za każdą rozpoczętą godzinę opóźnienia.

   3. W przypadku wystąpienia okoliczności uzasadniających zapłatę przez Wykonawcę kar umownych, Zamawiający może według własnego wyboru:

   a) potrącać kary umowne z wynagrodzenia należnego Wykonawcy;

   b) wezwać Wykonawcę do zapłaty kar umownych w terminie 14 dni od daty otrzymania pisemnego wezwania do ich zapłaty.

   4. Zastrzeżenie kar umownych nie wyłącza możliwości dochodzenia przez Zamawiającego odszkodowania na zasadach ogólnych za szkodę przewyższającą wartość zastrzeżonych kar.

§ 12
Ograniczenie, zawieszenie Usług, Reklamacje

1. Reklamacje Zamawiającego w związku z niewykonaniem lub nienależytym wykonaniem Usługi powinny określać:
   a) numer i datę zawarcia Umowy;
   b) nazwę Zamawiającego
   c) rodzaj Usługi i parametry techniczne, które zostały naruszone;
   d) zarzuty Zamawiającego i okoliczności uzasadniające reklamację,
   e) ewentualny proponowany sposób rozstrzygnięcia reklamacji.
2. Wykonawca udzieli odpowiedzi na reklamację w terminie 7 dni od momentu jej otrzymania.
3. W odpowiedzi na reklamację Wykonawca wskaże ,czy uznaje reklamację oraz w jaki sposób zamierza ją rozpatrzyć lub poinformuje o braku podstaw do uznania reklamacji wraz z uzasadnieniem swojego stanowiska.

§ 13
Okres obowiązywania Umowy

1. Niniejsza Umowa została zawarta na czas określony od dnia ..... do dnia ..... roku.
2. Zamawiający ma prawo rozwiązać Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca.
3. Wykonawca ma prawo do natychmiastowego zaprzestania świadczenia Usługi oraz do rozwiązania Umowy bez zachowania okresu wypowiedzenia, jeżeli pomimo pisemnego wezwania do przywrócenia stanu zgodnego z prawem lub umową w wyznaczonym, ni krótszym niż 7 dni terminie Zamawiający:

a) narusza przepisy prawa w związku z realizacją Umowy lub narusza postanowienia Umowy;

4. Zamawiający ma prawo do natychmiastowego rozwiązania Umowy bez zachowania okresu wypowiedzenia, jeśli

   a) przerwa w dostępie do Usługi, niezależnie od jej przyczyny, trwa dłużej niż 3 dni.

   b) w przypadku powtarzających się opóźnień w obsłudze zgłoszeń awarii określonych § 9 umowy lub ich usuwaniu.

5. Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy;
6. Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o okolicznościach uzasadniających odstąpienie.
7. W przypadku odstąpienia od umowy Wykonawca może żądać wynagrodzenia jedynie za część umowy należycie wykonaną do dnia ustania obowiązywania umowy.
8. Oświadczenie o odstąpieniu, wypowiedzeniu lub rozwiązaniu Umowy powinno zostać złożone na piśmie pod rygorem nieważności.
9. Po zakończeniu obowiązywania Umowy, Wykonawca zobowiązany jest w terminie do 7 dni od zakończenia obowiązywania Umowy, zapisać dane zgromadzone na udostępnionych przez Operatora serwerach na nośniku fizycznym w powszechnie obsługiwanym formacie umożliwiającym edycję i przekazać je Abonentowi lub, w przypadku otrzymania od Zamawiającego zgody, dane umieścić na serwerze ftp i udostępnić Zamawiającemu. Następnie Wykonawca, po potwierdzeniu przez Zamawiającego otrzymania zapisanych danych, zobowiązany jest usunąć dane z serwerów Wykonawcy. Wykonawca z chwilą wydania i w ramach wynagrodzenia określonego w niniejszej Umowie przenosi na zamawiającego prawo własności nośnika fizycznego, na którym utrwalono dane.

§ 14

Postanowienia końcowe

1. Wszelkie zmiany Umowy wymagają formy pisemnego aneksu pod rygorem nieważności.
2. Prawem właściwym dla zobowiązań wynikających z Umowy jest prawo polskie.
3. Wszelkie spory wynikające z Umowy będą rozstrzygane przez sąd właściwy dla siedziby Zamawiającego. Strony zobowiązują się w każdym przypadku dążyć do ugodowego rozstrzygnięcia sporu powstałego na gruncie stosowania niniejszej Umowy.
4. Żadna ze Stron Umowy nie może przenieść praw lub obowiązków z niej wynikających na osobę trzecią bez uprzedniej pisemnej zgody drugiej Strony.
5. Wszelkie zawiadomienia i oświadczenia związane z wykonywaniem Umowy mogą być składane za pomocą poczty elektronicznej na adresy email wskazane w paragrafie §2, ust. 1, za wyjątkiem oświadczeń dla których Umowa wyraźnie wymaga formy pisemnej. Oświadczenia w formie pisemnej przesyłane będą na adresy Stron podane na wstępie Umowy, z zastrzeżeniem ust. 6 poniżej.
6. O każdej zmianie adresu e-mail do korespondencji lub adresu pocztowego, Strona niezwłocznie powiadomi drugą Stronę w formie pisemnej.
7. Zapytanie ofertowe nr 18/2019 z dnia ..... i oferta Wykonawcy z dnia ....., stanowią załączniki nr ..... i ..... do niniejszej umowy i stanowią jej integralną część..
8. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Wykonawca **Zamawiający**

Zamówienie publiczne 18/2019

Załącznik nr 1. Podstawowe parametry środowiska Cloud do umowy nr: .....
z dnia .....

	Parametry IaaS	**Ilość**
1	vCPU Intel® Xeon® 2.4 GHz	
2	GB Ram Pamięć	
3	GB HDD 30 000 IOPS	
4	IPv4 zewnętrzne adresy (jeden w cenie)	
5	Microsoft® Exchange Standard 15 GB – skrzynka	
6	Microsoft® Exchange Basic 10 GB – skrzynka	
7	Ochrona antywirusowa dla stacji roboczych i serwerów fizycznych	
8	System Servicedesk	

*W związku z aktualizacją cenników dostawców zewnętrznych koszty oprogramowania/ licencji mogą podlegać aktualizacji cen. W przypadku braku akceptacji zaktualizowanych cen przez Zamawiającego ma on prawo do natychmiastowego wypowiedzenia umowy.

System operacyjny Linux	w cenie usługi
System operacyjny Microsoft Windows Server 2012 & 2016	w cenie usługi
Wirtualizacja VMware	w cenie usługi
Łącze symetryczne 100/100 Mbps bez limitu transferu	w cenie usługi
Ochrona DDoS	w cenie usługi
Port sieciowy 1 GB	w cenie usługi
VPN S2S (do 64 tuneli)	w cenie usługi
Backup co 24h, przechowywany do 7 dni	w cenie usługi
Snapshot przechowywany do 7 dni	w cenie usługi
Zarządzanie i billing OnApp	w cenie usługi
Zarządzanie zaawansowane vCloud Director	w cenie usługi