Usługi informatyczne w zakresie hostingu i ochrony. 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.

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 poniżej 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 poniżej parametrami wymaganymi przez Zamawiającego.

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

KOD CPV:

48800000-6 – Systemy i serwery operacyjne

72415000-2 - Usługi hostingowe dla stron WWW

72317000-0 - Usługi przechowywania danych

II. Termin rozpoczęcia świadczenia usługi

Od dnia 01.01.2019 przez okres 12 miesięcy.

III. Miejsce i termin składnia 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 21.12.2018 r. do godz. 12:00.**

IV. Sposób obliczania ceny

1. Wykonawca poda cenę brutto oferty w Formularzu Ofertowym, sporządzonym według wzoru stanowiącego Załącznik Nr 1. Cena ofertowa podana przez wykonawcę w Formularzu Oferty zostanie ustalona na okres ważności umowy i nie będzie podlegała zmianom.
2. Ceny muszą być wyrażone w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
3. Wykonawca musi uwzględnić w cenie oferty wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania zamówienia oraz wszelkie opłaty i podatki wynikające z obowiązujących przepisów.

4. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
5. Rozliczenia między zamawiającym a wykonawcą będą prowadzone w PLN.

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.
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.

   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.
4. 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.
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.

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	Przepustowość łącza do sieci Internet	5

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

$$\frac{\text{oferta najtańsza}}{\text{oferta badana}} \times 50 = LP$$

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

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 w 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.

VII. 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 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	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.

	zgodnie z EN 1143-1.	
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 100Mbps	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	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i

	Klienta (Zamawiającego) przez przynajmniej15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną	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 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 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.
13	Bezpiecznie szyfrowane połączenie do środowiska zamawiającego umożliwiające obsługę administracyjną oraz pracę z użyciem indywidualnych kont użytkowników.	Zagrożenie wynikające z niezabezpieczonego połączenia zdalnego umożliwiającego wgląd w transmisję danych.
	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.
4	Stały monitoring parametrów środowiska klienta w zakresie wydajności, przepustowości, wykorzystania zasobów indywidualnie dla każdego systemu.	Zagrożenie chwilowej, lub całkowitej niewydolności systemu lub serwera spowodowanego obciążeniem.

VIII. 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.

Zamówienie publiczne 26/2018

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
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 – 115 kont

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 – 17 kont

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 – 115 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

6. Specyfikacja systemu obsługi zgłoszeń - Servicedesk

Lp.	Minimalne wymagania
1	Obsługę indywidualnych kont dla zgłaszających
2	Komunikację dwukierunkową ze zgłaszającym bezpośrednio z systemu
3	Możliwość tworzenia powiązań pomiędzy zadaniami
4	Możliwość indywidualnego tworzenia przepływu zgłoszeń osobno dla każdego typu zgłoszeń
5	Zarządzanie uprawnieniami
6	Zarządzanie powiadomieniami
7	Integracja z pocztą e-mail

Załączniki:

- Załącznik nr 1 – formularz ofertowy

- Załącznik nr 2 – wzór umowy

DYREKTOR
TORUŃSKIEGO CENTRUM USŁUG WSPÓLNYCH
Paweł Modrzyński

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	Zagrożenie długotrwałego zalania	

	najmniej 5 metrów powyżej poziomu wody stuletniej	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 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	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.	

	1143-1.		
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 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	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji	

	pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Klientowi (Zamawiającemu). Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	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

_____

Zamówienie publiczne 26/2018

Załącznik nr 2 - wzór umowy

UMOWA USŁUGI CLOUD

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, zwaną dalej Zamawiającym,

reprezentowaną przez:

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

zwaną dalej **Abonentem**,

a

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

reprezentowanym/ą przez:

.....

zwane dalej **Stronami.**

§1
Przedmiot Umowy

1. *Przedmiotem Umowy jest świadczenie przez Operatora na rzecz Abonenta usługi chmury obliczeniowej w modelu PaaS (Platform as a Service), zwanej dalej* ***Usługą****, polegającej na oddaniu do dyspozycji Abonenta zasobów informatycznych w postaci m.in.: powierzchni dyskowej, pamięci operacyjnej oraz mocy obliczeniowej z oprogramowaniem lub bez.*
2. Operator 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 Abonenta w zakresie i terminie zgodnym ze złożonym drogą elektroniczną zamówieniem (dalej jako **Zamówienie**).
4. Operator udostępni Usługę w dniu 1.01.2019r.

§2
Komunikacja

1. Wszelkie komunikaty, zamówienia, informacje i dokumenty związane z realizacją zawartej Umowy Strony będą przekazywały sobie drogą elektroniczną na adresy email:
   a) Operator wyznacza adres email: .....

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 4/2017 na podstawie § 11 Regulaminu Organizacyjnego Toruńskiego Centrum Usług Wspólnych.

b) Abonent wyznacza adres email: sekretariat@tcuw.torun.pl, l.nowak@tcuw.torun.pl,

2. Każda ze Stron nie ponosi odpowiedzialności za skutki wadliwego funkcjonowania serwera pocztowego lub skrzynki odbiorczej poczty elektronicznej drugiej Strony.

§3
Wynagrodzenie

1. W zamian za świadczenie Usługi na zasadach określonych w niniejszej Umowie, Abonent zobowiązuje się do zapłaty na rzecz Operatora wynagrodzenia w wysokości ..... zł brutto (słownie: ..... zł 00/100 gr) płatnego w 12 miesięcznych ratach. W przypadku rozszerzenia parametrów podstawowych na podstawie Zamówienia, o którym mowa w paragrafie 1, ust. 1 Abonent zobowiązuje się do zapłaty na rzecz Operatora wynagrodzenia w wysokości ustalonej na podstawie obowiązujących u Operatora cen, wyliczonego na podstawie złożonych przez Abonenta zamówień w danym okresie rozliczeniowym.
2. Pełny okres rozliczeniowy rozpoczyna się pierwszego dnia kalendarzowego miesiąca i kończy w ostatnim dniu kalendarzowym tego samego miesiąca.
3. Wynagrodzenie, o którym mowa w ust. 1 naliczane będzie od dnia 01.01.2019 r.
4. Do należnego Operatorowi Wynagrodzenia każdorazowo zostanie doliczony należny podatek VAT według obowiązującej stawki w dniu obowiązywania Umowy.
5. Płatność Wynagrodzenia, o którym mowa w ust.1 nastąpi na podstawie faktury vat wystawianej na koniec ostatniego dnia danego okresu rozliczeniowego z terminem płatności 14 dni.
6. Abonent wyraża zgodę na otrzymywanie faktur vat drogą elektroniczną w formacie PDF, na adres email Abonenta wskazany w paragrafie §2, ust. 1, lit. b).
7. Za dzień dokonania zapłaty Strony uznają dzień, w którym zostanie obciążony rachunek bankowy Abonenta.

§4
Prawa i obowiązki Stron

1. Abonent na podstawie niniejszej Umowy otrzymuje możliwość korzystania z Usługi w okresie ustalonym w Umowie.
2. Abonent 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. Abonent w szczególności nie może korzystać z Usługi 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 Operatora;
   e) naruszania praw osób trzecich, w szczególności dóbr osobistych, praw autorskich i innych praw własności intelektualnej.
4. Operator 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, z zastrzeżeniem ust. 6 poniżej. Usługi udostępniane za pomocą strony internetowej uznaje się za dostępne dla Abonenta jeżeli są widzialne na pierwszym routerze poza siecią Operatora.
5. Operator w ramach zapewnienia dostępności Usługi zobowiązuje się wyłącznie do utrzymywania prawidłowego działania i sprawności urządzeń i zasobów sieciowych w ramach sieci wewnętrznej Operatora. Operator nie ponosi odpowiedzialności za okoliczności leżące po stronie innych podmiotów, w szczególności działania operatorów telekomunikacyjnych, dostawców dostępu do sieci Internet i sieci komórkowych, awarie zasilania, niewłaściwe funkcjonowanie urządzeń poza siecią wewnętrzną Operatora.

6. Operator zapewnia Abonentowi dostępność Usługi na poziomie SLA ..... w skali roku podczas trwania Umowy.
7. W celu zapewnienia odpowiedniego standardu świadczenia Usługi Operator zastrzega sobie prawo do robienia możliwie jak najkrótszych przerw technicznych nie dłuższych niż.....w dostępności Usługi w związku z obsługą, konserwacją, rozbudową lub aktualizacją zasobów sieci wewnętrznej Operatora. O planowanych przerwach technicznych Operator poinformuje Abonenta nie później niż na 48h przed planowaną przerwą. Informacja zostanie przekazana drogą elektroniczną na adres email Abonenta wskazany w paragrafie §2, ust. 1, lit. b) i/lub zamieszczona na .....
8. Operator zobowiązuje się do zapewnienia ciągłości funkcjonowania Usługi, w szczególności do usuwania awarii, błędów, leżących po stronie Operatora w dostępności Usługi, w terminie:
   a) dla błędów kategorii „krytyczny", czyli dla całkowitego braku dostępności Usługi w czasie 4 godzin od przyjęcia zgłoszenia;
   b) dla błędów kategorii „średni", czyli dla braku możliwości realizacji zakładanych funkcjonalności lub wystąpienia obniżenia jakości warunków pracy - w czasie do zakończenia następnego dnia roboczego następującego po dniu przyjęcia zgłoszenia błędu.
9. Operator jest zobowiązany do zapewnienia odpowiednich zabezpieczeń swojej sieci wewnętrznej przed wirusami komputerowymi, atakami hakerskimi lub utratą danych. Odpowiedzialność Operatora ogranicza się do wprowadzenia tych zabezpieczeń.
10. Abonent w związku z korzystaniem z Usługi, może przesyłać, przechowywać lub rozpowszechniać jedynie takie dane, do korzystania z których jest uprawniony i których umieszczenie w zasobach Operatora nie stanowi naruszenia obowiązującego prawa, praw osób trzecich lub zobowiązań umownych. Operator nie ponosi odpowiedzialności za treść danych przesyłanych, przechowywanych lub rozpowszechnianych przez Abonenta w związku z korzystaniem z usług, lub za jakiekolwiek naruszenia prawa przez Abonenta. W szczególności Operator nie sprawdza, nie rozpowszechnia, ani też w żaden sposób nie wykorzystuje danych przechowywanych lub przesyłanych przez Abonenta.
11. W przypadku uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych przesyłanych, przechowywanych lub rozpowszechnianych przez Abonenta w związku z korzystaniem z Usługi, Operator podejmie wszelkie środki nakazane przez prawo i przewidziane w Umowie, a ponadto będzie uprawniony do usunięcia danych Abonenta.
12. Operator zobowiązuje się przyznać Abonentowi 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 Abonentowi w terminie do dnia 1.01.2019r.

§ 5
Odpowiedzialność Stron

1. Abonent ponosi pełną odpowiedzialność za zgodny z Umową i przepisami prawa sposób korzystania z Usługi oraz za działania wszelkich osób, którym udostępnia zasoby otrzymane od Operatora w ramach świadczenia Usługi.
2. Abonent jest zobowiązany do należytego zabezpieczenia własnych danych dostępu do indywidualnego Konta Użytkownika w portalu ..... . Abonent ponosi pełną odpowiedzialność za skutki udostępnienia danych dostępu osobom niepowołanym, bez względu na sposób w jaki to udostępnienie nastąpiło, także jeśli miało to miejsce wskutek niedbałości Abonenta.
3. Z zastrzeżeniem ust. 4 Operator może ponosić na podstawie Umowy odpowiedzialność odszkodowawczą wobec Abonenta za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy.
4. Operator nie ponosi odpowiedzialności za ewentualne szkody spowodowane:
   a) brakiem dostępności Usługi dla Abonenta, chyba że ten brak wynika z powodu okoliczności leżących po stronie Operatora, z zastrzeżeniem § 4 ust. 7 Umowy;
   b) okolicznościami powstałymi z winy osób trzecich lub Abonenta, w szczególności naruszeniem przez Abonenta postanowień Umowy;
   c) działaniem oprogramowania zainstalowanego przez Abonenta;

d) działaniem wirusów komputerowych lub atakami hakerskimi lub utratą danych przez Abonenta, pod warunkiem wprowadzenia zabezpieczeń, o których mowa w § 4 ust. 9 Umowy.

5. *W przypadku wystąpienia przez osoby trzecie z jakimikolwiek roszczeniami względem Operatora w związku ze sposobem korzystania z Usługi przez Abonenta, Abonent zobowiązuje się zwolnić Operatora z wszelkiej odpowiedzialności. Abonent podejmie niezbędne działania mające na celu zażegnanie sporu i poniesie w związku z tym wszelkie uzasadnione koszty. W szczególności, w przypadku wytoczenia przez osobę trzecią powództwa przeciwko Operatorowi, Abonent wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie pozwanej oraz pokryje wszelkie uzasadnione koszty i odszkodowania, w tym uzasadnione koszty obsługi prawnej poniesione przez Operatora.*

§ 6
Prawa autorskie

1. Operator oświadcza i zapewnia, iż posiada majątkowe prawa autorskie lub odpowiednie licencje do korzystania z oprogramowania udostępnianego Abonentowi w ramach świadczenia Usługi, a także uprawnienie do sublicencjonowania niniejszego oprogramowania w zakresie niezbędnym do spełnienia zobowiązania z ust. 2 poniżej.
2. O ile jest to konieczne dla prawidłowego świadczenia Usługi, Operator udziela Abonentowi 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.
3. Abonent nie jest uprawniony do:
   a) korzystania z oprogramowania na większej liczbie stanowisk niż to wynika z nadanych uprawnień, 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. Abonent może w związku z korzystaniem z Usługi przechowywać lub przeprowadzać operacje na danych osobowych.
2. Administratorem danych osobowych, o których mowa w ust. 1 powyżej jest Abonent. Operator nie decyduje o celach i środkach przetwarzania tych danych osobowych, a jedynie udostępnia w ramach świadczenia usług zasoby pozwalające na przechowywanie danych. Operator stosuje środki techniczne i organizacyjne zapewniające ochronę danych przechowywanych i przetwarzanych przez Abonenta 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. W przypadku uzyskania wiarygodnej wiadomości o korzystaniu przez Abonenta z usług będących przedmiotem Umowy w sposób sprzeczny z przepisami ustawy o ochronie danych osobowych lub 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 Operator podejmie wszelkie środki nakazane przez prawo i przewidziane w Umowie,
4. Operator oświadcza, że serwery fizyczne za pomocą których świadczone są Usługi będące przedmiotem Umowy znajdują się na terenie Rzeczpospolitej Polskiej, a przechowywane dane w żadnym przypadku w toku świadczenia Usługi nie są przesyłane poza obszar Rzeczpospolitej Polskiej.

5. O ile będzie to konieczne dla prawidłowego świadczenia Usługi Strony zobowiązują się do zawarcia odrębnej umowy o powierzeniu przetwarzania danych osobowych.

§ 8
Wymagania techniczne korzystania z Usług

1. Abonent 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. *Operator nie ponosi odpowiedzialności za problemy techniczne i ograniczenia techniczne występujące na sprzęcie komputerowym, z którego korzysta Abonent, 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 Abonentowi korzystanie z Usług.*

§ 9
Wsparcie techniczne

1. Operator zobowiązuje się do usuwania awarii, błędów urządzeń w ramach swojej sieci wewnętrznej, 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.
2. Abonent może zgłaszać awarie, błędy pocztą elektroniczną na adres: ..... . W przypadku otrzymania zgłoszenia awarii, błędu Operator w najkrótszym możliwym czasie nie dłuższym niż 48 godzin dokona analizy zasadności zgłoszenia.
3. Jeżeli w wyniku analizy zasadności zgłoszenia nie zostanie potwierdzone istnienie awarii lub jeśli ustalona przyczyna awarii nie wynika z okoliczności, za które odpowiedzialność ponosi Operator, Operator powiadomi Abonenta o braku podstaw do interwencji.
4. Jeżeli w wyniku analizy zasadności zgłoszenia zostanie ustalona przyczyna awarii mieszcząca się w zakresie odpowiedzialności Operatora, Operator niezwłocznie przystąpi do usuwania awarii i powiadomi Abonenta o przewidywanym terminie jej usunięcia. Operator 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. Informacjami Poufnymi są również informacje, których obowiązek utrzymania w tajemnicy obciąża Stronę na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

3. Za Informacje Poufne w rozumieniu niniejszej Umowy uznaje się również treść danych przechowywanych lub przesyłanych przez Abonenta z wykorzystaniem zasobów Operatora 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 własnością Strony Ujawniającej. Wszelkie Informacje Poufne oraz ich kopie zostaną 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 lub zobowiązanie umowne 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, 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.

§ 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:

a) rekompensata za każdy 1% niedostępności Usługi poniżej gwarantowanego w Umowie poziomu , o którym mowa w *§4, ust. 6* wynosi 10% 1/12 wartości wynagrodzenia brutto , o którym mowa w *§3* ust. 1 Umowy z zastrzeżeniem §5 ust. 3 i 4 Umowy;

b) maksymalna rekompensata w jednym okresie rozliczeniowym wynosić do 100% wartości wynagrodzenia brutto okresu rozliczeniowego, o którym mowa w *§3* ust. 1 Umowy.

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

a) za opóźnienie Operatora 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 godzinę opóźnienia.

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

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

a) potrącać kary umowne z wynagrodzenia należnego Operatorowi;

b) wezwać Operatora 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 Abonenta odszkodowania na zasadach ogólnych za szkodę przewyższającą wartość zastrzeżonych kar.

§ 12
Ograniczenie, zawieszenie Usług, Reklamacje

1. *W przypadku jakiegokolwiek naruszenia przez Abonenta postanowień Umowy*, jak również w przypadku otrzymania przez Operatora uzasadnionej wiadomości o naruszeniu przez *Abonenta* w związku z korzystaniem z Usługi przepisów prawa, dobrych obyczajów lub praw osób trzecich, *Operatorowi* przysługuje w każdym czasie, bez prawa Abonenta do jakiegokolwiek odszkodowania lub zwrotu kosztów, uprawnienie do czasowego ograniczenia lub zawieszenia świadczonych Usług ze skutkiem natychmiastowym.
2. Reklamacje Abonenta w związku z niewykonaniem lub nienależytym wykonaniem Usługi powinny określać:
   a) numer i datę zawarcia Umowy;
   b) nazwę Abonenta
   c) rodzaj Usługi i parametry techniczne;
   d) zarzuty Abonenta i okoliczności uzasadniające reklamację,
   e) ewentualny proponowany sposób rozstrzygnięcia reklamacji.
3. Operator udzieli odpowiedzi na reklamację w terminie 7 dni od momentu jej otrzymania. W przypadku gdy reklamacja zgłoszona przez Abonenta będzie wymagała uzupełnienia, termin na odpowiedź liczy się od momentu otrzymania ostatecznych wymaganych przez Operatora informacji.
4. W odpowiedzi na reklamację Operator wskaże czy uznaje reklamację oraz w jaki sposób zamierza ją rozpatrzyć lub poinformuje o braku podstaw do uznania reklamacji wraz z uzasadnieniem swojego stanowiska.
5. Stanowisko Operatora w sprawie reklamacji jest ostateczne.

§ 13
Okres obowiązywania Umowy

1. Niniejsza Umowa została zawarta na czas określony od dnia 1.01.2019 r. do dnia 31.12.2019 roku.
2. Abonent ma prawo rozwiązać Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca.

3. Operator ma prawo do natychmiastowego zaprzestania świadczenia Usługi oraz do rozwiązania Umowy bez zachowania okresu wypowiedzenia, jeżeli:
   a) Abonent narusza przepisy prawa lub postanowienia Umowy;
   b) Abonent korzysta z Usługi w sposób sprzeczny z jej przeznaczeniem i parametrami technicznymi;
   c) Abonent korzysta z Usługi w sposób niezgodny w Umową a grożący wyrządzeniem szkody Operatorowi, innym Klientom Operatora lub użytkownikom sieci Internet.
   d) Abonent dopuszcza się zwłoki z zapłatą Wynagrodzenia określonego w §3 niniejszej Umowy co najmniej przez 14 dni.
4. Abonent 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
5. Abonent 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; Abonent może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach,
6. W przypadku odstąpienia od umowy Operator może żądać wynagrodzenia jedynie za część umowy wykonaną do dnia ustania obowiązywania umowy.
7. Oświadczenie o odstąpieniu, wypowiedzeniu lub rozwiązaniu Umowy powinno zostać złożone na piśmie pod rygorem nieważności.
8. Po zakończeniu obowiązywania Umowy, Operator 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 i przekazać je Abonentowi lub, w przypadku otrzymania od Abonenta zgody, dane umieścić na serwerze ftp i udostępnić Abonentowi. Następnie Operator zobowiązany jest usunąć dane z serwerów Operatora. Operator zobowiązuje się przenieść na zamawiającego prawo własności nośnika fizycznego na którym utrwalono dane.

§ 14

Postanowienia końcowe

1. Wszelkie zmiany Umowy wymagają formy pisemnej 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 Abonenta. 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. Opis przedmiotu zamówienia i oferta Operatora stanowią załączniki do niniejszej umowy i stanowią jej integralną część..
8. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Operator	Abonent

Zamówienie publiczne 26/2018

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

	Parametry IaaS	**Ilość**
1	vCPU Intel® Xeon® 2.4 GHz	8
2	GB Ram Pamięć	13
3	GB HDD 30 000 IOPS	500
4	IPv4 zewnętrzne adresy (jeden w cenie)	4
5	Microsoft® Exchange Standard 15 GB – skrzynka	10
6	Microsoft® Exchange Basic 10 GB – skrzynka	115
7	Bitdefender GravityZone dla stacji roboczych i serwerów fizycznych	115
8	System Servicedesk	1

*W związku z aktualizacją cenników dostawców zewnętrznych koszty oprogramowania/ licencji mogą podlegać aktualizacji cen. W przypadku braku akceptacji zaktualizowanych cen przez Abonenta 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