Toruńskie Centrum Usług Wspólnych
87-100 Toruń, pl. św. Katarzyny 9, tel. +48 56 611 89 91
e-mail: sekretariat@tcuw.torun.pl, www.tcuw.torun.pl

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)

Rodzaj zamówienia: Usługi

w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji o wartości zamówienia nieprzekraczającej progów unijnych, o których mowa w art. 3 ust. 1 pkt 1 Ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz. U. z 2026 r. poz. 793 ze zm.) – dalej określanej w niniejszej SWZ jako Ustawa

„Zapewnienie dla TCUW infrastruktury teleinformatycznej o wysokiej dostępności w modelu chmury obliczeniowej wraz z usługami towarzyszącymi.”

nr sprawy: 45/2026

Specyfikacja niniejsza zawiera 84 strony.

Zatwierdził: Dyrektor TCUW – Łukasz Nowak

Łukasz Nowak

Elektronicznie podpisany przez Łukasz Nowak
Data: 2026.11.05 14:36:53 +01'00'

Toruń, dnia 05.11.2026 r.

Część I - Postanowienia ogólne

1. Informacja o Zamawiającym

Zamawiającym jest: Gmina Miasta Toruń
działająca poprzez **Toruńskie Centrum Usług Wspólnych w Toruniu**
Adres: 87-100 Toruń, plac Św. Katarzyny 9,
tel.: (56) 611 89 91
Adres strony internetowej Zamawiającego: https://tcuw.torun.pl/bip.html
NIP: 8792688682, REGON: 366286234

Osobą uprawnioną do kontaktów z Wykonawcami jest: Magdalena Lorenc
adres poczty elektronicznej: przetargi@tcuw.torun.pl
tel.: 730013409

Niniejsze zamówienie dotyczy wyboru Wykonawcy na dostarczenie, wdrożenie, utrzymanie i administrowanie środowiskiem chmury obliczeniowej IaaS wraz z usługami towarzyszącymi tj. usługą bezpieczeństwa, kopiami zapasowymi, przestrzenią WORM, usługami Microsoft 365 oraz dodatkowym wsparciem IT dla TCUW.

Wartość zamówienia jest niższa aniżeli wartość progów unijnych, o których mowa w art. 3 ust. 1 pkt 1 Ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz. U. z 2026 r. poz.793), a większa aniżeli 170 000,00 złotych.

2. Tryb udzielenia zamówienia - podstawa prawna

1) Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 1 Ustawy.
2) Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3) Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych o jakich mowa w art. 3 ust. 1 pkt 1 Ustawy.
4) Zamawiający nie przewiduje złożenia oferty w postaci katalogów elektronicznych.
5) Postępowanie jest prowadzone na stronie internetowej prowadzonego postępowania https://tcuw.ezamawiajacy.pl, bezpośredni link do postępowania: https://tcuw.ezamawiajacy.pl/pn/TCUW/demand/334443/notice/public/details
6) SWZ dostępna jest na stronie internetowej prowadzonego postępowania, stronie internetowej Zamawiającego www.tcuw.torun.pl w Biuletynie Zamówień Publicznych od dnia publikacji ogłoszenia do zakończenia postępowania (nie krócej niż do dnia udzielenia zamówienia).
7) Językiem postępowania o udzielenie zamówienia jest język polski. Cała korespondencja wymieniana pomiędzy Wykonawcami, a Zamawiającym prowadzona będzie w języku polskim.

3. Wykonawcy

1) O udzielenie zamówienia mogą się ubiegać Wykonawcy będący osobami fizycznymi, osobami prawnymi lub jednostkami organizacyjnymi nie posiadającymi osobowości prawnej, a także Wykonawcy ci występujący wspólnie (np.: spółka cywilna, konsorcjum), o ile spełniają warunki określone w Ustawie oraz w niniejszej SWZ.
2) Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 Ustawy, tj. mających status zakładu pracy chronionej, spółdzielnie socjalne oraz innych Wykonawców, których głównym celem lub głównym celem działalności ich wyodrębnionych organizacyjnie jednostek, które będą realizowały zamówienie, jest społeczna i zawodowa integracja osób społecznie marginalizowanych.
3) Zamówienie może zostać udzielone Wykonawcy, który:
   a) nie podlega wykluczeniu na podstawie art. 108 ust. 1 Ustawy
   b) nie podlega wykluczeniu na podstawie art.109 ust 1 pkt 4) Ustawy
   c) spełnia warunki udziału w postępowaniu określone w pkt 14 SWZ
   d) złożył ofertę niepodlegającą odrzuceniu na podstawie art. 226 ust. 1 Ustawy
   e) nie podlega wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2025 r. poz. 514 z późn. zm.).

4. Podwykonawcy

1) Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.
2) Jeśli wykonanie zamówienia zostanie powierzone podwykonawcom Wykonawca w swojej ofercie jest zobowiązany wskazać wykonanie której części zamówienia zamierza powierzyć podwykonawcom, wraz z podaniem nazwy (firmy) podwykonawców.
3) Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 ust. 1 Ustawy, w celu wykazania spełniania warunków udziału w postępowaniu Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Zamawiający powoływał się w trakcie postępowania o udzielenie zamówienia.

5. Oferty wariantowe i częściowe, umowy ramowe i aukcje elektroniczne

1) Zamawiający nie dopuszcza składania ofert wariantowych.
2) Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
3) Zamawiający nie przewiduje aukcji elektronicznej.
4) Zamawiający nie dopuszcza składania ofert częściowych.
5) Wykonawca może złożyć tylko jedną ofertę. Oferty nie zawierające pełnego zakresu przedmiotu zamówienia zostaną odrzucone.
6) W przypadku, gdy nie zostanie złożona co najmniej jedna oferta niepodlegająca odrzuceniu,

postępowanie zostanie unieważnione

7) Uzasadnienie braku podziału postępowania na części:

Zamawiający nie dopuszcza składania ofert częściowych. Podział zamówienia na części nie jest uzasadniony z przyczyn technicznych, organizacyjnych oraz funkcjonalnych.

Przedmiot zamówienia obejmuje kompleksowe świadczenie zintegrowanych usług informatycznych, składających się z infrastruktury chmurowej IaaS, usług administracyjnych, bezpieczeństwa teleinformatycznego, kopii zapasowych, usług Microsoft 365, systemów zarządzania tożsamością i dostępem (Active Directory, MFA), usług VPN, ochrony stacji roboczych i serwerów, przestrzeni WORM oraz całodobowego monitoringu i wsparcia technicznego. Poszczególne elementy zamówienia są ze sobą technologicznie powiązane i tworzą jedno spójne środowisko teleinformatyczne.

Podział zamówienia na części skutkowałby koniecznością współpracy wielu wykonawców odpowiedzialnych za różne elementy infrastruktury, co istotnie zwiększałoby ryzyko wystąpienia problemów integracyjnych, trudności w ustalaniu odpowiedzialności za awarie oraz wydłużenia czasu reakcji na incydenty i usuwania usterek. W przypadku środowiska objętego wymaganiami wysokiej dostępności (HA), ciągłego monitorowania, ochrony bezpieczeństwa oraz rygorystycznych parametrów SLA, niezbędne jest zapewnienie jednolitego modelu zarządzania, utrzymania i odpowiedzialności za całość świadczonych usług.
Realizacja zamówienia przez jednego wykonawcę gwarantuje pełną kompatybilność wszystkich komponentów rozwiązania, zachowanie wymaganych parametrów bezpieczeństwa, spójność procesów administracyjnych oraz efektywne zarządzanie usługami świadczonymi w modelu 24/7/365. Pozwala również na skuteczne egzekwowanie wymaganych poziomów SLA, RPO i RTO oraz zapewnia jednego wykonawcę odpowiedzialnego za prawidłowe funkcjonowanie całego środowiska.

6. Zamówienia, o których mowa w art. 214 ust. 1 i 8 Ustawy

Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 8 Ustawy w zw. z art. 305 pkt 1 Ustawy.

7. Dopuszczalność rozwiązań równoważnych do wskazywanych przez Zamawiającego

Wszelkie użyte w niniejszej SWZ i załącznikach do niej 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 SWZ i załącznikach do niej, stanowią jedynie przykłady zastosowań lub wymagań i należy rozumieć je każdorazowo jak opatrzone dopiskiem „lub równoważne”.
Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego.

Wykonawca może zaproponować taki produkt, który będzie spełniać wszystkie wymagane parametry określone przez Zamawiającego w Opisie Przedmiotu Zamówienia (OPZ). Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego zobowiązany jest wykazać na etapie składania oferty, że oferowany produkt spełnia wymagania postawione przez Zamawiającego.
Licencje równoważne muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. W przypadku wątpliwości dotyczących równoważności oferowanego rozwiązania równoważnego Zamawiający wezwie Wykonawcę do złożenia we wskazanym terminie wyjaśnień dotyczących treści oferty. Ciężar udowodnienia równoważności spoczywa na Wykonawcy. Ocena równoważności zaoferowanych licencji zostanie dokonana w oparciu o wymagania określone przez Zamawiającego w OPZ oraz złożone przez Wykonawcę dowody dla potwierdzenia równoważności. Ponadto, w takiej sytuacji Wykonawca zobowiązany jest w ofercie podać nazwę, producenta, model lub symbol lub numer katalogowy lub wersję oprogramowania równoważnego identyfikującego jednoznacznie oferowane oprogramowanie.
W każdym miejscu OPZ, w którym użyto znaku towarowego, nazwy lub pochodzenia, Zamawiający dopuszcza zaoferowanie przez Wykonawcę rozwiązań równoważnych. Za równoważny przedmiot zamówienia Zamawiający uzna produkt o cechach (parametrach) zgodnych lub lepszych niż produkt określony w OPZ. Wykonawca powołujący się na rozwiązania równoważne musi wykazać, że spełniają one warunki określone w OPZ. W celu wykazania Wykonawca jest zobligowany podać nazwę produktów równoważnych, a także przeprowadzić dowód równoważności poprzez opis porównawczy parametrów produktów wyspecyfikowanych przez Zamawiającego w OPZ z parametrami produktów oferowanych jako równoważne. Wykonawca w celu udowodnienia, że oferuje rozwiązania równoważne ma również obowiązek wykazać w jaki sposób oferowany model licencyjny jest równoważny z modelem licencyjnym wyspecyfikowanym przez Zamawiającego w OPZ. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w pierwotnej dokumentacji ani do zmiany ceny, ani do naruszenia przepisów prawa.

8. Wizja lokalna

Zamawiający nie przewiduje obowiązku odbycia przez Wykonawcę wizji lokalnej lub sprawdzenia przez Wykonawcę dokumentów niezbędnych do realizacji zamówienia**.**

9. Projektowane postanowienia umowy

1) Zamawiający zawrze umowę w sprawie przedmiotowego zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią załącznik nr 4 do SWZ.

10. Użyte skróty

1) **Ustawa** - Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2026 r.

poz. 793 z późn. zm.)

2) **Rozporządzenie** - Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz.U. z 2020 r. poz. 2415).
3) **Platforma** - platforma zakupowa prowadzona przez Marketplanet OnePlace, za pośrednictwem której Zamawiający prowadzi postępowanie o udzielenie zamówienia. Wejście na platformę następuje przez link: https://tcuw.ezamawiajacy.pl.
4) **KSC** – ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (tj. Dz. U. 2026 poz. 252).
5) **Ustawa o certyfikacji** – Ustawa z dnia 5 sierpnia 2025 r. o certyfikacji wykonawców zamówień publicznych (Dz.U. poz. 1235 ze zm.).

Część II - Przedmiot zamówienia i termin jego realizacji

11. Przedmiot zamówienia

1) Opis przedmiotu zamówienia:
realizacja kompleksowej usługi, polegającej na dostarczeniu, skonfigurowaniu, wdrożeniu, utrzymaniu i administracji środowiskiem chmury obliczeniowej IaaS wraz z usługami towarzyszącymi tj. usługą bezpieczeństwa, kopiami zapasowymi, przestrzenią WORM, usługami Microsoft 365 oraz dodatkowym wsparciem IT.
Wykonawca będzie oferował usługę w oparciu o infrastrukturę technologiczną ośrodka centrum przetwarzania danych zlokalizowanego na terytorium Unii Europejskiej lub Lichtensteinu, Islandii, Norwegii. Dane, kopie zapasowe oraz pozostałe zasoby objęte usługą muszą być przechowywane i przetwarzane wyłącznie na terytorium państwa członkowskiego Unii Europejskiej lub państwa należącego do Europejskiego Obszaru Gospodarczego (EOG). Centrum danych musi spełniać wymagania wysokiej dostępności, bezpieczeństwa i ochrony danych adekwatne do charakteru świadczonych usług.
Ponadto Wykonawca musi zapewnić łącza do sieci Internet, infrastrukturę teletechniczną wraz z niezbędnymi urządzeniami, oprogramowaniem i licencjami potrzebnymi do prawidłowego uruchomienia i działania usługi. Wykonawca musi zapewnić wsparcie usługi w trybie 24/7/365.
2) Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1 do niniejszego SWZ.

3) **Nazwa i kod określony we Wspólnym Słowniku Zamówień**:
48800000-6 - Systemy i serwery operacyjne,
72415000-2 - Usługi hostingowe dla stron WWW

4) Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:
a) produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art.

33 ust. 4 KSC, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;

b) produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 KSC, ani usług ICT lub procesów ICT określonych w tej decyzji.

Niespełnienie powyższego wymagania skutkuje odrzuceniem oferty odpowiednio na podstawie art. 226 ust. 1 pkt 17 albo pkt 19 Ustawy.

Wykonawca jest zobowiązany do realizacji zamówienia przy użyciu produktów ICT, usług ICT oraz procesów ICT odpowiadających treści oferty, dokumentom zamówienia oraz postanowieniom umowy. Zastąpienie w toku realizacji umowy producenta, dostawcy technologii, modelu, wersji, środowiska świadczenia usługi albo procesu ICT może nastąpić wyłącznie w przypadkach prawnie dopuszczalnych oraz z zachowaniem wymagań wynikających z art. 454 i art. 455 Ustawy, a także zgodnie z postanowieniami umowy określającymi dopuszczalne podstawy i warunki zmiany.

12. Termin i miejsce realizacji zamówienia

Termin realizacji zamówienia: Usługa musi być skonfigurowana, uruchomiona i dostępna od **1.01.2027 r. do 31.12.2028 r**.

Miejsce realizacji zamówienia: Usługa będzie świadczona z wykorzystaniem infrastruktury centrum przetwarzania danych Wykonawcy zlokalizowanej na terytorium państw UE lub EOG. Odbiorcą usługi oraz miejscem korzystania z niej jest Toruńskie Centrum Usług Wspólnych, pl. Św. Katarzyny 9, 87-100 Toruń.

Część III - Warunki udziału w postępowaniu i podstawy wykluczenia Wykonawcy

13. Podstawy wykluczenia z postępowania

1) O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu, o którym mowa w art. 108 ust. 1 Ustawy. Z postępowania o udzielenie zamówienia wyklucza się wykonawcę:

a) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

- udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
- handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
- o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2026 r. poz. 95 i 615) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2026 r. poz. 253 i 791),
- finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

- o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
- powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 1567),
- przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
-o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej - lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

b) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

c) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

d) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

e) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności, jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

f) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

2) Zamawiający przewiduje wykluczenie Wykonawcy w następujących spośród przypadków, o których mowa w art. 109 ust. 1 Ustawy:

a) w stosunku, do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.

3) Z udziału w postępowaniu Zamawiający wyklucza Wykonawcę, do którego stosuje się przepis

art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2025 r. poz. 514 ze zm.), tj. wykonawcę:

a) wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącym środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006 ze zm., dalej rozporządzenie 765/2006) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014 ze zm., dalej rozporządzenie 269/2014) albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy;

b) którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644 ze zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww. ustawy;

c) którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2026 r. poz. 522, 640 i 644) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ww. ustawy.

3) Wykluczenie Wykonawcy następuje zgodnie z art. 111 Ustawy.

4) Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2, 5 lub art.109 ust.1 pkt 4, jeżeli udowodni Zamawiającemu, że spełnił łącznie przesłanki określone w art. 110 ust. 2 Ustawy.

5) Zamawiający oceni, czy podjęte przez Wykonawcę czynności są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, a jeżeli uzna, że nie są wystarczające, wykluczy Wykonawcę.

6) Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

14. Warunki udziału w postępowaniu

1) Zamawiający nie stawia warunku dotyczącego zdolności do występowania w obrocie gospodarczym.

2) Zamawiający wymaga spełnienia następującego warunku dotyczącego uprawień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:

WARUNEK: Wykonawca musi być zarejestrowanym operatorem telekomunikacyjnym. Spełnienie warunku zostanie ocenione na podstawie przedłożonego zaświadczenia o wpisie do rejestru przedsiębiorców telekomunikacyjnych.

3) Zamawiający wymaga spełnienia następującego warunku dotyczącego sytuacji ekonomicznej i finansowej Wykonawcy.

WARUNEK: Wykonawca musi posiadać ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia, którego suma gwarancyjna wynosi co najmniej 5 000 000 PLN. Wykonawca jest zobowiązany zapewnić trwałość ubezpieczenia przez cały okres związania umową. Jeżeli suma gwarancyjna została określona w walucie innej niż PLN, Zamawiający dokona jej przeliczenia według średniego kursu NBP z dnia publikacji ogłoszenia o zamówieniu.

4) Zamawiający wymaga spełnienia następującego warunku dotyczącego zdolności technicznej lub zawodowej:

WARUNEK:
Wykonawca musi posiadać wdrożone i potwierdzone aktualnymi certyfikatami wydanymi przez niezależną akredytowaną jednostkę certyfikującą:
a) normę ISO 22301 na usługi IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowej (backupu)
b) normę ISO 27001 na usługi IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowej (backupu)
c) normę ISO 27017 na usługi IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowej (backupu)
d) normę ISO 9001 na usługi IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowej (backupu).

Wymóg ten został określony w celu zapewnienia najwyższego poziomu bezpieczeństwa informacji oraz ciągłości działania usług, zgodnie z zgodnie z celami określonymi w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2) oraz międzynarodowymi standardami branżowymi. Posiadanie certyfikowanych systemów zarządzania potwierdza stosowanie przez Wykonawcę ustandaryzowanych procedur oraz najlepszych praktyk w zakresie bezpieczeństwa informacji, ciągłości działania i jakości świadczonych usług.
Zamawiający dopuszcza zaświadczenia wydane przez jednostki oceniające zgodność mające siedzibę w innych państwach członkowskich Unii Europejskiej oraz równoważne środki potwierdzające stosowanie równoważnych środków zarządzania jakością, bezpieczeństwem informacji i ciągłością działania, jeżeli Wykonawca nie ma możliwości uzyskania wymaganych certyfikatów z przyczyn od niego niezależnych. Zamawiający zastrzega sobie prawo do weryfikacji przedstawionych dokumentów i żądania dodatkowych wyjaśnień lub dowodów równoważności.

5) Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania

o udzielenie zamówienia.

6) Zamawiający przewiduje wykluczenie podmiotów udostępniających zasoby w trybie art. 118 Ustawy i podwykonawców z tych samych przyczyn, co Wykonawcy.
7) Zamawiający określając warunki udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt 4 Ustawy nie odnosi się do poziomów zdolności, o których mowa w art. 5 Ustawy o certyfikacji, ponieważ przepisy wykonawcze, o których mowa w art. 5 ust. 4 i 5 Ustawy o certyfikacji określające poziomy zdolności, nie zostały wydane.

15. Wykonawcy występujący wspólnie

1) Wykonawcy mogą ubiegać się wspólnie o udzielenie zamówienia.
2) W przypadku złożenia wspólnej oferty przez oddzielne podmioty, współubiegający się o udzielenie zamówienia winni ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia.
3) Żaden z Wykonawców wspólnie ubiegających się o niniejsze zamówienie nie może podlegać wykluczeniu na podstawie art. 108 ust. 1 Ustawy w zw. z pkt. 13 ppkt 1) niniejszej SWZ oraz art. 109 ust. 1 pkt. 4 w zw. z pkt 13 ppkt 2) SWZ oraz art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2025 r. poz. 514 ze zm.) w zw. pkt. 13 ppkt. 3) niniejszej SWZ.
4) Wszelka korespondencja prowadzona będzie wyłącznie z pełnomocnikiem.
5) Wykonawcy wspólnie ubiegający się o niniejsze zamówienie, których oferta zostanie uznana za najkorzystniejszą, przed podpisaniem umowy o realizację zamówienia, są zobowiązani przedstawić Zamawiającemu stosowne pisemne porozumienie (umowę) zawierające w swojej treści uregulowanie współpracy tych Wykonawców na potrzeby niniejszego postępowania.
6) W przypadku oferty składanej przez podmioty prowadzące działalność w formie spółki cywilnej, Wykonawcami w rozumieniu Ustawy są wszyscy wspólnicy tej spółki i są traktowani jako Wykonawcy wspólnie ubiegający się o udzielenie zamówienia.
7) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia warunki udziału w postępowaniu będą oceniane zgodnie z art. 117 ustawy Prawo zamówień publicznych.
   a) W odniesieniu do warunku dotyczącego uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, Zamawiający uzna warunek za spełniony, jeżeli co najmniej jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia posiada wymagane uprawnienia i zrealizuje usługi, do których wykonania uprawnienia te są wymagane.
   b) W odniesieniu do warunków dotyczących sytuacji ekonomicznej lub finansowej warunek zostanie uznany za spełniony, jeżeli wykonawcy wykażą, że co najmniej jeden z wykonawców realizujący usługi IaaS lub usługi kopii zapasowych objęte przedmiotem zamówienia posiada ubezpieczenie OC w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną nie mniejszą niż 5 000 000 zł.

c) W odniesieniu do warunku posiadania certyfikatów ISO 22301, ISO 27001, ISO 27017 oraz ISO 9001, wymagane certyfikaty musi posiadać ten Wykonawca lub ci Wykonawcy, którzy będą realizować usługi chmury obliczeniowej (IaaS), WORM oraz usługi wykonywania, przechowywania i odtwarzania kopii zapasowych objęte zakresem tych certyfikatów.

8) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączą do oferty oświadczenie, z którego będzie wynikało, które usługi wykonają poszczególni Wykonawcy, zgodnie z art. 117 ust. 4 ustawy Prawo zamówień publicznych.

16. Udostępnianie zasobów.

1) Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2) Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Zobowiązanie podmiotu udostępniającego zasoby potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
a) zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
b) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
3) W przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, Wykonawca wraz z oświadczeniem, o którym mowa w pkt 17 ppkt 1) lit. a SWZ, przedstawia oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby, zgodnie z art. 125 ust. 5 Ustawy;
4) Zamawiający żąda od Wykonawcy, który polega na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby na zasadach określonych w art. 118 Ustawy, przedstawienia podmiotowych środków dowodowych, o których mowa w pkt 19 ppkt 1 SWZ dotyczących tych podmiotów, potwierdzających, że nie zachodzą wobec nich podstawy wykluczenia z postępowania.

Część IV - Oświadczenia i dokumenty wymagane od Wykonawcy

17. Dokumenty i oświadczenia składane wraz z ofertą

1) Oświadczenia i dokumenty dołączane do składanej oferty:
a) oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu, w zakresie wskazanym przez Zamawiającego, o którym mowa w art. 125 ust. 1

Ustawy, stanowiące dowód potwierdzający brak podstaw wykluczenia i spełnianie warunków udziału w postępowaniu na dzień składania ofert, tymczasowo zastępujący wymagane przez Zamawiającego podmiotowe środki dowodowe. Wzór oświadczenia stanowi załącznik nr 3 do SWZ;

b) W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie, o którym mowa powyżej, składa każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu;

c) Wykonawca, który polega na zdolnościach podmiotów udostępniających zasoby składa wraz z ofertą dokumenty i oświadczenia, o których mowa w pkt 16 ppkt 2 i 3 SWZ;

d) Pełnomocnictwo lub dokumenty, z których wynika prawo do podpisania oferty w przypadku, gdy oferta została podpisana przez inną osobę niż umocowana w dokumencie rejestrowym Wykonawcy;

e) W przypadku gdy oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa – dowody, o których mowa w pkt 26 SWZ;

f) Wykaz rozwiązań równoważnych z jego opisem lub normami w przypadku, gdy Wykonawca powołuje się na rozwiązania równoważne, aby wykazać, że oferowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego.

2) Jeżeli wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 Ustawy, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że oferta wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub zachodzą przesłanki unieważnienia postępowania.

3) W zakresie nieuregulowanym SWZ, zastosowanie mają przepisy Rozporządzenia.

4) Dokumenty lub oświadczenia, o których mowa w Rozporządzeniu i niniejszej SWZ, składa się zgodnie

18. Certyfikat wykonawcy zamówień publicznych.

1) Wykonawca może, zamiast odpowiednich podmiotowych środków dowodowych wymaganych przez Zamawiającego w niniejszym postępowaniu, posłużyć się certyfikatem wykonawcy zamówień publicznych, jeżeli certyfikat ten potwierdza okoliczności wymagane przez Zamawiającego w zakresie braku podstaw wykluczenia lub spełniania warunków udziału w postępowaniu.
2) Wykonawca może, zamiast odpowiednich podmiotowych środków dowodowych wymaganych na potwierdzenie braku podstaw wykluczenia lub spełniania warunków udziału w postępowaniu, złożyć certyfikat potwierdzający udzielenie certyfikacji wykonawcy zamówień publicznych, o którym mowa w art. 124 ust. 2 Ustawy, potwierdzający udzielenie certyfikacji odpowiednio w zakresie niepodlegania wykluczeniu lub zdolności wykonawcy do należytego wykonania zamówienia. W przypadku posługiwania się certyfikatem, o którym mowa w zdaniu poprzedzającym, wykonawca wskazuje w oświadczeniu, o którym mowa w

art. 125 ust. 1 Ustawy, że będzie posługiwał się certyfikatem oraz podaje:
   a) numer i oznaczenie certyfikatu,
   b) nazwę podmiotu certyfikującego,
   c) okres ważności certyfikacji oraz
   d) zakres, w jakim certyfikat ma potwierdzać brak podstaw wykluczenia lub spełnianie warunków udziału w postępowaniu.

3) Certyfikat zastępuje odpowiednie podmiotowe środki dowodowe wyłącznie w zakresie, w jakim z jego treści wynika potwierdzenie braku podstaw wykluczenia lub spełniania warunków udziału w postępowaniu określonych w niniejszej SWZ. Jeżeli certyfikat obejmuje wyłącznie część podstaw wykluczenia lub część warunków udziału w postępowaniu, wykonawca jest obowiązany wykazać pozostały zakres zgodnie z wymaganiami określonymi w SWZ.
4) Zamawiający dokonuje oceny skuteczności certyfikatu z uwzględnieniem zakresu certyfikacji, okresu jej ważności, statusu certyfikacji ujawnionego w bazie certyfikacji oraz zgodności certyfikatu z wymaganiami określonymi w niniejszej SWZ. W przypadku zawieszenia ważności certyfikacji albo utraty ważności certyfikatu w toku postępowania o udzielenie zamówienia zamawiający wzywa wykonawcę do złożenia, w wyznaczonym terminie, podmiotowych środków dowodowych w zakresie, w jakim certyfikat miał potwierdzać brak podstaw wykluczenia lub spełnianie warunków udziału w postępowaniu.
5) Złożenie certyfikatu nie wyłącza uprawnienia zamawiającego do żądania wyjaśnień.
6) W przypadkach przewidzianych przepisami Ustawy oraz Ustawy o certyfikacji, w szczególności w razie powzięcia uzasadnionych wątpliwości co do zakresu certyfikacji, jej aktualności albo zgodności certyfikatu z wymaganiami niniejszego postępowania.

19. Dokumenty składane na wezwanie

1) Zgodnie z art. 274 ust. 1 Ustawy, Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych wskazanych w pkt 2)-5).
2) W celu wykazania braku podstaw do wykluczenia z postępowania z przyczyn, o których mowa w art. 108 ust. 1 Ustawy Zamawiający wezwie do przedłożenia dotyczących odpowiednio Wykonawcy, Wykonawców ubiegających się o wspólne udzielenie zamówienia, podmiotu, o którym mowa w art. 118 Ustawy, na zdolnościach lub sytuacji którego polega Wykonawca, lub podwykonawcy, nie będącego podmiotem, o którym mowa w art. 118 Ustawy:
   a) informacji z Krajowego Rejestru Karnego w zakresie:
      - art. 108 ust. 1 pkt 1 i 2 Ustawy
      - art. 108 ust. 1 pkt 4 Ustawy, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,

   -sporządzonej niewcześniej niż 6 miesięcy przed jej złożeniem;
   b) oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 Ustawy o braku przynależności do tej samej grupy kapitałowej w rozumieniu Ustawy z dnia 16 lutego

2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2025 r. poz. 1714), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej;

c) oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 Ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez Zamawiającego, o których mowa w:
- art. 108 ust. 1 pkt 3 Ustawy,
- art. 108 ust. 1 pkt 4 Ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
- art. 108 ust. 1 pkt 5 Ustawy, dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
- art. 108 ust. 1 pkt 6 Ustawy,
- oraz art. 109 ust. 1 pkt 4 Ustawy.

d) odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 Ustawy w zw. z pkt. 13 pkkt. 2) niniejszej SWZ, sporządzonych niewcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

Zamawiający nie wezwie do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w jednolitym dokumencie dane umożliwiające dostęp do tych środków.

3) W celu potwierdzenia spełnienia przez Wykonawcę warunku dotyczącego uprawień do prowadzenia określonej działalności gospodarczej lub zawodowej, Zamawiający wezwie do przedłożenia zaświadczenia o wpisie do rejestru przedsiębiorców telekomunikacyjnych prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej.
W przypadku Wykonawców mających siedzibę poza terytorium Rzeczypospolitej Polskiej, Zamawiający uzna za równoważne dokumenty wydane w kraju siedziby Wykonawcy, potwierdzające posiadanie uprawnień do wykonywania działalności odpowiadającej działalności telekomunikacyjnej objętej przedmiotem zamówienia.

4) W celu potwierdzenia spełniania warunku udziału w postępowaniu dotyczącego sytuacji ekonomicznej lub finansowej Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia dokumentu potwierdzającego, że Wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną nie mniejszą niż 5 000 000,00 zł.
W celu potwierdzenia spełniania warunku udziału w postępowaniu dotyczącego zdolności technicznej lub zawodowej Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia następujących dokumentów:

a) Aktualnego certyfikatu ISO 22301, wydanego przez niezależną akredytowaną

jednostkę certyfikującą, potwierdzającego wdrożenie i stosowanie systemu zarządzania ciągłością działania w zakresie usług IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowych (backupu).

b) Aktualnego certyfikatu ISO 27001, wydanego przez niezależną akredytowaną jednostkę certyfikującą, potwierdzającego wdrożenie i stosowanie systemu zarządzania bezpieczeństwem informacji w zakresie usług IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowych (backupu).

c) Aktualnego certyfikatu ISO 27017, wydanego przez niezależną akredytowaną jednostkę certyfikującą, potwierdzającego stosowanie dobrych praktyk bezpieczeństwa dla usług chmury obliczeniowej w zakresie usług IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowych (backupu).

d) Aktualnego certyfikatu ISO 9001, wydanego przez niezależną akredytowaną jednostkę certyfikującą, potwierdzającego wdrożenie i stosowanie systemu zarządzania jakością w zakresie usług IaaS (cloud) oraz wykonywania i przechowywania kopii zapasowych (backupu).

e) W przypadku powoływania się na rozwiązania równoważne, dokumentów potwierdzających, że stosowane przez Wykonawcę środki zapewniają poziom bezpieczeństwa, ciągłości działania i jakości nie niższy niż wynikający odpowiednio z norm ISO 22301, ISO 27001, ISO 27017 oraz ISO 9001.

20. Zagraniczne dokumenty i oświadczenia potwierdzające brak podstaw wykluczenia

1) W przypadku gdy Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami RP zamiast:

a) informacji z Krajowego Rejestru Karnego, o której mowa w części IV pkt 19 ppkt 2) lit. a) SWZ - składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w części IV pkt 19 ppkt 2) lit. a) SWZ, wystawione nie wcześniej niż 6 miesięcy przed ich złożeniem.

b) informacji, której mowa w części IV pkt. 19 ppkt. 2) lit. d - składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, niewcześniej niż 3 miesiące przed ich złożeniem, potwierdzające odpowiednio, że:

- nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.

2) Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 20 ppkt 1) powyżej, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4 zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o

oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy , wystawionym w terminach nie wcześniejszych, niż wskazane w pkt. 1) lit a) lub b) powyżej.

3) Postanowienia niniejszego pkt 20 stosuje się odpowiednio do podmiotów udostępniających zasoby Wykonawcy, mających siedzibę lub miejsce zamieszkania poza terytorium RP.

21. Informacja o przedmiotowych środkach dowodowych

1. W przypadku, w którym z pkt. 2 poniżej wynika żądanie przez Zamawiającego przedmiotowych środków dowodowych:

1) **przedmiotowe środki dowodowe podlegają przedłożeniu wraz z ofertą**.

2) **W przypadku niezłożenia przedmiotowych środków dowodowych wraz z ofertą, Zamawiający nie przewiduje wezwania do złożenia lub uzupełnienia przedmiotowych środków dowodowych.**

2. Zamawiający żąda przedłożenia wraz z ofertą następujących przedmiotowych środków dowodowych na potwierdzenie, że oferowane usługi spełniają określone przez Zamawiającego wymagania, cechy lub kryteria (w tym kryteria oceny ofert):

1) W zakresie etykiet, o których mowa w art. 104 Ustawy, na potwierdzenie spełniania wymaganych cech środowiskowych, społecznych lub innych:

Zamawiający nie żąda przedłożenia etykiet, o których mowa w art. 104 Ustawy

2) w zakresie certyfikatów, o których mowa w art. 105 Ustawy, w celu potwierdzenia zgodności oferowanych usług z wymaganiami, cechami lub kryteriami określonymi w opisie przedmiotu zamówienia lub kryteriami oceny ofert, lub wymaganiami związanymi z realizacją zamówienia zamawiający żąda od Wykonawcy przedłożenia:

1) kopi aktualnego certyfikatu ANSI/TIA-942 Rated 3;

2) kopi aktualnego certyfikatu Tier III Facility;

3) oświadczenia, że usługi objęte zamówieniem będą świadczone z centrum danych posiadającego wskazane certyfikaty.

Zamawiający informuje, że dokumenty wskazane powyżej stanowią środki dowodowe służące ocenie ofert w ramach kryteriów oceny ofert. W przypadku niezłożenia wraz z ofertą dokumentów, o których mowa w pkt 1-3, albo złożenia dokumentów niepotwierdzających spełniania wymagań określonych przez Zamawiającego, Zamawiający nie będzie wzywał Wykonawcy do ich złożenia, uzupełnienia ani poprawienia. W takim przypadku oferta otrzyma 0 punktów w kryterium oceny ofert, którego dokumenty te dotyczą.

Powyższe nie dotyczy sytuacji, w której dokument został złożony wraz z ofertą, lecz zawiera omyłki lub budzi wątpliwości wymagające wyjaśnienia, o ile wezwanie do wyjaśnień nie prowadziłoby do niedozwolonej zmiany treści oferty ani uzupełnienia brakującego środka dowodowego.

3) w zakresie pozostałych przedmiotowych środków dowodowych (art. 106 ustawy)

W celu potwierdzenia, że oferowane usługi odpowiadają wymaganiom określonym przez

Zamawiającego, Zamawiający żąda od Wykonawcy przedłożenia Specyfikacji technicznej ośrodka centrum przetwarzania danych (Załącznik nr 2 do SWZ), z której wynikać będzie spełnianie wymagań opisanych w niniejszej SWZ i załącznikach do niej.

Część V - Wymagania dotyczące wadium

22. Wysokość wadium

Wykonawca nie przewiduje obowiązku wpłacenia wadium.

Część VI - Sposób obliczenia ceny oferty

23. Sposób obliczenia ceny oferty

1) Formą wynagrodzenia za przedmiot zamówienia zgodnie z projektowanymi postanowieniami umowy jest wynagrodzenie na podstawie ceny ryczałtowej uwzględniające podatek VAT. Dla oceny ofert należy ustalić cenę ofertową jako maksymalne wynagrodzenie za realizację przedmiotu zamówienia.
2) Podana w ofercie cena musi być wyrażona w złotych polskich [PLN]. Cena musi uwzględniać wszystkie wymagania niniejszej SWZ oraz obejmować wszelkie koszty (w tym należności publicznoprawne) jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.
3) Sposób zapłaty i rozliczenia za realizację niniejszego zamówienia, określone zostały projektowanych postanowieniach umowy, stanowiących załącznik nr 4 do niniejszej SWZ.
4) Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
5) Wykonawca, który ma siedzibę lub miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, poda cenę netto oraz brutto (zawierającą VAT).
6) W przypadku Wykonawcy, który nie podlega obowiązkowi podatkowemu w zakresie VAT na terenie Rzeczypospolitej Polskiej i podał cenę netto (bez VAT), jeżeli wybór jego oferty prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z Ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2026 r. poz. 1263 ze zm.), dla celów zastosowania kryterium ceny lub Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. Taki Wykonawca ma obowiązek w ofercie:
    a) poinformować Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
    b) wskazać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
    c) wskazać wartość towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
    d) wskazać stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

24. Cena ofertowa

1) Cena ofertowa podana przez Wykonawcę w Formularzu Ofertowym nie będzie podlegała zmianom. Stawka podatku VAT jest określana zgodnie z Ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2026 r. poz. 1263 ze zm.).
2) Cena obejmuje wartość przedmiotu zamówienia, podatek VAT.
3) Nie należy stosować żadnych upustów.
4) Wszystkie wartości powinny być liczone w walucie polskiej, w tym ceny jednostkowe powinny być liczone z dokładnością do dwóch miejsc po przecinku w rozumieniu Ustawy z dnia 9 marca 2014 r. o informowaniu o cenach towarów i usług (Dz. U. z 2023 poz. 168 z późn. zm.) oraz Ustawy z dnia 7 lipca 1994 r. o denominacji złotego (Dz. U. z 1994 r. Nr 84, poz. 386 z późn. zm.).

Część VII - Opis sposobu przygotowywania ofert;

Uwaga! Zamawiający rekomenduje, aby Wykonawca, przed przystąpieniem do składania ofert w systemie, zapoznał się z Instrukcją korzystania z systemu, która dostępna jest w sekcji „Baza Wiedzy” oraz zasadami rejestracji w systemie, o których mowa w regulaminie dostępnym pod adresem https://oneplace.marketplanet.pl/regulamin.

25. Sposób przygotowania i składania oferty.

1) Ofertę składa się w postaci elektronicznej za pomocą Platformy pod adresem https://tcuw.ezamawiajacy.pl w terminie wskazanym w SWZ.
2) Złożenie oferty odbywa się poprzez wypełnienie zdefiniowanych przez Zamawiającego na Platformie dokumentów:
a) Formularza oferty – zakres danych wypełnianych przez Wykonawcę został określony w zakładce „Oferta” oraz podpisanie ich kwalifikowanym podpisem elektronicznym, podpisem osobistym lub podpisem zaufanym osoby/osób upoważnionej/ upoważnionych do reprezentowania Wykonawcy zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.
b) Załączenie do oferty oświadczeń i dokumentów, o których mowa w pkt 17 SWZ.
3) Ofertę, oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu, podmiotowe środki dowodowe, zobowiązanie podmiotu udostępniającego zasoby, wykaz rozwiązań równoważnych oraz pełnomocnictwo, przekazuje się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, tj. rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, opatrzonej kwalifikowanym podpisem elektronicznym lub elektronicznym podpisem zaufanym lub elektronicznym podpisem osobistym.
4) W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio

Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby, zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby, zwane dalej „upoważnionymi podmiotami", jako dokument elektroniczny, Wykonawca przekazuje ten dokument.
5) W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
6) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt powyżej, dokonuje w przypadku:
a) podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania - odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
b) przedmiotowych środków dowodowych - odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
c) innych dokumentów - odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
7) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 6 może dokonać również notariusz.
8) Przez cyfrowe odwzorowanie należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
9) Wykonawca może złożyć tylko jedną ofertę.
10) Wykonawca składa ofertę zgodnie z wymaganiami określonymi w SWZ. Treść oferty musi odpowiadać treści SWZ.
11) Do złożenia oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy ważnego kwalifikowanego podpisu elektronicznego, podpisu zaufanego lub podpisu osobistego.
12) Oferta musi być sporządzona w języku polskim.
13) Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski. W przypadku, o którym mowa w § 14 Rozporządzenia, Zamawiający może żądać od Wykonawcy przedstawienia tłumaczenia na język polski wskazanych przez Wykonawcę i pobranych samodzielnie przez Zamawiającego dokumentów.
14) Oferty należy składać za pośrednictwem Platformy pod adresem: https://tcuw.ezamawiajacy.pl
Link do postępowania:
https://tcuw.ezamawiajacy.pl/pn/TCUW/demand/334443/notice/public/details
15) Korzystanie z Platformy jest bezpłatne.

26. Informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu Ustawy o zwalczaniu nieuczciwej konkurencji

1) Wykonawca ma prawo zastrzec, że przekazane przez niego informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2026 r. poz. 85.), nie mogą być udostępniane, o ile uczyni to wraz z ich przekazaniem i w tym terminie wykaże (załączając stosowne uzasadnienie – dowody), że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Nie mogą stanowić tajemnicy przedsiębiorstwa informacje podawane do wiadomości po otwarciu ofert, tj. nazwa (albo imię i nazwisko), siedziba (lub miejsce prowadzonej działalności albo miejsce zamieszkania) Wykonawcy, informacje dotyczące ceny lub kosztu oferty.

2) Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w postaci oddzielnego pliku i opatrzone nazwą, z której wynika, że plik zawiera tajemnicę przedsiębiorstwa. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania będą traktowane jako jawne bez zastrzeżeń.

Część VIII - Składanie oferty i tryb udzielania wyjaśnień

27. Sposób komunikacji w postępowaniu

1) Korespondencję w niniejszym postępowaniu Zamawiający i Wykonawcy przekazują wzajemnie w języku polskim przy użyciu środków komunikacji elektronicznej za pośrednictwem Platformy pod adresem: https://tcuw.ezamawiajacy.pl.

2) Zamawiający nie przewiduje komunikowania się z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej. W sytuacjach awaryjnych (np. przerwy w funkcjonowaniu lub niedziałania Platformy) dopuszcza się komunikację za pomocą poczty elektronicznej, z wykorzystaniem adresu email: przetargi@tcuw.torun.pl z zastrzeżeniem, że oferta z załącznikami może być złożona wyłącznie za pomocą Platformy.

3) Każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt otrzymania korespondencji przekazanej w formie poczty elektronicznej.

4) Dokumentacja niniejszego postępowania została opublikowana na Platformie. W celu zapoznania się z dokumentacją postępowania wykonawca po przejściu na dedykowany zamawiającemu adres Platformy:

a) do upływu terminu składania ofert przechodzi do zakładki „Lista postępowań PZP”, wybiera zakładkę „Aktualne” i wyszukuje przedmiotowe postępowanie, a następnie klikając w wiersz postępowania, przechodzi do obszaru postępowania. Wykonawca ma możliwość pobrania każdego dokumentu odrębnie po naciśnięciu na wybrany załącznik lub w formie skompresowanej paczki po zaznaczeniu wybranych dokumentów.

b) po upływie terminu składania ofert przechodzi do zakładki „Lista postępowań PZP”, wybiera zakładkę „W toku”, wyszukuje przedmiotowe postępowanie, a następnie klikając w wiersz postępowania, przechodzi do obszaru postępowania.

5) Złożenie oferty wymaga zalogowania na Platformie poprzez aplikację Marketplanet OnePlace.
6) Do złożenia oferty wystarczające jest założenie bezpłatnego konta BASIC. Instrukcja założenia konta zawarta jest na Platformie w zakładce „Baza wiedzy”.
7) Założenie konta Wykonawcy w aplikacji Marketplanet OnePlace wymaga akceptacji „Regulaminu korzystania z Marketplanet OnePlace”.
8) Wykonawca po wybraniu opcji „Przystąp do postępowania” zostanie przekierowany do strony https://oneplace.marketplanet.pl, gdzie zostanie powiadomiony o możliwości zalogowania lub założenia bezpłatnego konta. Wykonawca zakłada konto wykonując kroki procesu rejestracyjnego; podaje adres e- mail, ustanawia hasło, następnie powtarza hasło, wpisuje kod z obrazka, akceptuje regulamin, klika polecenie „zarejestruj się”.
9) UWAGA: Wiadomość potwierdzająca aktywację konta zostanie przesłana na adres e-mail użyty podczas rejestracji w ciągu 6 godzin roboczych od przesłania wniosku do akceptacji.
10) Jeżeli niezbędna jest szybsza weryfikacja wniosku, istnieje możliwość kontaktu z infolinią wsparcia (22 257 22 23) z prośbą o przyspieszenie weryfikacji wniosku rejestracyjnego. Infolinia jest czynna w dni robocze od godziny 9:00 do 17:00.
11) W związku z tym zamawiający zaleca wykonawcom uwzględnienie czasu niezbędnego na rejestrację w procesie złożenia Oferty w postaci elektronicznej.
12) Zwrócenie się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ nie wymaga logowania do Platformy. Sposób złożenia wniosku oraz przekazanie wyjaśnień zostało szczegółowo określone w pkt 28 SWZ.
13) Zamawiający wymaga przekazywania sobie przez strony postępowania oświadczeń, wniosków, zawiadomień oraz informacji przy użyciu środków komunikacji elektronicznej za pośrednictwem Platformy. Szczegółowa Instrukcja korzystania z Platformy dostępna jest w zakładce „Baza wiedzy”. Szczegóły na temat wykonywania poszczególnych czynności w toku postępowania zawarte są w Instrukcji użytkownika (Instrukcja dla wykonawcy).
14) Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na Platformie, w tym informację nt. specyfikacji połączenia, tj.:
a) stały dostęp do sieci Internet o gwarantowanej przepustowości niemniejszej niż 512 kb/s;
b) komputer klasy PC lub MAC, spełniający wymagania zainstalowanego systemu operacyjnego oraz wymagania używanej przeglądarki internetowej;
c) zainstalowana dowolna przeglądarka internetowa w wersji wspieranej przez producenta obsługująca TLS 1.2;
d) włączona obsługa JavaScript;
e) zainstalowany program Acrobat Reader lub inny obsługujący pliki w formacie .pdf.
15) Zamawiający zgodnie z § 11 ust. 2 ww. Rozporządzenia dopuszcza formaty przesyłanych danych tj. plików o wielkości do 2 GB w formatach: .pdf, .xls, .xlsx, .doc, .docx, .txt, .rtf, .xps, .odt, .ods, .odp, .ppt, .pptx, .csv, .jpg, .jpeg, .tif, .tiff, .geotiff, .png, .svg, .wav, .mp3, .avi, .mpg, .mpeg, .mp4, .m4a,.mpeg4, .ogg, .ogv, .zip, .tar, .gz, .gzip, .7z, .html, .xhtml, .css,

.xml, .xsd, .gml, .rng, .xsl, .xslt. TSL, XMLsig, XAdES, CAdES, ASIC, XMLenc.

16) Zamawiający zgodnie z § 11 ust. 2 ww. Rozporządzenia określa informacje na temat kodowania i czasu odbioru danych tj.: plik załączony przez Wykonawcę na Platformie zakupowej i zapisany, widoczny jest w Systemie, jako zaszyfrowany – format kodowania UTF8.

17) Możliwość otwarcia plików zawierających ofertę dostępna jest dopiero po odszyfrowaniu przez Zamawiającego po upływie terminu składania ofert.

18) Oznaczenie czasu odbioru danych przez Platformę stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg czasu lokalnego serwera synchronizowanego odpowiednim źródłem czasu.

19) W przypadku problemów technicznych dotyczących pracy Platformy można się kontaktować z serwisem dostępnym codziennie od poniedziałku do piątku (z wyłączeniem dni ustawowo wolnych od pracy) w godzinach od 8:00 do 17:00:

20) pod numerem telefonu: +48 (22) 25 72 223,

21) pod adresem e-mail: oneplace@marketplanet.pl

22) Oświadczenia, wnioski, zawiadomienia lub informacje, które wpłyną do Zamawiającego, uważa się za dokumenty złożone w terminie, jeśli ich czytelna treść dotrze do Zamawiającego przed upływem tego terminu (wczytania na Platformie).

23) Za datę wpływu oferty, oświadczeń, wniosków, zawiadomień oraz informacji przekazywanych przez Strony przyjmuje się datę i godzinę ich wysłania za pośrednictwem Platformy. W przypadku braku potwierdzenia otrzymania korespondencji przez wykonawcę, Zamawiający domniema, że korespondencja wysłana przez Zamawiającego za pośrednictwem Platformy na konto Wykonawcy, została mu doręczona w sposób umożliwiający zapoznanie się z jej treścią.

24) Każdorazowo, jeśli w niniejszej SWZ jest mowa o opatrzeniu/podpisaniu dokumentu/oświadczenia kwalifikowanym podpisem elektronicznym, Zamawiający wymaga, aby kwalifikowany podpis elektroniczny wystawiony był przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

25) Każdorazowo, jeśli w niniejszej SWZ jest mowa o opatrzeniu/podpisaniu dokumentu/oświadczenia podpisem zaufanym lub podpisem osobistym, należy przez to rozumieć odpowiednio: podpis zaufany, o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz podpis osobisty, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych.

26) W korespondencji związanej z niniejszym postępowaniem wykonawcy powinni posługiwać się znakiem postępowania: 45/2026.

27) Sposób sporządzenia dokumentów elektronicznych, ofert, oświadczeń, o których mowa w art. 125 ust. 1 Ustawy, podmiotowych środków dowodowych, przedmiotowych środków dowodowych, oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, musi być zgodny z wymaganiami określonymi w wydanym na podstawie art. 70 Ustawy rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie

zamówienia publicznego lub konkursie oraz w Rozporządzeniu.
28) Wymagane zgodnie z niniejszą SWZ podmiotowe środki dowodowe, inne dokumenty lub oświadczenia, o których mowa w Rozporządzeniu, dotyczące Wykonawcy lub podmiotów udostępniających zasoby, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 118 Ustawy oraz dotyczące podwykonawców, składane są w formie określonej w Rozporządzeniu.

28. Wyjaśnienia i pytania

1) Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
2) Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak niepóźniej niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego niepóźniej niż na 4 przed upływem terminu składania ofert.
3) W przypadku, gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ppkt 2 powyżej, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
4) Treść zapytań wraz z wyjaśnieniami zamawiający udostępnia na stronie internetowej prowadzonego postępowania, a w przypadkach, o których mowa w art. 280 ust. 2 i 3 Ustawy, przekazuje wykonawcom, którym przekazał SWZ, bez ujawniania źródła zapytania.

29. Modyfikacja treści SWZ

1. W uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu do składania ofert, zmodyfikować treść niniejszej SWZ. Dokonaną w ten sposób modyfikację Zamawiający udostępnia na stronie internetowej prowadzonego postępowania.
2. Modyfikacje są każdorazowo wiążące dla Wykonawców od dnia publikacji na Platformie.
3. W przypadku, gdy zmiana treści SWZ jest istotna dla sporządzenia oferty lub wymaga od wykonawców dodatkowego czasu na zapoznanie się ze zmianą treści SWZ i przygotowanie ofert, Zamawiający przedłuży termin składania ofert, kierując się zasadą określoną w art. 286 ust. 3 Ustawy. O przedłużeniu terminu składania ofert Zamawiający zawiadamia wszystkich Wykonawców, którym przekazał niniejszą SWZ oraz udostępnia tę informację na stronie internetowej prowadzonego postępowania.
4. Jeżeli zmiana treści SWZ, będzie prowadziła do zmiany treści ogłoszenia o zamówieniu Zamawiający dokona zmiany treści ogłoszenia o zamówieniu w sposób przewidziany w art. 286 ust. 9 Ustawy oraz, jeśli będzie to konieczne przedłuży termin składania ofert zgodnie z art. 271 ust. 3 Ustawy.
5. W przypadku rozbieżności pomiędzy treścią SWZ a treścią udzielonych wyjaśnień i zmian, jako obowiązującą należy przyjąć treść informacji zawierającej późniejsze oświadczenie zamawiającego.

30. Zebranie Wykonawców

Zamawiający nie przewiduje zwołania zebrania Wykonawców w celu wyjaśnienia wątpliwości

dotyczących treści niniejszej SWZ. Zamawiający odpowie na pytania dotyczące treści SWZ w sposób zgodny z art. 284 Ustawy.

Część IX - Informacje o trybie składania, otwarcia oraz badania ofert

31. Składanie ofert

Oferty należy składać **do dnia 13.11.2026 r. do godz. 10:00** wyłącznie za pośrednictwem Platformy.
Link: https://tcuw.ezamawiajacy.pl/pn/TCUW/demand/334443/notice/public/details

32. Zmiana lub wycofanie oferty

Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Platformy. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

33. Związanie ofertą

1) Wykonawca pozostaje związany złożoną ofertą do dnia **12.12.2026 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2) W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, Zamawiający przed upływem terminu związania ofertą zwraca się do Wykonawców jednokrotnie o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, niedłuższy jednak niż 30 dni.

34. Otwarcie ofert

1) Otwarcie ofert nastąpi poprzez odszyfrowanie wczytanych na Platformie ofert w dniu **13.11.2026 r. o godz. 10:15,** przy czym niepóźniej niż dnia następnego po dniu, w którym upłynął termin składania ofert. W przypadku awarii systemu teleinformatycznego, przy użyciu którego następuje otwarcie ofert, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
2) Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
3) Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
   a) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej bądź miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
   b) cenach lub kosztach zawartych w ofertach.

35. Badanie ofert, sposób poprawiania omyłek, uzupełnianie dokumentów

1) Na posiedzeniu niejawnym Zamawiający oceni spełnianie przez Wykonawców warunków udziału w postępowaniu oraz dokona zbadania ofert pod względem przyjętych w SWZ wymagań. Następnie dokona kwalifikacji Wykonawców do wykluczenia z ubiegania się o udzielenie zamówienia i kwalifikacji ofert do odrzucenia. Spośród ofert nie odrzuconych Zamawiający dokona oceny ofert i wybierze ofertę najkorzystniejszą.
2) Zamawiający poprawia w ofercie:
   a) oczywiste omyłki pisarskie,
   b) oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   c) inne omyłki polegające na niezgodności oferty z dokumentami zamówienia pod warunkiem, że nie powodują one istotnych zmian w treści oferty.
3) O poprawieniu ww. omyłek Zamawiający niezwłocznie zawiadomi Wykonawcę, którego oferta została poprawiona. W przypadku, gdy Wykonawca w terminie odpowiednim wyznaczonym przez Zamawiającego nie wyrazi zgody na poprawienie omyłki, o której mowa w pkt. 35 ust. 2 c) SWZ lub nie zakwestionuje jej poprawienia uznaje się, że wyraził on zgodę na poprawienie omyłki.
4) Zamawiający może zwracać się do Wykonawców o udzielenie wyjaśnień dotyczących treści złożonej oferty w trybie art. 223 ust 1 Ustawy.

36. Informacja dotycząca badania rażąco niskiej ceny

1) Jeżeli zaoferowana cena lub koszt, lub ich istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia lub budzą wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwraca się o udzielenie wyjaśnień w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu, lub ich istotnych części składowych.
2) W przypadku gdy cena całkowita oferty złożonej w terminie 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 niepodlegających odrzuceniu na podstawie art. 226 ust. 1 pkt 1 i 10, Zamawiający zwraca się o udzielenie wyjaśnień, o których mowa w ust. 1, 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, Zamawiający może zwrócić się o udzielenie wyjaśnień, o których mowa w ust. 1.
3) Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na Wykonawcy.

4) Odrzuceniu jako oferta z rażąco niską ceną lub kosztem, podlega oferta Wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej w ofercie ceny lub kosztu.

Część X - Tryb i zasady wyboru najkorzystniejszej oferty

37. Tryb badania i oceny oferty, negocjacje

1) Badania i oceny ofert będzie dokonywała komisja przetargowa.
2) Zamawiający dokona kwalifikacji Wykonawców do wykluczenia z ubiegania się o udzielenie zamówienia i kwalifikacji ofert do odrzucenia.
3) Spośród ofert nieodrzuconych Zamawiający dokona oceny ofert i wybierze ofertę najkorzystniejszą.

38. Kryteria oceny oferty

1) Zamawiający dokona oceny ofert. Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów po zsumowaniu wartości punktowej wszystkich kryteriów.
2) W celu wyboru najkorzystniejszej oferty Zamawiający przyjął następujące kryteria - przypisując im odpowiednio wagę procentową:

a) **cena oferty - 60%**
Cena za realizację dostawy zgodnie z przedmiotem zamówienia. Zamawiający przyzna punkty w tym kryterium w oparciu o informacje podane w Formularzu ofertowym.

b) **ośrodek przetwarzania danych – 20%**

Punkty zostaną przyznane za centrum przetwarzania danych, z którego świadczone będą usługi objęte zamówieniem.

a) Centrum danych posiada aktualny certyfikat ANSI/TIA-942 Rated 3– 10 pkt;
b) Centrum danych posiada aktualny certyfikat Tier III Facility– 10 pkt.

Maksymalna liczba punktów możliwa do uzyskania w ramach kryterium wynosi 20 pkt.

c) **dostępność usługi SLA - 20%**
Zamawiający przyzna punkty w tym kryterium w oparciu o informacje podane w Formularzu ofertowym.

39. Zasady oceny ofert wg ustalonych kryteriów

Wykonawca może uzyskać punkty w liczbie od zera do 100. Za korzystniejszą ofertę zostanie uznana oferta, która otrzyma największą liczbę punktów stanowiących sumę punktów przyznanych za kryterium a), b), c) wg. poniższego wzoru.

Cot = PC + PDC + PSLA

gdzie:

Cot oznacza: liczba punktów przyznanych za całość oferty,
PC oznacza: liczba punktów przyznanych za kryterium ceny,
PDC oznacza: liczba punktów przyznanych za ośrodek przetwarzania danych,
PSLA oznacza: liczba punktów przyznanych za kryterium dostępności usługi SLA.

Każda oferta może uzyskać za dane kryterium określoną liczbę punktów przy zastosowaniu wzorów:

$$\textit{a) cena oferty} = \frac{\textit{najniższa oferowana cena spośród złożonych ofert}}{\textit{cena oferty badanej}} \times \textit{100 pkt x znaczenie kryterium tj. 60\%}$$

b) ośrodek przetwarzania danych

Zamawiający przyzna punkty w tym kryterium w oparciu o informacje podane w Formularzu ofertowym, które muszą być potwierdzone **certyfikatami załączonymi** do Formularza ofertowego.

Punkty za to kryterium zostaną przyznane w skali punktowej od 10 do 20 pkt., wg poniższej zasady:

Posiadany aktualny certyfikat ANSI/TIA-942 Rated 3: 10 pkt
Posiadany certyfikat Tier III Facility: 10 pkt

c) dostępność usługi SLA - 20%

Zamawiający przyzna punkty w tym kryterium w oparciu o informacje podane w Formularzu ofertowym.

Punkty za to kryterium zostaną przyznane w skali punktowej od 0 do 20 pkt. wg poniższej zasady:

Gwarancja dostępności usługi od 99,90% do 99,98% SLA w skali roku – 0 pkt
Gwarancja dostępności usługi od 99,99% SLA w skali roku – 20 pkt

Minimalny wymagany poziom dostępności usługi (SLA) wynosi 99,90% w skali roku. Oferty przewidujące poziom dostępności usługi niższy niż 99,90% zostaną odrzucone jako niezgodne z warunkami zamówienia.

Zamawiający udzieli zamówienia Wykonawcy, którego oferta zdobędzie największą ilość punktów

we wszystkich kryteriach łącznie.
Punktacja będzie liczona według powyższych kryteriów. Łączna ocena oferty stanowić będzie sumę punktów uzyskanych przez ofertę we wszystkich trzech kryteriach, na zasadach jak powyżej.
Liczba punktów wynikająca z działań matematycznych będzie zaokrąglana do dwóch miejsc po przecinku wedle reguł matematycznych.

Stosownie do art. 248 Ustawy, jeżeli Zamawiający nie może dokonać wyboru oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybiera ofertę z najniższą ceną. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa powyżej, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy składający oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

Część XI - Zobowiązania Wykonawcy związane z umową w sprawie zamówienia publicznego oraz realizacja zamówienia.

40. Zamawiający nie wymaga wniesienia zabezpieczenie należytego wykonania.

41. Zamawiający nie przewiduje udzielenia Wykonawcy zaliczek na poczet wykonania zamówienia.

42. Ogłoszenie o wyborze najkorzystniejszej oferty i zawarcie umowy

1) Niezwłocznie po wyborze oferty najkorzystniejszej, Zamawiający zawiadomi równocześnie Wykonawców, którzy złożyli oferty oraz udostępni na stronie internetowej prowadzonego postępowania (Platformie) informacje o wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację.
2) Niezwłocznie po wyborze oferty najkorzystniejszej, Zamawiający zawiadomi równocześnie Wykonawców, którzy złożyli oferty o Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne.
3) Wykonawca, którego oferta zostanie wybrana powiadomiony zostanie o terminie i miejscu zawarcia umowy.
4) Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy-Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

5) Wykonawcy wspólnie ubiegający się o zamówienie (którzy zostali wybrani do realizacji przedmiotu zamówienia) winni przed podpisaniem umowy dostarczyć dokument regulujący ich współpracę.

43. Zasady wprowadzania w umowie zmian wysokości wynagrodzenia należnego Wykonawcy

1. Wszelkie zmiany w umowie będą mogły być dokonywane wyłącznie w zakresie dopuszczonym ustawą Prawo zamówień publicznych, w szczególności art. 455 pzp, wymagają zgodnej woli stron oraz zachowania formy pisemnej, pod rygorem nieważności. Zmiana postanowień Umowy może nastąpić w przypadku następujących zmian:
1) Wykonawca z przyczyn leżących po stronie Zamawiającego nie może dotrzymać terminów określonych w harmonogramie wdrożenia;
2) nastąpiła Siła Wyższa rozumiana jako zdarzenie lub połączenie zdarzeń obiektywnie niezależnych od Stron, które zasadniczo i istotnie utrudniają wykonywanie części lub całości zobowiązań wynikających z niniejszej Umowy, których Strony nie mogły przewidzieć i którym nie mogły zapobiec, ani ich przezwyciężyć, i im przeciwdziałać poprzez działanie z należytą starannością ogólnie przewidzianą dla cywilnoprawnych stosunków zobowiązaniowych;
3) wystąpiła zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy – w zakresie odpowiadającym wpływowi zmiany przepisu na przedmiot umowy;
4) wystąpiła zmiana stawki podatku od towarów i usług VAT oraz podatku akcyzowego, jeżeli zmiana ta będzie miała wpływ na koszty wykonania Zamówienia przez Wykonawcę VAT - zmiana wysokości przysługującego Wykonawcy wynagrodzenia odpowiednio do całkowitej wysokość wzrostu lub obniżenia kosztów Wykonawcy zamówienia publicznego wynikających z podwyższenia lub obniżenia stawki podatku od towarów i usług lub podatku akcyzowego;
5) wystąpiła zmiana wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów Ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, jeżeli zmiana ta będzie miała wpływ na koszty wykonania Zamówienia przez Wykonawcę – w takim wypadku zmiana wynagrodzenia nastąpi proporcjonalnie do wykazanego przez Wykonawcę zakresu wpływu podwyższenia wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej na koszt wykonania zamówienia, jeżeli Wykonawca wykaże zatrudnianie pracowników wyłącznie przy realizacji przedmiotu zamówienia w pełnym wymiarze czasu pracy na podstawie umowy o pracę, otrzymujących minimalne wynagrodzenie lub na podstawie innej umowy, otrzymujących wynagrodzenie w wysokości minimalnej stawki godzinowej;
6) wystąpiła zmiana zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne, jeżeli zmiana ta będzie miała wpływ na koszty wykonania Zamówienia przez Wykonawcę – w takim wypadku zmiana wynagrodzenia nastąpi odpowiednio do sumy wzrostu kosztów Wykonawcy zamówienia publicznego oraz drugiej strony umowy o pracę lub innej umowy cywilnoprawnej łączącej Wykonawcę zamówienia publicznego z osobą fizyczną nie prowadzącą działalności gospodarczej, wynikających z konieczności odprowadzenia dodatkowych składek od

wynagrodzeń osób zatrudnionych na umowę o pracę lub na podstawie innej umowy cywilnoprawnej zawartej przez wykonawcę z osobą fizyczną nie prowadzącą działalności gospodarczej, a biorących udział w realizacji zamówienia przy założeniu braku zmiany wynagrodzenia netto tych osób;
7) wystąpiła zmiana zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych, jeżeli zmiana ta będzie miała wpływ na koszty wykonania Zamówienia przez Wykonawcę – w takim wypadku zmiana wynagrodzenia nastąpi odpowiednio do wzrostu kosztów związanych bezpośrednio z realizacją zamówienia publicznego wynikającą z wpłat do PPK dokonywanych przez podmioty zatrudniające uczestniczące w wykonaniu zamówienia publicznego, w zakresie obciążającym podmiot zatrudniający.
8) Strony mogą dokonać istotnych zmian umowy w przypadku uzasadnionej przyczynami technicznymi, w szczególności ujawnionymi na etapie wdrożenia, konieczności zmiany:
a) sposobu wykonania umowy w obszarach: organizacyjnym, wykorzystywanych narzędzi, przyjętych metod i kanałów komunikacji,
b) zakresu przedmiotu umowy w obszarze wymagań funkcjonalnych lub niefunkcjonalnych, jeżeli rezygnacja z danego wymagania lub zastąpienie go innym, spowoduje zoptymalizowane dopasowanie przedmiotu umowy do potrzeb Zamawiającego,
Zamawiający dopuszcza wprowadzenie odpowiednich zmian uwzględniających stwierdzone przyczyny techniczne, polegających w szczególności na modyfikacji wymagań Zamawiającego lub zmianie sposobu ich realizacji;
2. Stosownie do art. 439 ust. 1 ustawy Prawo zamówień publicznych Strony umowy uprawnione są do żądania zmiany wynagrodzenia zwanej dalej „waloryzacją”, w przypadku zmiany kosztów związanych z realizacją zamówienia.
3. Waloryzacja, o której mowa w ust. 2 powyżej ustalana będzie w następujący sposób:
1) Waloryzacji podlega jedynie wynagrodzenie za niezrealizowaną cześć umowy;
2) Waloryzacja będzie ustalana w oparciu o zmianę wskaźnika wysokości przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw za poprzedni rok ogłaszanego przez Prezesa GUS, zwanego dalej „Wskaźnikiem”;
3) Waloryzacja nastąpi na wniosek Strony, po każdych 6 miesiącach od zawarcia Umowy, jeżeli Wskaźnik ulegnie zmianie o co najmniej 7% wyliczony jako różnica między wartością wskaźnika z miesiąca poprzedzającego miesiąc złożenia wniosku, o którym mowa w pkt. 9), oraz wartością wskaźnika sprzed 7 miesięcy poprzedzających miesiąc złożenia wniosku, o którym mowa w pkt 9), ogłaszany przez Prezesa Głównego Urzędu Statystycznego (GUS) w Biuletynie Statystycznym GUS;
4) Początkowy termin ustalenia zmiany wynagrodzenia, o której mowa w zdaniu poprzednim wyznaczony jest na dzień zawarcia Umowy;
5) W przypadku likwidacji ww. Wskaźnika lub zmiany podmiotu, który go ustala, mechanizm, powyższe zasady stosuje się odpowiednio do wskaźnika i podmiotu ustalającego, które zgodnie z odpowiednimi przepisami prawa zastąpią ww. Wskaźnik lub podmiot go ustalający;
6) Waloryzacja wywołuje skutek od dnia podpisania stosownego aneksu do Umowy i obejmuje wynagrodzenie należne od dnia zawarcia aneksu;
7) Łączna wartość zmiany wynagrodzenia, jaką dopuszcza Zamawiający w efekcie zastosowania

niniejszych postanowień o waloryzacji wynosi 5% w stosunku do wynagrodzenia początkowego;
8) Postanowień umownych w zakresie waloryzacji nie stosuje się od chwili osiągnięcia limitu, o którym mowa w pkt. 7) powyżej;
9) Wykonawca wystąpi z wnioskiem o zmianę kwoty wynagrodzenia w zakresie określonym w niniejszym paragrafie z co najmniej 14-dniowym wyprzedzeniem wobec wnioskowanej daty obowiązywania nowego wynagrodzenia. Wniosek powinien zawierać wyczerpujące uzasadnienie faktyczne i prawne;
10) Zamawiający po zaakceptowaniu wniosku, o którym mowa w pkt 9), wyznaczy datę podpisania aneksu.
4. Jeżeli wynagrodzenie Wykonawcy zostało zmienione zgodnie z ust. 2-3 powyżej, zobowiązany jest on do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom kosztów dotyczących zobowiązania podwykonawcy, jeżeli łącznie spełnione są następujące warunki:
1) przedmiotem umowy są roboty budowlane, dostawy lub usługi;
2) okres obowiązywania umowy przekracza 6 miesięcy.
5. Zmiana Umowy może nastąpić za zgodą obu Stron wyrażoną na piśmie, pod rygorem nieważności.
6. Zmiany dotyczą wyłącznie rat wynagrodzenia niezapłaconych do dnia dokonania przez strony zmiany umowy.

Część XIII - Środki ochrony prawnej

44. Środki ochrony prawnej:

1) Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Ustawy, przysługują środki ochrony prawnej zgodnie z Działem IX Ustawy.
2) Odwołanie przysługuje od niezgodnej z przepisami Ustawy czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia (w tym na projektowane postanowienia Umowy) lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie Ustawy.
3) Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami Ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności prawne i faktyczne uzasadniające wniesienie odwołania.
4) Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej. Opatrzone odpowiednio własnoręcznym podpisem lub podpisem zaufanym. Odwołujący przesyła Zamawiającemu odwołanie (wniesione w formie elektronicznej lub postaci elektronicznej) lub kopię odwołania przed upływem terminu na jego wniesienie w taki sposób, żeby mógł on się zapoznać z jego treścią przed upływem tego terminu.
5) Terminy na wniesienie odwołania określone zostały w art. 515 Ustawy.
6) Szczegółowe zasady postępowania po wniesieniu odwołania określają przepisy Działu IX

Ustawy.

7) Na orzeczenie KIO stronom oraz uczestnikom postępowania przysługuje skarga do sądu.
8) Skargę wnosi się za pośrednictwem Prezesa KIO do Sądu Okręgowego w Warszawie – Sądu zamówień publicznych w terminie 14 dni od dnia doręczenia orzeczenia KIO, przesyłając jednocześnie jej odpis przeciwnikowi skargi.

Część XIV – Obowiązek Informacyjny w zakresie danych osobowych. Obowiązki Wykonawcy w zakresie danych osobowych

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

1) administratorem danych osobowych jest Gmina Miasta Toruń działająca poprzez Toruńskie Centrum Usług Wspólnych w Toruniu, adres: 87-100 Toruń, plac Św. Katarzyny 9,
2) w sprawach związanych z przetwarzaniem danych osobowych w ramach prowadzonego postępowania można kontaktować się z powołanym inspektorem ochrony danych osobowych, dostępnym pod adresem: Plac św. Katarzyny 9, 87-100 Toruń, e-mail: iod@tcuw.torun.pl,
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego na „Zapewnienie dla TCUW infrastruktury teleinformatycznej o wysokiej dostępności w modelu chmury obliczeniowej wraz z usługami towarzyszącymi."
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 Ustawy oraz ewentualnie organy rozpatrujące środki ochrony prawnej wniesione w toku postępowania i uczestnicy postępowań wywołanych ich wniesieniem,
5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 Ustawy, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy oraz w odpowiednim zakresie - okres rękojmi i gwarancji a także okres czasu do chwili przedawnienia roszczeń związanych z realizacją umowy,
6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem Ustawowym określonym w przepisach Ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z Ustawy,
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8) posiada Pani/Pan:
   a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;

c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) nie przysługuje Pani/Panu:
a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

10) Zgodnie z:
a) art. 75 Ustawy – w przypadku korzystania przez osobę z uprawnienia, o którym mowa w art. 15 ust. 1-3 RODO Zamawiający może żądać od osoby występującej z żądaniem wskazania dodatkowych informacji umożliwiających doprecyzowanie nazwy lub datę zakończonego postępowania o udzielenie zamówienia publicznego.
b) art. 19 ust. 2 i art. 76 Ustawy skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 RODO nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z Ustawą, ani naruszać integralności protokołu postępowania oraz jego załączników.
c) art. 19 ust. 3 i art. 74 ust. 3 Ustawy - Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 RODO nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego lub konkursu; w przypadku gdy wniesienie takiego żądania spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole postępowania lub załącznikach do tego protokołu, od dnia zakończenia postępowania o udzielenie zamówienia Zamawiający nie udostępnia tych danych, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2RODO.

11) W myśl art. 74 ust. 4 Ustawy zasada jawności, o której mowa w art. 74 ust. 1 Ustawy, ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 RODO zebranych w toku postępowania o udzielenie zamówienia publicznego. Ograniczenia zasady jawności, o których mowa w art. 74 ust. 3 i art. 18 ust. 3-6 Ustawy stosuje się odpowiednio.

12) W odniesieniu do danych osobowych przekazywanych Zamawiającemu a nie dotyczących bezpośrednio Wykonawcy (np. danych osobowych jego pracowników, reprezentantów, współpracowników, podwykonawców, osób, którymi posługuje się przy realizacji zamówienia, osób, które udostępniają mu zasoby na potrzeby udziału w postępowaniu itp.) Wykonawca zobowiązany jest do dopełnienia obowiązków informacyjnych, o których mowa w art. 13 lub 14 RODO, w tym do przekazania im informacji odnośnie administrowania ich danymi przez Zamawiającego oraz do złożenia wraz z ofertą oświadczenia o ich dopełnieniu pod rygorem odpowiedzialności odszkodowawczej wobec Zamawiającego.

Część XV - Postanowienia końcowe

46. Unieważnienie postępowania

1) Zamawiający unieważni postępowanie w sytuacjach określonych w art. 255 - 258 Ustawy.
2) O unieważnieniu postępowania Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy ubiegali się o udzielenie zamówienia w tym postępowaniu.
3) W przypadku unieważnienia postępowania o udzielenie zamówienia Zamawiający niezwłocznie zawiadomi wykonawców, którzy ubiegali się o udzielenie zamówienia w unieważnionym postępowaniu, o wszczęciu kolejnego postępowania, które dotyczy tego samego przedmiotu zamówienia lub obejmuje ten sam przedmiot zamówienia.

47. Sprawy nieuregulowane SWZ

W sprawach nieuregulowanych w niniejszej SWZ zastosowanie mają przepisy Ustawy oraz obowiązujące przepisy wykonawcze.

48. Załącznikami do SWZ są następujące wzory i dokumenty:

1) Opis przedmiotu zamówienia
2) Formularz specyfikacji technicznej
3) Oświadczenie wykonawcy o którym mowa w art. 125 ust. 1 ustawy
4) Projektowane postanowienia umowy (wzór Umowy)
5) Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej
6) Oświadczenie składane na wezwanie o aktualności informacji

Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

I Wymagania dla ośrodka przetwarzania danych w ramach którego oferowana będzie usługa i Wykonawca będzie przetwarzał dokumenty Zamawiającego w zakresie bezpieczeństwa

1) Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) Zamawiający wymaga od Wykonawcy uruchomienia i wdrożenia infrastruktury teleinformatycznej w modelu chmury obliczeniowej (IaaS) wraz z zapewnieniem rozwiązań w obszarze kopii bezpieczeństwa (backup) w celu spełnienia przez Zamawiającego wymogów bezpieczeństwa w obszarze łańcucha dostaw.
2) Z uwagi na potrzebę wysokiej dostępności infrastruktury IT będącej przedmiotem zamówienia, Zamawiający oczekuje, aby proponowane rozwiązanie IaaS i backup spełniało najwyższe, dostępne na terenie Unii Europejskiej standardy bezpieczeństwa teleinformatycznego. Wymagania dla ośrodka centrum danych (Primary Data Center, dalej „PDC") są obligatoryjne. Wykluczone jest częściowe spełnianie któregokolwiek wymogu. Zamawiający na etapie realizacji umowy zastrzega możliwość weryfikacji i wezwania Wykonawcy do udokumentowania spełniania każdego z wymogów określonych poniżej:
    a) PDC musi posiadać odpowiednie zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych Zamawiającego. Wykonawca ponosi odpowiedzialność w zakresie bezpieczeństwa informacji i danych przechowywanych na wykorzystanej infrastrukturze teleinformatycznej PDC.
    b) PCD musi posiadać zabezpieczenia sprzętu teleinformatycznego co najmniej w postaci:
        i. izolacji sprzętu krytycznego (dedykowana przestrzeń wyłącznie dla urządzeń serwerowych);
        ii. ochrony przed uszkodzeniem infrastruktury serwerowej w postaci zamykanych szaf rack;
        iii. prowadzenia rejestru wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego;
        iv. ochrony przed dostępem dla osób nieupoważnionych w trybie 24/7;
        v. ochrony świadczonej przez licencjonowaną firmę ochroniarską w trybie 24/7,
    c) PDC musi realizować profesjonalne utrzymanie i konserwację posiadanej infrastruktury teleinformatycznej co najmniej w postaci:

i. posiadania i stosowania procedury kontroli, regularnych przeglądów zgodnie z zaleceniami producentów, konserwacji i naprawy sprzętu teleinformatycznego, energetycznego i klimatyzacyjnego;

ii. napraw dokonywanych przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami lub autoryzowane serwisy zewnętrzne;

iii. usuwaniem nośników danych ze sprzętu teleinformatycznego przed przekazaniem do naprawy lub serwisu;

iv. stosowania bezpiecznej utylizacji lub przekazywania sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi);

v. prowadzenia aktualnego rejestru: przeglądów, incydentów, awarii i usterek.

d) PDC musi spełniać wymagania bezpieczeństwa w zakresie parametrów powalających wyeliminować wskazane zagrożenia:

Parametr	Wyeliminowanie zagrożenia
1. Obiekt i lokalizacja	
PDC zlokalizowane na terenie UE, a wszystkie dane Zamawiającego będą gromadzone i przetwarzane wyłączenie na terenie UE lub Lichtenstainu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.
PDC posiada ogrodzony, zamknięty teren wraz z ograniczoną strefą wejść.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji).
PDC jest usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji) w wyniku działań działania sił natury.
PDC jest położony niemniej niż 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania. Wysoka intensywność oddziaływania sytuacji krytycznych.
PDC jest oddalony niemniej niż 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów,

organizacji imprez masowych dla 10 tys. osób i więcej).	ryzyko zamieszek, zniszczeń.
PDC nie posiada ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z urządzeniami serwerowymi.	Zagrożenie przecieków, zalania infrastruktury IT lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).
PDC posiada niemniej niż 15 metrów oddalenia urządzeń serwerowych udostępnionych Zamawiającemu od źródeł pól zakłócających takich jak transformatory SN i WN.	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pól zakłócających pracę urządzeń elektrycznych i magnetycznych.
PDC posiada podłogę techniczną w pomieszczeniu z serwerami.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.
PDC spełnienia 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.
2. Węzły telekomunikacyjne	
PDC posiada połączenie światłowodowe z niezależnymi operatorami telekomunikacyjnymi, w tym niemniej niż 2 operatorów o zasięgu krajowym jest podłączonych niezależnymi drogami światłowodowymi.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora zewnętrznego.
Dojścia połączeń PDC wykonane są dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.
PDC posiada węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP oraz ochroną DDoS.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.
PDC posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%.	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.

PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.
PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.
3. Zasilanie energetyczne	
PDC posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż 99,999%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.
PDC posiada niemniej niż dwie niezależne linie zasilania dostępne dla infrastruktury IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.
PDC posiada 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.
PDC posiada redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.
System zasilaczy awaryjnych UPS w PDC gwarantuje podtrzymanie zasilania urządzeń serwerowych oraz infrastruktury towarzyszącej, przeznaczonej dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatów i ich 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.
Agregaty prądotwórcze PDC posiadają 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.
4. Bezpieczeństwo	

PDC jest wyposażone w system sygnalizacji włamania i napadu, system wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.
PDC posiada ochronę całego obiektu realizowaną przez profesjonalną zewnętrzną licencjonowaną firmę ochrony mienia. Ochrona realizowana jest w trybie 24/7.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.
PDC posiada system CCTV, który zapewnia ciągły 24/7 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.
System CCTV w PDC powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres nie krótszy niż 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.
System SKD (System Kontroli Dostępu) w PDC obejmuje niemniej niż trzy strefy dostępu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po terenie i obiekcie.
Dostęp do strefy I (teren w otoczeniu obiektu) w PDC podlega identyfikacji na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów) wkraczających na ogrodzony teren w otoczeniu obiektu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
Dostęp do strefy II (strefa technologiczna) w PDC możliwy jest wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
Dostęp do strefy III (pomieszczenia ze sprzętem serwerowym Zamawiającego) w PDC możliwy jest wyłącznie przy użyciu łącznie 2 elementów	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.

identyfikacji: SKD, osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego.	
PDC posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.
PDC posiada 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.
5. Monitoring	
PDC posiada elektroniczny system przyjmowania zgłoszeń dotyczących awarii dostępny w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.
PDC posiada stałe i całodobowe 24/7/365 monitorowanie poprawności pracy infrastruktury 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.

II. Wymagania SLA i czas reakcji

a. SLA dla oferowanego rozwiązania musi wynosić nie mniej niż 99,9% w skali roku (lub więcej zgodnie z deklaracją złożoną przez Wykonawcę w ofercie);
b. obsługa utrzymania i zarządzania oferowanego rozwiązania musi być realizowana w trybie 24/7/365;
c. przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w sposób autoryzowany w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status, wraz z historią wszystkich zgłoszeń;
d. Czas reakcji na zgłoszenie musi wynosić nie więcej niż 15 minut od przyjęcia zgłoszenia;
e. Czas usunięcia Awarii musi wynosić do 6 godzin od przyjęcia zgłoszenia;
f. Czas usunięcia Incydentu musi wynosić do 24 godziny od przyjęcia zgłoszenia.

III. Specyfikacja usługi

1) Przedmiotem zamówienia jest konfiguracja, uruchomienie i utrzymanie kompleksowego rozwiązania zapewnienia dostępu do bezpiecznej i wysokodostępnej infrastruktury teleinformatycznej HA (High Availability) w modelu chmury obliczeniowej IaaS wraz z usługami towarzyszącymi, w tym:
    a. **Chmura IaaS** - realizacja kompleksowej usługi polegającej na dostarczeniu usługi chmury obliczeniowej, w ramach której zostanie przygotowane i uruchomione środowisko teleinformatyczne w modelu IaaS wraz niezbędnym oprogramowaniem i jego dalszym prawidłowym utrzymaniem na potrzeby systemów i aplikacji Zamawiającego;
    b. **Kopia zapasowa backup** - realizacja kompleksowej usługi polegającej na dostarczeniu rozwiązania kopii zapasowej, w ramach którego zostanie przygotowane i uruchomione środowisko teleinformatyczne w modelu IaaS wraz niezbędnym oprogramowaniem i jego dalszym prawidłowym utrzymaniem na potrzeby realizacji testowych odtworzeń wykonywanych kopii zapasowych (backup) Zamawiającego;
    c. **Połączenia sieciowe** - realizacja kompleksowej usługi polegającej na dostarczeniu połączeń sieciowych, które są niezbędne do prawidłowego działania usług, o których mowa w lit. a-b) powyżej;
    d. **Przestrzeń dyskowa WORM** – realizacja kompleksowej usługi polegającej na gromadzeniu i bezpiecznym przechowywaniu danych w przestrzeni dyskowej z wykorzystaniem technologii obiektowej spełniającej jednocześnie funkcjonalności technologii WORM (Write Once, Read Many);
    e. **Usługi towarzyszące** - zapewnienie niezbędnych usług towarzyszących w postaci poczty email i bezpieczeństwa informatycznego, dodatkowego wsparcia technicznego i administracyjnego.

2) Uruchomienie usług, o których mowa w pkt. 1 lit. a-d) powyżej wraz z wykonaniem bezprzerwowej migracji systemów teleinformatycznych, aplikacji oraz danych cyfrowych z obecnie wykorzystywanych zasobów teleinformatycznych Zamawiającego do zasobów Wykonawcy dostarczonych w ramach przedmiotowego Zamówienia musi zostać wykonane w terminie do dnia **31.12.2026 roku**. Wykonawca ponosi pełną odpowiedzialność za wszelkie błędy konfiguracyjne i instalacyjne w infrastrukturze, która jest przedmiotem Zamówienia, które spowodują utratę danych z systemów i aplikacji Zamawiającego na etapie migracji z obecnej infrastruktury Zamawiającego do infrastruktury Wykonawcy.

3) **Szczegółowy opis Chmury IaaS**
    a. Wykonawca ma obowiązek dostarczyć infrastrukturę teleinformatyczną w modelu chmury obliczeniowej wraz z zapewnieniem dostępność HA (bez pojedynczego

punktu awarii) wszystkich dostarczonych zasobów IaaS na czas trwania umowy, w tym min.:

i. zgodnie z bieżącymi potrzebami Zamawiającego konfigurować i utrzymywać instancje serwerowe maszyn wirtualnych (VM), gotowe do instalacji własnych aplikacji i systemów Zamawiającego lub podmiotów przez niego wskazanych;

ii. zgodnie z bieżącymi potrzebami Zamawiającego instalować, utrzymywać i aktualizować na VM systemy operacyjne (Windows Server; Linux);

iii. skonfigurować i utrzymywać wewnętrzne połączenia sieciowe pomiędzy poszczególnymi VM oraz pozostałymi komponentami;

iv. skonfigurować i udostępnić łącza telekomunikacyjne zgodnie z określonymi w SWZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować operacje i zadania ze wszystkich VM oraz pozostałych komponentów zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę;

v. skonfigurować i udostępnić łącza do sieci Internet, zgodnie z określonymi w OPZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować operacje i zadania ze wszystkich instancji serwerowych oraz pozostałych komponentów zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę;

vi. skonfigurować i utrzymywać ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej;

vii. skonfigurować i utrzymywać na każdej VM, na której będzie to wskazane, oprogramowanie antywirusowe, aktualizowane na bieżąco, zarządzane z jednej konsoli administracyjnej, zabezpieczającej przed zagrożeniami należącymi do kategorii zagrożeń wirusowych systemów informatycznych;

viii. udostępnić system zbierania i przechowania logów zdarzeń z urządzeń sieciowych w celu stałego monitorowania wydajności rozwiązania;

ix. świadczyć usługę administrowania i utrzymywania uruchomionych VM do poziomu systemu operacyjnego włącznie (Windows Server; Linux), zgodnie z wytycznymi i bieżącymi potrzebami Zamawiającego;

i. zapewnić niezbędne licencje i oprogramowanie związane z realizacją przedmiotu zamówienia;

ii. świadczyć obsługę wsparcia zgodnie z określonymi parametrami wskazanymi w OPZ.

b. Zamawiający oczekuje dostarczenia infrastruktury teleinformatycznej w modelu chmury obliczeniowej IaaS z infrastruktury PDC, spełniającej minimalne wymogi bezpieczeństwa opisane w OPZ.

c. Zmawiający oczekuje zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z

najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres obowiązywania umowy.

d. Zamawiający oczekuje instalacji systemów operacyjnych Windows Server lub Linux z możliwością ich aktualizacji do najnowszych wersji dla każdej VM w ramach realizowanego przedmiotu zamówienia. Szczegółową listę VM wraz z rodzajem wymaganego systemu operacyjnego Zamawiający będzie przekazywał Wykonawcy zgodnie z bieżącym zapotrzebowaniem.

e. Zamawiający oczekuje uruchomienia infrastruktury teleinformatycznej w modelu chmury obliczeniowej wraz z niezbędnym do prawidłowego działania oprogramowaniem systemowym i narzędziowym o parametrach nie gorszych niż określone poniżej i pozwalających wykreować dowolną ilość maszyn wirtualnych VM o dowolnych parametrach każda (CPU, RAM, HDD, SSD), w ramach przydzielonej puli zasobów. Wymagana pula zasobów została wskazana poniżej i jako wymóg minimalny musi wynosić:

   i. architektura x86-64
   ii. interfejs sieciowy: 2x10 Gbps
   iii. procesor CPU min. Intel Gold 3,4 GHz: 48 vCPU
   iv. pamięć operacyjna RAM min. DDR4 2933MHz: 126 GB
   v. przestrzeń dyskowa klasy SSD min. 50 000 IOPS: 5 TB
   vi. przestrzeń dyskowa klasy NVMe min. 200 000 IOPS: 5 TB GB
   vii. publiczne adresy IPv4 w ilości adresów użytecznych: 10 szt.
   viii. odseparowane sieci vLAN w ilości: bez limitu ilość
   ix. powołane maszyny wirtualne wraz z zainstalowanym systemem operacyjnym Windows Server i Linux w ilości: 15

f. Wykonawca musi zapewnić rozwiązania wirtualizacji wspierające systemy Windows Server, preferowanym systemem wirtualizacji jest Microsoft Hyper-V.

g. Wykonawca musi zapewnić niezawodność i ciągłość pracy serwerów wirtualnych i serwera plików w ramach rozwiązania HA. W przypadku awarii pojedynczego komponentu (np. serwer fizyczny, dysk) musi następować automatyczne bezprzerwowe przełączenie urządzeń w celu utrzymania ciągłości pracy dostarczonych zasobów.

h. Na brzegu klastra wirtualizacyjnego wymagany jest system ochrony bezpieczeństwa WAN Firewall / UTM pracujące w klastrze. Urządzenia muszą być objęte wsparciem producenta oraz pełnym pakietem subskrypcji przez cały okres świadczenia usługi. Odpowiednie zarządzanie klastrem firewall, połączeniami VPN oraz regułami będzie

odpowiedzialnością Wykonawcy. W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje:

i. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
ii. Kontrola Aplikacji.
iii. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
iv. Ochrona przed malware.
v. Ochrona przed atakami - Intrusion Prevention System.
vi. Kontrola stron WWW.
vii. Zarządzanie pasmem (QoS, Traffic shaping).
viii. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
ix. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
x. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
xi. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
xii. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
xiii. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
xiv. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN oraz wykorzystanie w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
xv. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe oraz możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
xvi. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

xvii. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

xviii. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

xix. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

xx. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

xxi. W ramach filtra WWW muszę być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

xxii. Filtr WWW musi dostarczać kategorie stron zabronionych prawem np.: Hazard.

xxiii. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

xxiv. Filtr WWW musi dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

xxv. Funkcja Safe Search musi przeciwdziałać pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google.

xxvi. System musi pozwalać określać, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

xxvii. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

xxviii. System musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

xxix. System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

i. Zamawiający oczekuję, że do zadań realizowanych przez Wykonawcę w ramach dostarczonej infrastruktury należeć będzie administracyjna zasobami informatycznymi w zakresie:
    i. migracji z dotychczasowych zasobów Zamawiającego,
    ii. utrzymania i aktualizacji całego środowiska,
    iii. instalacji i konfiguracji systemów operacyjnych,
    iv. instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności HA,
    v. aktualizacji oprogramowania ze względu na błędy bezpieczeństwa,
    vi. utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa,
    vii. realizacji bieżących czynności administracyjnych,
    viii. przyjmowania zgłoszeń technicznych,
    ix. analiz incydentów oraz problemów wraz pełnym przywracaniem funkcjonalności.

j. Niezależnie od powyższego zakresu czynności, po uruchomieniu usługi do dyspozycji w ramach świadczonej usługi wsparcia administracyjnego Wykonawca udostępni zasoby ludzkie w postaci dodatkowych 50 roboczogodzin pracy Administratorów i Specjalistów IT na prace zlecone przez Zamawiającego.

4) **Szczegółowy opis Kopii zapasowych backup**

a. Wykonawca ma obowiązek dostarczyć usługę, która musi obejmować wszystkie VM będące składnikami środowiska teleinformatycznego IaaS Zamawiającego, oraz wszystkie dane zgromadzone w usłudze Microsoft 365.

b. Zamawiający oczekuje aby dane cyfrowe kopii zapasowych były gromadzone i przechowywane przez Wykonawcę w sposób bezpieczny w infrastrukturze teleinformatycznej centrum danych PDC, która spełnia wymogi bezpieczeństwa opisane w OPZ.

c. Wykonawca zapewni wszystkie niezbędne licencje i oprogramowanie związane z realizacją zadania.

d. Zakres realizacji kopii zapasowych zadania obejmuje:
    i. 15 szt. VM (15 licencji dla maszyn wirtualnych - Veeam Backup & Replication Standard – VM);
    ii. 128 szt. kont Microsoft 365 (128 licencji dla użytkowników- Veeam Backup for Microsoft Office 365 – User);

iii. rozmiar repozytorium musi być dostosowany do realizacji harmonogramu opisanego w punkcie poniżej (maksymalny rozmiar repozytorium nie przekroczy 25 TB);

e. Zamawiający oczekuje realizacji harmonogramu kopii zapasowych wykonywanych w modelu GFS:

i. S - kopia dzienna z retencją 7 dni wstecz;

ii. F - kopia tygodniowa z retencją 4 tygodnie wstecz;

iii. G - kopia miesięczna z retencją 12 miesięcy wstecz.

f. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób zautomatyzowany umożliwi dokonanie na żądnie Zamawiającego odtworzenia kopii zapasowej wybranej VM i weryfikacji spójności wszystkich odtwarzanych danych. Wszelkie zasoby IaaS wraz z oprogramowaniem niezbędnym do odtworzenia kopii zapasowej musi zapewnić Wykonawca. Zamawiający zastrzega, że testowe odtworzenie kopi zapasowych może być realizowane nie częściej niż 1 raz w miesiącu.

g. Wykonawca będzie realizował pełne wsparcie eksperckie, merytoryczne i administracyjne w zakresie prawidłowego działania systemu kopii zapasowych i zarządzania całością systemu kopii zapasowych, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres realizacji usługi.

h. Zamawiający oczekuje, aby wszystkie dane były szyfrowane kluczem szyfrującym o długości co najmniej 4096 bit oraz algorytmem szyfrującym powszechnie uznanym za bezpieczny.

i. Zamawiający oczekuje dostarczenia monitoringu kopii zapasowych, który charakteryzuje się następującymi parametrami:

i. interwały sprawdzania poprawności działania powinny być częstsze niż 5 min;

ii. system musi w czasie rzeczywistym informować o aktualnym stanie kopii zapasowej;

iii. system musi w czasie rzeczywistym raportować o wolnej przestrzeni dyskowej;

iv. system musi w czasie rzeczywistym monitorować wszystkie ustalone z Wykonawcą w trakcie wdrożenia parametry, jak np. czas wykonania kopii zapasowej czy ilość przetworzonych danych (rozmiar);

v. Zamawiający oczekuje, że w ramach realizacji systemu będzie możliwe osiągniecie RTO na poziomie 1h dla pojedynczej VM oraz RPO 12h dla całego środowiska kopii zapasowych.

j. Wykonawca zobligowany jest do dostarczenia systemu, który posiada następujący minimalny zestaw funkcjonalności w ramach dostarczonego rozwiązania:

i. rozwiązanie musi umożliwiać odtworzenie całej VM jak również pojedynczych plików bezpośrednio z kopii zapasowej (bez konieczności przywracania w całości VM, aby odzyskać pojedynczy plik), niezależnie od systemu operacyjnego maszyny wirtualnej;

ii. rozwiązanie musi być wyposażone w wewnętrzne mechanizmy kompresji - wykluczone jest stosowanie narzędzi innych, niż producenta rozwiązania systemu kopii zapasowej;

iii. mechanizm kompresji i deduplikacji musi być dostępny tylko dla danych nie zaszyfrowanych zarówno po stronie systemu operacyjnego VM i serwerów fizycznych oraz zaszyfrowanych przez dostarczony system kopii zapasowych;

iv. rozwiązanie musi umożliwiać pełne uruchomienie VM z kopii zapasowej w przypadku awarii oraz równoczesną realizację jej przywracania. Równolegle muszą mieć możliwość działać dwa procesy: (1) proces przywracania VM z kopii zapasowej, (2) proces jej poprawnego, pełnego funkcjonowania w trakcie operacji przywracania;

v. rozwiązanie musi umożliwiać przywracanie pojedynczych elementów aplikacyjnych z kopii zapasowych bez konieczności wcześniejszego przywrócenia całej VM. Do tych elementów zaliczają się co najmniej: pojedyncze wiadomości email lub pojedyncze wiersze i tabele baz danych;

vi. rozwiązanie musi być wyposażone w funkcję zaawansowanego monitorowania i raportowania infrastruktury, posiadać inteligentną diagnostykę i możliwość wykorzystywania infrastruktury i planowania mocy obliczeniowej, jak również musi umożliwiać analizę danych pierwotnych i dostosowywanie raportów, w tym tworzenie raportów umożliwiających konsolidowanie danych z wielu raportów w jednym zbiorczym zestawieniu.

5) **Szczegółowy opis połączeń sieciowych**

a. Wykonawca ma obowiązek dostarczyć usługę połączeń telekomunikacyjnych i sieciowych pozwalających na płynne działanie wszystkich systemów i rozwiązań umieszczonych w środowisku teleinformatycznych Wykonawcy, w tym:

i. zapewnić połączenia do sieci Internet za pomocą co najmniej trzech niezależnych operatorów telekomunikacyjnych o zasięgu co najmniej krajowym;

ii. dostępna dla całej dostarczonej infrastruktury przepustowość łącza do Internetu musi wynosić co najmniej 4 Gbps (łącze symetryczne) bez limitu transferu przesyłanych danych;

iii. zapewnić ochronę 24/7/365 przed atakami DDoS w pełnym zakresie przepustowości dla dostarczanych łącz, o których mowa powyżej wraz z dostępem do raportów nt. szczegółów ataków DDoS w przypadku ich realizacji;

iv. zapewnić połączenia między VM na interfejsach co najmniej 10G Ethernet. Każdy serwer fizyczny używany do wystawienia zasobów w ramach środowiska teleinformatycznego musi być połączony dwoma niezależnymi drogami, do dwóch niezależnych przełączników sieciowych, co najmniej 1 połączeniem 10G Ethernet na każdej drodze.

6) **Szczegółowy opis przestrzeni dyskowej WORM**

a. Wykonawca ma obowiązek dostarczyć usługę gromadzenia i bezpiecznego przechowywania danych w przestrzeni dyskowej z wykorzystaniem technologii obiektowej spełniającej jednocześnie funkcjonalności technologii WORM (Write Once, Read Many).

b. Usługa z funkcjonalnością technologii WORM musi zapewniać niezmienność i nieusuwalność danych przez zadany czas, zapewniający funkcjonalność trwałego nośnika informacji, tj. zgodnych z ustawą z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2026 r. poz. 623 ze zm.), ustawą z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2026 r. poz. 1244 ze zm.), ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164 ze zm.) oraz zgodnie z wymaganiami wynikającymi z dyrektywy MiFID II (Dyrektywa 2014/65/UE) oraz dyrektywy PSD2 (Dyrektywa 2015/2366/UE).

c. Usługa musi gwarantować dostęp do przestrzeni dyskowej dla łącznej ilości 500 000 dokumentów. Zamawiający przewiduję, iż całkowity rozmiar pojedynczego dokumentu, który zostanie przesłany do przestrzeni dyskowej wynosie nie więcej niż 2 MB.

d. Usługa musi zostać dostarczona w ramach klastra wysokiej dostępności HA. Dane składowane mają być minimum w dwóch kopiach na odseparowanych fizycznie i logicznie nośnikach w dwóch lokalizacjach (strefach) oddalonych od siebie (PDC – Primary Data Center, oraz SDC – Secondary Data Center) nie mniej niż 100 km w linii prostej. Każda kopia ma być niezależnie zabezpieczona przed utratą spowodowaną fizyczną awarią co najmniej dwóch dowolnych nośników danych (dysków), oraz fizycznego jednoczesnego uszkodzenia co najmniej dwóch serwerów kontrolujących pracę dysków. Zabezpieczenie każdej z dwóch stref musi zapewniać niezależną automatyczną odbudowę poziomu bezpieczeństwa w przypadku awarii dysku w czasie krótszym niż 1h. W przypadku awarii całego serwera czas automatycznego powrotu do pełnego poziomu bezpieczeństwa ma być krótszy niż 12h.

e. Usługa ma posiadać wbudowane mechanizmy przechowywania zarówno danych składowych jako obiekty, jak i metadanych systemowych oraz metadanych własnych (informacji opisujących obiekty / dane).

f. Usługa ma posiadać możliwość integrowania rozwiązania z istniejącym oprogramowaniem u Zamawiającego. Wymagane jest zapewnienie dostępu do danych poprzez REST API (REST – Representational State Transfer – styl

architektury oprogramowania opierający się o zbiór wcześniej określonych reguł opisujących jak definiowane są zasoby, a także umożliwiających dostęp do nich. Preferowany format komunikatów to JSON), (API – Application Programming Interface – zestaw reguł definiujący komunikację pomiędzy programami komputerowymi).

g. Usługa ma posiadać funkcjonalność replikacji synchronicznej pomiędzy minimum dwoma przestrzeniami dyskowymi tego samego typu. Dane po replikacji mają w dalszym ciągu zachowywać cechy trwałego nośnika WORM.

h. Usługa ma posiadać wbudowane mechanizmy zapewniające możliwość potwierdzenia autentyczności danych składowanych. Mechanizmy te muszą opierać się o wyliczenia sumy kontrolnej dla każdego składowanego obiektu. Wymagane jest wsparcie dla co najmniej następujących algorytmów kryptograficznych: MD5, SHA-1, SHA-256, SHA-512.

i. Gwarancja dostępności dokumentów zapisanych w przestrzeni dyskowej WORM ma obejmować okres 24 miesięcy od daty zakończenia umowy. Po zakończeniu umowy, Gwarancja dostępności danych cyfrowych zapewnia udostępnienie dokumentów Zamawiającemu na jego wezwanie.

j. Usługa ma posiadać mechanizm lub procedurę nieodwracalnego niszczenia danych dla których okres retencji 24 miesięcy został przekroczony.

7) **Szczegółowy opis usług towarzyszących**

Wykonawca ma obowiązek dostarczyć i świadczyć usługi dodatkowe, w tym:

a. **Oprogramowanie antywirusowe** - wykonawca ma obowiązek dostarczyć oprogramowanie antywirusowe w modelu usługowym na cały okres trwania umowy. Oprogramowanie musi chronić stacje robocze Użytkowników i wszystkie systemy maszyn wirtualnych w ramach dostarczonego rozwiązania. Zamawiający oczekuje dostarczenie oprogramowania antywirusowego w ilości 143 szt.
Minimalne wymagania funkcjonalno-użytkowe dla dostarczanej ochrony antywirusowej muszą obejmować:
   i. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
   ii. Rozwiązanie musi mieć możliwość integracji z systemem klasy SIEM, umożliwiając automatyczne przekazywanie logów, oraz wymuszenia reakcji na systemie operacyjnym.
   iii. Zamawiający posiada i używa rozwiązanie oparte na licencji firmy Eset
   iv. Dostarczone licencje muszą zapewniać nieprzerwany dostęp do wszystkich funkcjonalności oferowanego rozwiązania antywirusowego, aktualizacji oraz wsparcia producenta przez cały okres obowiązywania umowy.
   v. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.

vi. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

vii. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

viii. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

ix. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

x. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

xi. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

xii. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

xiii. Rozwiązanie musi wspierać architekturę ARM64.

xiv. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

xv. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

xvi. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

xvii. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

xviii. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

xix. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

xx. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

xxi. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

xxii. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

xxiii. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

xxiv. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

xxv. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

xxvi. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

xxvii. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

xxviii. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

xxix. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

xxx. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

xxxi. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

xxxii. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

xxxiii. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

xxxiv. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

xxxv. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

xxxvi. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

xxxvii. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

xxxviii. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.

xxxix. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

xl. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

xli. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

xlii. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

xliii. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

xliv. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

xlv. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

xlvi. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

xlvii. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.

xlviii. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

xlix. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

l. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

li. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

lii. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

liii. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

liv. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

lv. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.

lvi. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

lvii. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

lviii. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

lix. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

lx. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

lxi. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

lxii. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.

Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

lxiii. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

lxiv. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

lxv. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji

lxvi. szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu

lxvii. antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

lxviii. Konsola administracyjna musi mieć możliwość tagowania obiektów.

lxix. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

b. **Konto pocztowe Microsoft 365 Business Standard** - Wykonawca ma obowiązek dostarczyć konta pocztowe dla Użytkowników w modelu usługowym na cały okres trwania umowy. Zamawiający oczekuje dostarczenia 128 szt. kont.

c. **Konto pocztowe Microsoft 365 Business Basic** - Wykonawca ma obowiązek dostarczyć konta pocztowe dla Użytkowników w modelu usługowym na cały okres trwania umowy. Zamawiający oczekuje dostarczenia 30 szt. kont.

d. **Konto Microsoft Power BI Premium** - Wykonawca ma obowiązek dostarczyć konta dla Użytkowników w modelu usługowym na cały okres trwania umowy. Zamawiający oczekuje dostarczenia 4 szt. kont.

e. **Konto Microsoft Exchange Plan 2** - Wykonawca ma obowiązek dostarczyć konta dla Użytkowników w modelu usługowym na cały okres trwania umowy. Zamawiający oczekuje dostarczenia 3 szt. kont.

f. **Konto Microsoft SQL** - Wykonawca ma obowiązek dostarczyć konta dla Użytkowników w modelu usługowym na cały okres trwania umowy. Zamawiający oczekuje dostarczenia 1 szt. kont.

g. **Bezpieczne połączenie VPN -** Wykonawca ma obowiązek skonfigurować i dostarczyć usługę bezpiecznego połączenia VPN polegającej na zestawieniu bezpiecznej komunikacji pomiędzy infrastrukturą teleinformatyczną Wykonawcy a stacją roboczą każdego Użytkownika w celu umożliwienia realizacji pracy zdalnej. Połączenie VPN musi być realizowane w podziale na dwie separowane grupy użytkowników z różnymi uprawnieniami dostępu. Zamawiający na etapie realizacji wskaże podział Użytkowników na grupy. Zamawiający oczekuje dostarczenia 50 szt. połączeń.

h. **System uprawnień AD** - Wykonawca ma obowiązek skonfigurować i dostarczyć usługę systemu uprawnień typu Active Directory dla każdego uruchomionego Użytkownika końcowego Zamawiającego w ramach wraz AD Connect na potrzeby komunikacji z usługą Microsoft 365. Podstawowe wymagania konfiguracji muszą spełniać następujące wymagania:

   i. umożliwia scentralizowane zarządzanie obiektami (serwery, drukarki czy udostępnione pliki), a także przypisywanie uprawnień do tychże zasobów,

   ii. umożliwia uwierzytelnienie obiektów (np. użytkowników, komputerów) i autoryzacja (lub jej odmowa) dostępu do innych obiektów (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji,

   iii. umożliwia konfigurację obiektów,

   iv. możliwość działania w rozproszonych sieciach,

   v. możliwość działania w środowisku Microsoft Windows Server,

   vi. możliwość konfiguracji za pomocą narzędzi graficznych i z linii komend,

   vii. możliwość tworzenia skryptów,

   viii. aktywne wsparcie protokołu LDAP (Lightweight Directory Access Protocol).

   Usługa Active Directory musi być realizowana w architekturze wysokiej dostępności. Awaria pojedynczego elementu infrastruktury nie może powodować utraty możliwości uwierzytelniania użytkowników, stosowania polityk domenowych ani zarządzania usługą katalogową.

i. **Aplikacja Authenticator** - Wykonawca ma obowiązek dostarczyć, zainstalować i skonfigurować aplikację typu Authenticator zapewniającą wieloskładnikowe uwierzytelnianie (MFA) dla 128 użytkowników systemów Zamawiającego.

   i. Zakres prac do zrealizowania przez Wykonawcę:

      1. instalacja i konfiguracja aplikacji dla użytkowników,
      2. integracja z istniejącymi systemami logowania,
      3. konfiguracja polityk bezpieczeństwa i zasad MFA,
      4. przeprowadzenie testów działania,

5. szkolenie administratorów i użytkowników.

ii. Aplikacja musi umożliwiać:

1. uwierzytelnianie MFA (kody jednorazowe, powiadomienia push),
2. logowanie bezhasłowe,
3. odzyskiwanie dostępu do konta,
4. obsługę kont Microsoft.

iii. Rozwiązanie musi zapewniać bezpieczne przechowywanie danych uwierzytelniających oraz umożliwiać centralne zarządzanie politykami bezpieczeństwa

j. Dodatkowe wsparcie techniczne i administracyjne

Wykonawca zapewni wsparcie techniczne i administracyjne w dni robocze w godzinach 08:00-16:00.

W ramach świadczonej usługi Wykonawca zapewni co najmniej:

1. Wsparcie w zakresie Active Directory oraz AD Connect:

- tworzenie i usuwanie kont użytkowników,

- resetowanie haseł użytkowników,

- zarządzanie grupami oraz uprawnieniami użytkowników,

- zarządzanie politykami grupowymi (GPO),

- administrację, konfigurację i utrzymanie usług Active Directory oraz AD Connect.

2. Administrowanie usługami Microsoft 365:

- Microsoft Teams,

- OneDrive,

- Exchange Online,

- zarządzanie użytkownikami i przypisanymi licencjami,

- zarządzanie domenami wykorzystywanymi przez Zamawiającego, w tym domeną tcuw.torun.pl,

- konfigurację, administrację oraz utrzymanie usług Microsoft 365.

Toruńskie Centrum Usług Wspólnych
87-100 Toruń, pl. św. Katarzyny 9, tel. +48 56 611 89 91
e-mail: sekretariat@tcuw.torun.pl, www.tcuw.torun.pl

Załącznik nr 2 do SWZ

FORMULARZ SPECYFIKACJI TECHNICZNEJ
UWAGA! Formularz składa się z ofertą

Informacja o spełnieniu wymagań dla ośrodka centrum przetwarzania danych, w ramach którego oferowana będzie usługa i w którym wykonawca będzie przetwarzał dokumenty Zamawiającego.

Lokalizacja ośrodka centrum przetwarzania danych:_____

1. Wymagania obligatoryjne dla ośrodka centrum przetwarzania danych.

Parametr	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1. Obiekt i lokalizacja		
PDC zlokalizowane na terenie UE, a wszystkie dane Zamawiającego będą gromadzone i przetwarzane wyłączenie na terenie UE lub Lichtenstainu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.	
PDC posiada ogrodzony, zamknięty teren wraz z ograniczoną strefą wejść.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji).	
PDC jest usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji) w wyniku działań działania sił natury.	
PDC jest położony niemniej niż 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania. Wysoka intensywność oddziaływania sytuacji krytycznych.	
PDC jest oddalony niemniej niż 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych dla 10	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko	

tys. osób i więcej).	zamieszek, zniszczeń.	
PDC nie posiada ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z urządzeniami serwerowymi.	Zagrożenie przecieków, zalania infrastruktury IT lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).	
PDC posiada niemniej niż 15 metrów oddalenia urządzeń serwerowych udostępnionych Zamawiającemu od źródeł pól zakłócających takich jak transformatory SN i WN.	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pól zakłócających pracę urządzeń elektrycznych i magnetycznych.	
PDC posiada podłogę techniczną w pomieszczeniu z serwerami.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.	
PDC spełnienia 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.	
2. Węzły telekomunikacyjne		
PDC posiada połączenie światłowodowe z niezależnymi operatorami telekomunikacyjnymi, w tym niemniej niż 2 operatorów o zasięgu krajowym jest podłączonych niezależnymi drogami światłowodowymi.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora zewnętrznego.	
Dojścia połączeń PDC wykonane są dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.	
PDC posiada węzeł dostępowy do sieci Internet dopięty do minimum 2	Zapewnienie niezawodności i jakości transmisji danych w ramach	

różnych operatorów z zaimplementowanym protokołem BGP oraz ochroną DDoS.	sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.	
PDC posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%.	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.	
PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.	
PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.	
3. Zasilanie energetyczne		
PDC posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż 99,999%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.	
PDC posiada niemniej niż dwie niezależne linie zasilania dostępne dla infrastruktury IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.	
PDC posiada 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.	
PDC posiada redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.	

System zasilaczy awaryjnych UPS w PDC gwarantuje podtrzymanie zasilania urządzeń serwerowych oraz infrastruktury towarzyszącej, przeznaczonej dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatów i ich 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.	
Agregaty prądotwórcze PDC posiadają 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.	
4. Bezpieczeństwo		
PDC jest wyposażone w system sygnalizacji włamania i napadu, system wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.	
PDC posiada ochronę całego obiektu realizowaną przez profesjonalną zewnętrzną licencjonowaną firmę ochrony mienia. Ochrona realizowana jest w trybie 24/7.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.	
PDC posiada system CCTV, który zapewnia ciągły 24/7 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.	

System CCTV w PDC powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres nie krótszy niż 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.	
System SKD (System Kontroli Dostępu) w PDC obejmuje niemniej niż trzy strefy dostępu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po terenie i obiekcie.	
Dostęp do strefy I (teren w otoczeniu obiektu) w PDC podlega identyfikacji na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów) wkraczających na ogrodzony teren w otoczeniu obiektu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
Dostęp do strefy II (strefa technologiczna) w PDC możliwy jest wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
Dostęp do strefy III (pomieszczenia ze sprzętem serwerowym Zamawiającego) w PDC możliwy jest wyłącznie przy użyciu łącznie 2 elementów identyfikacji: SKD, osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
PDC posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.	
PDC posiada ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków	

Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.	
5. Monitoring		
PDC posiada elektroniczny system przyjmowania zgłoszeń dotyczących awarii dostępny w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.	
PDC posiada stałe i całodobowe 24/7/365 monitorowanie poprawności pracy infrastruktury 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. PDC posiada zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Bezpieczeństwo sprzętu informatycznego:

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Izolacja sprzętu krytycznego (dedykowana przestrzeń wyłącznie dla urządzeń serwerowych)	
2	Ochrona przed uszkodzeniem infrastruktury serwerowej w postaci zamykanych szaf rack	
3	Prowadzenie rejestru wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego	
4	Ochrona przed dostępem dla osób nieupoważnionych w trybie 24/7	
5	Ochrona świadczona przez licencjonowaną firmę ochroniarską w trybie 24/7	

3. Wymagania obligatoryjne: utrzymanie i konserwacja posiadanej infrastruktury teleinformatycznej

	Zakres	Wykonawca spełnia (TAK / NIE)
1	PDC musi posiadać i stosować procedury kontroli, regularnych przeglądów zgodnie z zaleceniami producentów, konserwacji i naprawy sprzętu teleinformatycznego, energetycznego i klimatyzacyjnego.	
2	Naprawy dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami lub autoryzowane serwisy zewnętrzne	
3	Należy usuwać nośniki danych ze sprzętu teleinformatycznego przed przekazaniem do naprawy lub serwisu	
4	Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).	
5	Należy prowadzić aktualne rejestry: przeglądów, incydentów, awarii i usterek.	

Załącznik nr 3 do SWZ

Oświadczenie o braku podstaw do wykluczenia wykonawcy i spełnienia warunków udziału w postępowaniu

na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych

Przystępując do postępowania na **zapewnienie dla TCUW infrastruktury teleinformatycznej o wysokiej dostępności w modelu chmury obliczeniowej wraz z usługami towarzyszącymi**

działając w imieniu Wykonawcy:

Pełna nazwa:
Siedziba/adres:
NIP/PESEL:
REGON:
KRS/CEiDG:
Reprezentowany(a) przez (imię, nazwisko, stanowisko):

Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 i art. 109 ust. 1 pkt) 4 ustawy Prawo Zamówień Publicznych.

Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2025 r. poz. 514 ze zm.).
Oświadczam, że nie jestem wykonawcą:
a) wymienionym w wykazach określonych w rozporządzeniu 765/2006 z dnia 18 maja 2006 r. dotyczącym środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006 ze zm., dalej rozporządzenie 765/2006) i rozporządzeniu 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014 ze zm., dalej rozporządzenie 269/2014) albo wpisanym na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy;
b) którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1285, 1723 i 1843) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy;
c) którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy.

*Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Prawo Zamówień Publicznych (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub art. 109 ust.1 pkt 4 ustawy PZP). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy PZP podjąłem następujące środki naprawcze:

.....
.....

**Wykonawca wypełnia, jeżeli ma zastosowanie albo wykreśla, jeżeli nie ma zastosowania*

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w pkt 14 Specyfikacji Warunków Zamówienia.

**Stosuje tylko wykonawca/ wykonawca wspólnie ubiegający się o zamówienie, który samodzielnie wykazuje spełnienie warunków.*

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego pkt 14 Specyfikacji Warunków Zamówienia, polegam na zdolnościach lub sytuacji następującego/ych podmiotu/ów udostępniającego/ych zasoby:

.....
.....

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

w następującym zakresie:

.....
.....

(określić odpowiedni zakres udostępnianych zasobów dla wskazanego podmiotu)

**Stosuje tylko wykonawca/ wykonawca wspólnie ubiegający się o zamówienie, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, a jednocześnie samodzielnie w pewnym zakresie wykazuje spełnianie warunków.*

INFORMACJA DOTYCZĄCA CERTYFIKATU WYKONAWCY ZAMÓWIEŃ PUBLICZNYCH

Oświadczam, że w niniejszym postępowaniu będę/nie będę posługiwał się certyfikatem, o którym mowa w art. 124 ust. 2 ustawy Prawo zamówień publicznych.

(W przypadku oświadczenia o posługiwaniu się certyfikatem należy podać poniższe informacje z nim związane)

Numer i oznaczenie certyfikatu: ……

Nazwa podmiotu certyfikującego, który wydał certyfikat: …….....

Okres ważności certyfikacji wykonawcy zamówień publicznych: …….

Podstawy wykluczenia, w zakresie których wykonawca/wykonawca ubiegający się wspólnie będzie posługiwał się certyfikatem: …….....

Warunki udziału w postępowaniu, w zakresie których wykonawca/wykonawca ubiegający się wspólnie będzie posługiwał się certyfikatem: ……

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

Zgodnie z art. 63 ust. 2 ustawy Pzp oświadczenie składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Złożenie oświadczenia w formie elektronicznej to złożenie oświadczenia w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym.

Toruńskie Centrum Usług Wspólnych
87-100 Toruń, pl. św. Katarzyny 9, tel. +48 56 611 89 91
e-mail: sekretariat@tcuw.torun.pl, www.tcuw.torun.pl

Załącznik nr 4 do SWZ

Projektowane postanowienia umowy

UMOWA nr ……..

Zawarta w dniu …… w Toruniu pomiędzy:
Gminą Miasta Toruń, ul. Wały gen. Sikorskiego 8, 87-100 Toruń, NIP 879-000-10-14, działającą poprzez Toruńskie Centrum Usług Wspólnych, z siedzibą w Toruniu przy pl. św. Katarzyny 9, 87-100 Toruń,
reprezentowane przez:
……..,
zwaną dalej **Zamawiającym**
a
…….. z siedzibą w …….., ul. ……,
reprezentowaną/ym przez:
……
zwaną dalej **Wykonawcą**.
zwane dalej **Stronami.**

§1
Przedmiot Umowy

1. Przedmiotem Umowy jest świadczenie przez Wykonawcę na rzecz Zamawiającego kompleksowej usługi polegającej na dostarczeniu, wdrożeniu, utrzymaniu i administrowaniu środowiskiem chmury obliczeniowej IaaS wraz z usługami towarzyszącymi tj. usługą bezpieczeństwa, kopiami zapasowymi, przestrzenią WORM, usługami Microsoft 365 oraz dodatkowym wsparciem IT dla TCUW, zwanej dalej **Usługą.** Szczegółowy zakres Usługi został wskazany w Opisie przedmiotu zamówienia i ofercie Wykonawcy, stanowiących załączniki do niniejszej umowy.
2. W Umowie następujące pojęcia i skróty będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisane z wielkiej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:

Definicja	**Opis**
Active Directory (AD)	Usługa katalogowa (hierarchiczna baza danych) dla systemów Windows będąca implementacją protokołu LDAP.
Administrator	Osoba, zespół osób lub jednostka zajmująca się zarządzaniem systemem wirtualizacji i maszynami wirtualnymi, odpowiadająca za ich sprawne działanie i posiadająca uprawnienia dostępowe do części administracyjnych systemu.
Awaria	Nieplanowane zdarzenie powodujące całkowity brak dostępu do usługi, skutkujące przerwaniem podstawowej funkcjonalności tej usługi trwające dłużej niż 15 minut.

Backup	System kopi zapasowych danych cyfrowych.
Baza danych	Część architektury systemu, program komputerowy pozwalający na gromadzenie i zarządzanie zbiorem danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody.
PDC	Podstawowy ośrodek przetwarzania danych Primary Data Center
HA	(High Availability) – Wysoka dostępność - określenie systemu informatycznego o wysokiej niezawodności i dostępności na poziomie nie mniejszym niż SLA 99,9% czasu w skali roku, który nie posiada pojedynczego punktu awarii.
IaaS	(Infrastructure as a Service) – Infrastruktura jako usługa - infrastruktura teleinformatyczna dostarczana w modelu usługowym.
Incydent	Nieplanowane zdarzenie powodujące lub mogące powodować obniżenie jakości usługi, np. ograniczone możliwości wprowadzania zmian, edycji lub modyfikacji, ale niepowodujące przerwy w działalności podstawowej funkcjonalności.
NBD	(Next Business Day) – następny dzień roboczy od przyjętego zgłoszenia
RTO	(Recovery Time Objective) - czas w jakim należy przywrócić procesy po wystąpieniu awarii.
RPO	(Recovery Point Objective) - akceptowalny poziom utraty danych wyrażony w czasie.
SLA	(Service Level Agreement) - gwarantowany poziom świadczenia usług, wyrażony jako dostępność usług mierzona w skali roku, począwszy od dania zawarcia umowy.
VM	Maszyna wirtualna
Zamawiający	Toruńskie Centrum Usług Wspólnych

3. Szczegółowy zakres Usługi obejmuje oddanie do dyspozycji Zamawiającego zasobów informatycznych wraz z niezbędnym oprogramowaniem, udostępnionych przez Wykonawcę w modelu usługowym.
4. Wykonawca udostępni gotową Usługę **od dnia 01.01.2027 r**.
5. Wykonawca zobowiązuje się do posiadania oraz utrzymywania przez cały okres obowiązywania Umowy następujących ubezpieczeń:

1) ubezpieczenia odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej związanej z przedmiotem Umowy, na sumę gwarancyjną nie mniejszą niż 5 000 000,00 zł na jedno i wszystkie zdarzenia w okresie ubezpieczenia;
2) ubezpieczenia od ryzyk cybernetycznych (Cyber Insurance), obejmującego co najmniej odpowiedzialność za incydenty bezpieczeństwa informacji, naruszenia ochrony danych osobowych, cyberataki, nieuprawniony dostęp do systemów teleinformatycznych, utratę lub uszkodzenie danych oraz skutki przerw w świadczeniu usług teleinformatycznych.

6. Ochrona ubezpieczeniowa, o której mowa w ust. 5, musi pozostawać nieprzerwanie w mocy przez cały okres obowiązywania Umowy.
7. W przypadku gdy okres obowiązywania polisy ubezpieczeniowej upływa przed zakończeniem realizacji Umowy, Wykonawca zobowiązany jest do zachowania ciągłości ochrony ubezpieczeniowej oraz do zawarcia kolejnej umowy ubezpieczenia na warunkach nie gorszych niż określone w niniejszej Umowie.
8. Wykonawca przedłoży Zamawiającemu, na każde jego żądanie, w terminie nie dłuższym niż 7 dni od dnia otrzymania wezwania, dokumenty potwierdzające posiadanie oraz obowiązywanie wymaganych ubezpieczeń, w szczególności kopie polis wraz z potwierdzeniem opłacenia składek.
9. Nieprzedłożenie dokumentów, o których mowa w ust. 8, lub dopuszczenie do przerwy w ciągłości wymaganej ochrony ubezpieczeniowej stanowi istotne naruszenie Umowy i uprawnia Zamawiającego do naliczenia kar umownych oraz, po bezskutecznym wezwaniu do usunięcia naruszenia, do rozwiązania Umowy ze skutkiem natychmiastowym z przyczyn leżących po stronie Wykonawcy.
10. Wykonawca zobowiązuje się przez cały okres obowiązywania Umowy zapewniać świadczenie usług IaaS oraz usług kopii zapasowych z wykorzystaniem infrastruktury spełniającej wszystkie wymagania techniczne, organizacyjne i bezpieczeństwa określone w Opisie Przedmiotu Zamówienia (OPZ) dotyczące Primary Data Center (PDC).
11. Wymagania określone dla PDC w OPZ mają charakter obligatoryjny i muszą być spełnione łącznie przez cały okres realizacji Umowy. Niedopuszczalne jest częściowe spełnienie któregokolwiek z wymagań.
12. W przypadku utraty zgodności infrastruktury z wymaganiami określonymi w OPZ Wykonawca zobowiązany jest niezwłocznie, nie później niż w terminie 3 dni roboczych od powzięcia informacji o takim zdarzeniu, poinformować o tym Zamawiającego oraz przedstawić plan i termin przywrócenia zgodności.
13. Zamawiający jest uprawniony na każdym etapie realizacji Umowy do weryfikacji spełniania przez Wykonawcę wymagań dotyczących PDC. W tym celu Zamawiający może wezwać Wykonawcę do przedstawienia, w terminie nie krótszym niż 5 dni roboczych, dokumentów, certyfikatów, raportów audytowych, oświadczeń lub innych dowodów potwierdzających spełnianie wymagań określonych w OPZ.
14. Niezależnie od dokumentów, o których mowa w pkt. 13 powyżej, Zamawiający może żądać dodatkowych wyjaśnień dotyczących spełniania wymagań przez centrum danych

wykorzystywane do realizacji Umowy, a Wykonawca zobowiązany jest do ich udzielenia w wyznaczonym terminie.

15. Stwierdzenie niespełniania któregokolwiek z wymagań określonych dla PDC stanowi nienależyte wykonanie Umowy i uprawnia Zamawiającego do zastosowania środków przewidzianych Umową, w szczególności naliczenia kar umownych lub rozwiązania Umowy z przyczyn leżących po stronie Wykonawcy, po bezskutecznym upływie wyznaczonego terminu na usunięcie niezgodności.

§2
Komunikacja

1. Wszelkie komunikaty, informacje i dokumentacje związaną z realizacją zawartej Umowy Strony będą przekazywały sobie drogą elektroniczną na adresy email wskazane poniżej, chyba że Strony postanowiły w treści Umowy inaczej.
   a) Wykonawca wyznacza adresy email: _____
   b) Zamawiający wyznacza adresy email: _____
2. Każda ze Stron zobowiązana jest do poinformowania drugiej Strony o zmianie danych kontaktowych, pod rygorem uznania komunikatów, zamówień, informacji i dokumentów przekazanych zgodnie z dotychczasowymi danymi za skutecznie doręczone.
3. Zmiana adresów email, o których mowa w ust. 1, powyżej nie wymaga aneksu do Umowy i odbywa się poprzez pisemne poinformowanie drugiej Strony.

§3
Wynagrodzenie

1. W zamian za świadczenie Usługi na zasadach określonych w niniejszej Umowie Zamawiający zobowiązuje się do zapłaty na rzecz Wykonawcy łącznego wynagrodzenia w wysokości brutto _____ złotych (słownie: _____). Jest to wynagrodzenie całkowite i maksymalne, które pozostanie niezmienne przez cały okres świadczenia Usługi.
2. Płatność zrealizowana będzie kwartalnie w terminie 14 dni po zakończeniu każdego kwartału trwania umowy i będzie wynosiła sumę wynagrodzenia, o którym mowa w ust. 1 podzieloną przez ilość wszystkich kwartałów w czasie obowiązywania umowy.
3. Płatność Wynagrodzenia, o którym mowa w ust.2 nastąpi na podstawie prawidłowo wystawionej i doręczonej Zamawiającemu faktury Vat.
4. Za dzień dokonania zapłaty Strony uznają dzień, w którym zostanie obciążony rachunek bankowy Zamawiającego.
5. Wykonawca zobowiązuje się wystawiać faktury wyłącznie w formie faktur ustrukturyzowanych za pośrednictwem KSeF, zgodnie z obowiązującymi przepisami prawa. Strony zgodnie postanawiają, że – z zastrzeżeniem wyjątków przewidzianych w powszechnie obowiązujących przepisach (np. awaria KSeF) – wyłącznie faktura wystawiona przez Wykonawcę i

zarejestrowana w KSeF (tj. opatrzona identyfikującym ją numerem KSeF) będzie uznawana za prawidłowo wystawioną i wywołującą skutki w zakresie płatności.

6. Wykonawca, poza przesłaniem faktury do KSeF, prześle Zamawiającemu w terminie 2 dni roboczych licząc od dnia wystawienia faktury ustrukturyzowanej wizualizację faktury w formacie PDF na adres e-mail: przetargi@tcuw.torun.pl. Wizualizacja powinna zawierać numer identyfikacyjny faktury nadany w KSeF oraz być opatrzona stosownym kodem QR. Strony zgodnie potwierdzają, że przesłana wizualizacja ma charakter wyłącznie informacyjno-pomocniczy i nie wywołuje żadnych skutków prawnych, w szczególności nie stanowi skutecznego doręczenia faktury, ani nie wywołuje skutków w zakresie biegu terminu płatności. Jedynie faktura udostępniona Zamawiającemu w KSeF stanowi podstawę płatności.
7. Faktura, poza elementami wymaganymi przepisami ustawy o VAT, musi zawierać następujące informacje niezbędne Zamawiającemu: (a) w części dotyczącej nabywcy – dopisek Odbiorca: Toruńskie Centrum Usług Wspólnych; (b) numer zamówienia 45/2026. Wykonawca zobowiązuje się umieścić powyższe dane w odpowiednich polach faktury ustrukturyzowanej (np. NrUmowy, NrZamowienia lub w polu opisowym faktury), tak aby były one widoczne na wizualizacji faktury.
8. Wszelkie dokumenty, które zgodnie z niniejszą umową mają zostać dołączone do faktury Wykonawca przekaże Zamawiającemu drogą elektroniczną wraz z wizualizacją faktury (PDF), na adres e-mail przetargi@tcuw.torun.pl, w terminie 2 dni od wystawienia faktury w KSeF. W tytule wiadomości lub treści albo nazwach plików stanowiących załączniki do faktury, Wykonawca wskaże nadany przez siebie numer faktury oraz identyfikator KSeF – celem jednoznacznego powiązania załączników z przedmiotową fakturą. Strony zgodnie postanawiają, że ze względu na ograniczenia KSeF załączniki nie będą przesyłane poprzez system KSeF, lecz w opisany wyżej sposób.
9. Brak zgłoszenia zastrzeżeń przez Zamawiającego w terminie 3 dni od otrzymania wizualizacji faktury, o której mowa w pkt 6 powyżej, oznacza akceptację treści faktury. W przypadku zgłoszenia uzasadnionych zastrzeżeń co do treści faktury (w szczególności w razie stwierdzenia wad świadczenia, błędnych pozycji lub kwot) – bieg terminu płatności ulega wstrzymaniu do czasu dostarczenia Zamawiającemu faktury korygującej uwzględniającej zgłoszone uwagi. Wykonawca zobowiązany jest wystawić fakturę korygującą w KSeF w terminie 2 dni od otrzymania zastrzeżeń Zamawiającego.
10. Wykonawca ponosi odpowiedzialność za poprawność i kompletność danych zawartych na fakturze ustrukturyzowanej przekazanej do KSeF, w szczególności za zgodność tych danych ze stanem faktycznym i postanowieniami umowy. W przypadku wystawienia faktury niezgodnej z umową lub z przepisami (w tym wadliwie wypełnionej struktury e-faktury), Wykonawca zobowiązuje się do niezwłocznego skorygowania lub ponownego wystawienia faktury zgodnie z obowiązującymi przepisami. Zamawiający nie odpowiada za opóźnienie płatności spowodowane wadliwością faktury leżącą po stronie Wykonawcy.
11. W przypadku niedostępności KSeF lub innej awarii uniemożliwiającej wystawienie faktury ustrukturyzowanej w systemie, Wykonawca niezwłocznie poinformuje o tym Zamawiającego. W okresie awarii Wykonawca wystawi fakturę w postaci elektronicznej poza KSeF (spełniającą wymagania art. 106nf ustawy o VAT, w szczególności zawierającą kod weryfikacyjny) i doręczy

ją Zamawiającemu na adres e-mail: przetargi@tcuw.torun.pl. W okresie trwania niedostępności KSeF Wykonawca wystawi fakturę w postaci elektronicznej (spełniającą wymagania art. 106nh ustawy o VAT, w szczególności zawierającą kod weryfikacyjny) i doręczy ją Zamawiającemu na adres e-mail: przetargi@tcuw.torun.pl. Po ustaniu awarii lub innej niedostępności KSeF Wykonawca prześle tę fakturę do KSeF niepóźniej niż w terminie 7 dni roboczych od dnia zakończenia awarii, a w przypadku niedostępności KSeF niepóźniej niż w następnym dniu roboczym (chyba że w tym terminie: wystąpi awaria – wówczas fakturę przesyła się w terminie 7 dni roboczych od zakończenia awarii; wystąpi awaria całkowita ogłaszana w środkach społecznego przekazu przez uprawnione do tego podmioty – wówczas faktury nie przesyła się do KSeF), celem nadania jej numeru identyfikacyjnego KSeF. Strony zgodnie postanawiają, że termin płatności takiej faktury rozpoczyna bieg od dnia nadania fakturze numeru KSeF (doręczenia w KSeF), chyba że przepisy prawa będą bezwzględnie stanowić inaczej. Niezależnie od powyższego, Zamawiający uprawniony jest wstrzymać płatność za fakturę wystawioną w trybie awaryjnym, jeżeli Wykonawca nie dopełni obowiązku przesłania jej do KSeF po ustaniu awarii w wyżej wskazanym terminie.

12. Zamawiający nie ponosi odpowiedzialności za skutki wynikające z awarii lub niedostępności systemu KSeF lub inne okoliczności niezależne od 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 Usługi.
3. Zamawiający w szczególności nie może korzystać z Usługi w celu:
    a. celowego powodowania przeciążenia, przepełniania, blokowania lub natłoku w sieci Internet, innych sieciach transmisji danych lub zasobach Wykonawcy;
    b. 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 najwyższą starannością. W szczególności zobowiązuje się zapewnić, aby Usługi były dostępne dla Zamawiającego w sposób ciągły, a elektroniczne dokumenty logiczne były należycie zabezpieczone w szczególności przed uszkodzeniem, utratą, ujawnieniem osobom nieuprawnionym.
5. Wykonawca zobowiązuje się do współpracy z Zamawiającym w celu dokonania rekonfiguracji dostarczonych usług i infrastruktury teleinformatycznej na potrzeby instalacji nowych aplikacji i serwisów Zamawiającego.

6. Wykonawca w ramach zapewnienia dostępności Usługi zobowiązuje się do utrzymywania prawidłowego działania i sprawności urządzeń i zasobów w ramach sieci Wykonawcy oraz prawidłowego działania Usługi.
7. Wykonawca zapewnia Zamawiającemu dostępność Usługi na poziomie SLA: .....% w skali roku podczas trwania Umowy.
8. Po zakończeniu Umowy Wykonawca zapewnia Zamawiającemu Gwarancję dostępności do danych cyfrowych zapisanych w infrastrukturze Wykonawcy przez okres 30 dni. Strony wspólnie definiują, że po upływie Gwarancji dostępności wszystkie dane zostaną trwale usunięte z przestrzeni dyskowej Wykonawcy.
9. 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 60 minut jednorazowo i łącznie 120 minut w miesiącu. Planowe przerwy na prace techniczne nie są wliczane do czasu niedostępności usługi SLA, o ile o planowanych przerwach na prace techniczne Wykonawca poinformuje Zamawiającego pocztą elektroniczną e-mail wraz z przewidywanym czasem zakończenia przerwy nie później niż na 48h przed planowaną przerwą, a Zamawiający wyrazi na to zgodę.
10. Dostęp do urządzeń, systemów oraz oprogramowania w ramach świadczonej usługi uzyskiwać będą wyznaczeni pracownicy Wykonawcy oraz pracownicy serwisu zewnętrznego pod nadzorem Wykonawcy.
11. Wykonawca nie sprawdza, nie rozpowszechnia, ani też w żaden sposób nie wykorzystuje treści danych przechowywanych lub przesyłanych przez Zamawiającego.
12. Na każde żądanie Zamawiającego Wykonawca w terminie 1 dnia roboczego od otrzymania żądania umożliwi Zamawiającemu pobrania kopii wszystkich danych cyfrowych Zamawiającego znajdujących się w infrastrukturze Wykonawcy.
13. Zamawiający ma prawo do przeprowadzenia testowego odtworzenia danych na każde wezwanie.
14. Wykonawca obowiązany jest do samodzielnego wykonywania przedmiotu Umowy i nie jest uprawniony do powierzania jej realizacji innym podmiotom bez uprzedniej pisemnej (pod rygorem nieważności) zgody Zamawiającego.

§ 5
Odpowiedzialność Stron

1. Wykonawca ponosi na podstawie Umowy pełną odpowiedzialność odszkodowawczą wobec Zamawiającego za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy.
2. Zamawiający jest zobowiązany do należytego zabezpieczenia własnych danych dostępu do indywidualnych kont użytkowników udostępnionych przez Wykonawcę. Zamawiający ponosi

odpowiedzialność za skutki wyłącznie świadomego udostępnienia danych dostępu osobom niepowołanym.

3. Wykonawca nie ponosi odpowiedzialności za ewentualne szkody spowodowane:
   a) okolicznościami wynikającymi z wyłącznej winy osób trzecich lub Zamawiającego, w szczególności naruszeniem przez Zamawiającego postanowień Umowy;
   b) działaniem nielegalnego oprogramowania zainstalowanego przez Zamawiającego;
   c) działaniem wirusów komputerowych lub złośliwym działaniem osób trzecich, jeżeli wykaże, że działając z najwyższą starannością, właściwą zawodowemu charakterowi świadczonych usług, nie był w stanie zapobiec ich zaistnieniu lub skutkom.

4. W przypadku, gdy z tytułu niewykonania lub nienależytego wykonania przez Wykonawcę, z przyczyn leżących po jego stronie, zobowiązań wynikających z postanowień niniejszej Umowy, zostanie zasądzone prawomocnym wyrokiem sądu od Zamawiającego na rzecz jakiejkolwiek osoby trzeciej odszkodowanie, Wykonawca zobowiązuje się pokryć wszelkie straty poniesione przez Zamawiającego w związku zaspokojeniem roszczeń takiej osoby, w szczególności łącznie z odsetkami i kosztami sądowymi, w terminie 7 (siedmiu) dni roboczych od daty otrzymania wezwania do zapłaty od Zamawiającego.
5. Zamawiający niezwłocznie powiadomi Wykonawcę o zgłoszonym przeciwko Zamawiającemu roszczeniu, wynikającym ze zdarzeń, o których mowa w ust.4 powyżej, a Wykonawca bez zbędnej zwłoki przekaże Zamawiającemu pisemne stanowisko dotyczące zasadności zgłoszonego roszczenia. W przypadku postępowania sądowego Zamawiający podejmie stosowne czynności zmierzające do umożliwienia Wykonawcy wzięcia udziału w tym postępowaniu i na zasadach określonych w obowiązujących przepisach prawa.

§ 6
Prawa autorskie

1. Wykonawca oświadcza i zapewnia, iż posiada majątkowe prawa autorskie oraz odpowiednie licencje do korzystania z oprogramowania w celu świadczenia Usługi dla Zamawiającego.
2. O ile jest to konieczne dla prawidłowego świadczenia Usługi, Wykonawca udzieli Zamawiającemu niewyłącznej i nieprzenaszalnej licencji/sublicencji na korzystanie z oprogramowania, w zakresie niezbędnym do korzystania z Usługi zgodnie z jej przeznaczeniem.

§ 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 powyżej lub ich procesorem. Wykonawca nie decyduje o celach i środkach przetwarzania tych danych osobowych, a jedynie udostępnia w ramach świadczenia Usługi zasoby pozwalające na

przechowywanie danych. Wykonawca stosuje środki techniczne i organizacyjne zapewniające ochronę danych przechowywanych i przetwarzanych przez Zamawiającego zgodnie z odpowiednimi, obowiązującymi przepisami o ochronie danych osobowych.

3. Wykonawca oświadcza, że serwery, za pomocą których świadczone są Usługi będące przedmiotem Umowy znajdują się na terenie Unii Europejskiej a przechowywane dane w żadnym przypadku w toku świadczenia Usługi nie są przesyłane poza obszar Unii Europejskiej.
4. O ile będzie to konieczne dla prawidłowego świadczenia Usługi Strony zawrą odrębną umowę o powierzeniu przetwarzania danych osobowych najpóźniej w dniu rozpoczęcia świadczenia Usługi będącej przedmiotem niniejszej Umowy.

§ 8
Wsparcie techniczne

1. Obsługa utrzymania i zarządzania oferowanego rozwiązania musi być realizowana w trybie 24/7/365.
2. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w sposób autoryzowany w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status, wraz z historią wszystkich zgłoszeń.
3. Czas reakcji na zgłoszenie musi wynosić nie więcej niż 15 minut od przyjęcia zgłoszenia.
4. Czas usunięcia Awarii musi wynosić do 6 godzin od przyjęcia zgłoszenia.
5. Czas usunięcia Incydentu musi wynosić do 24 godzin od przyjęcia zgłoszenia.
6. Zamawiający zgłasza awarie i incydenty za pomocą indywidualnego konta użytkownika w systemie Wykonawcy dostępnym pod adresem www …….. lub pocztą elektroniczną wyłącznie z użyciem adresów email wskazanych w § 2 ust. 1 lit. a).
7. Jeżeli w wyniku analizy zgłoszenia nie zostanie potwierdzone istnienie awarii lub incydentu lub jeśli ustalona przyczyna awarii lub incydentu nie wynika z okoliczności, za które odpowiedzialność ponosi Wykonawca, Wykonawca powiadomi Zamawiającego o braku podstaw do interwencji.
8. Jeżeli w wyniku analizy zgłoszenia zostanie ustalona przyczyna awarii lub incydentu mieszcząca się w zakresie odpowiedzialności Wykonawcy, Wykonawca niezwłocznie przystąpi do usuwania awarii lub incydentu.

§ 9
Ochrona Informacji Poufnych

1. Strony zobowiązują się do zachowania ścisłej poufności polegającej na tym, iż nie ujawnią żadnej nieuprawnionej osobie trzeciej Informacji Poufnych. 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 Umowy 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 prowadzoną przez Strony z 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 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 Umowy na zgodnie z obowiązującymi przepisami o ochronie danych osobowych..
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 będących przedmiotem Umowy.
4. Strona Otrzymująca zachowa Informacje Poufne Strony Ujawniającej w tajemnicy i w stosunku do nich podejmie co najmniej takie same środki ostrożności, oraz co najmniej takie same środki zabezpieczające, jak te stosowane przez Stronę Otrzymującą w stosunku do jej własnych Informacji Poufnych, 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.. Wszelkie Informacje Poufne oraz ich kopie zostaną zwrócone Stronie Ujawniającej w ciągu trzydziestu dni od otrzymania pisemnego żądania od Strony Ujawniającej.
5. Obowiązek zachowania poufności nie dotyczy Informacji Poufnych:
   a) których ujawnienia wymagają bezwzględnie obowiązujące przepisy prawa;
   b) których ujawnienie następuje na żądanie podmiotu uprawnionego 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) w których posiadanie Strona weszła zgodnie z obowiązującymi przepisami prawa, przed dniem uzyskania takich informacji na podstawie Umowy;

e) 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;

f) 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.

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 2 lat po jej wygaśnięciu lub rozwiązaniu- dotyczy Zamawiającego, a bezterminowo po jej wygaśnięciu lub rozwiązaniu w przypadku Wykonawcy.

§ 10
Kary umowne

1. W przypadku wystąpienia przerw w dostępności Usługi, których łączny czas spowoduje spadek dostępności Usługi poniżej gwarantowanego poziomu SLA, o którym mowa w §4 ust. 7 umowy, Zamawiający jest uprawniony do naliczenia kary umownej w wysokości 1 000,00 zł za każdy rozpoczęty 1% niedostępności Usługi poniżej gwarantowanego poziomu SLA, o którym mowa powyżej.
2. W przypadku dopuszczenia do przerwy w ciągłości któregokolwiek z ubezpieczeń wymaganych Umową, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 3 000 zł za każdy rozpoczęty dzień pozostawania bez wymaganej ochrony ubezpieczeniowej.
3. W przypadku stwierdzenia niespełniania przez PDC któregokolwiek z wymagań określonych w OPZ, Zamawiający naliczy Wykonawcy karę umowną w wysokości 2 000 zł za każdy rozpoczęty dzień utrzymywania się niezgodności, licząc od dnia stwierdzenia niezgodności lub upływu terminu wyznaczonego na jej usunięcie.
4. W przypadku nieprzedłożenia przez Wykonawcę, w terminie wyznaczonym przez Zamawiającego, dokumentów lub wyjaśnień potwierdzających spełnianie wymagań dotyczących PDC, Zamawiający naliczy karę umowną w wysokości 1 000 zł za każdy rozpoczęty dzień zwłoki.
5. Maksymalna wysokość kar wynosi do 30% wartości wynagrodzenia, o którym mowa w §3 ust. 1 Umowy.
6. 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.

7. Niezależnie od postanowień powyższych Zamawiający jest uprawniony do dochodzenia odszkodowania przewyższającego zastrzeżone kary umowne na zasadach ogólnych do wartości rzeczywiście poniesionej szkody z wyłączeniem utraconych korzyści.

§ 11
Ograniczenie, zawieszenie Usług, Reklamacje

1. Reklamacje Zamawiającego w związku z niewykonaniem lub nienależytym wykonaniem Usługi powinny być przesyłane w formie pisemnej i określać:
   a) zarzuty Zamawiającego i okoliczności uzasadniające reklamację,
   b) ewentualny proponowany sposób rozstrzygnięcia reklamacji.
2. Wykonawca udzieli odpowiedzi na reklamację w terminie 14 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.

§ 12
Okres obowiązywania Umowy

1. Niniejsza Umowa została zawarta na czas określony od dnia **01.01.2027** do dnia **31.12.2028** roku.
2. Wykonawca ma prawo do natychmiastowego zaprzestania świadczenia Usługi oraz do wypowiedzenia Umowy bez zachowania okresu wypowiedzenia, jeżeli pomimo zawiadomienia Zamawiającego o dostrzeżonych nieprawidłowościach i udzielenia odpowiedniego, nie krótszego niż 7 dni, terminu na ich usunięcia Zamawiający nadal narusza przepisy prawa lub istotne postanowienia Umowy;
3. Zamawiający ma prawo wypowiedzenia Umowy bez zachowania okresu wypowiedzenia, jeżeli pomimo zawiadomienia Wykonawcy o dostrzeżonych nieprawidłowościach i udzielenia odpowiedniego, nie krótszego niż 7 dni, terminu na ich usunięcie Wykonawca nadal narusza przepisy prawa lub istotne postanowienia Umowy.
4. 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. Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.
5. W przypadku odstąpienia od umowy Wykonawca może żądać wynagrodzenia jedynie za część umowy wykonaną do dnia ustania obowiązywania umowy.
6. Oświadczenie o odstąpieniu, wypowiedzeniu lub rozwiązaniu Umowy powinno zostać złożone na piśmie pod rygorem nieważności.

§ 13

Postanowienia końcowe

1. Zmiany w umowie wymagają formy pisemnej pod rygorem nieważności. **Zamawiający** przewiduje możliwość zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru **Wykonawcy**, w przypadku wystąpienia co najmniej jednej z poniższych okoliczności:
   a) siła wyższa uniemożliwiająca wykonanie przedmiotu umowy,
   b) zmiany organizacyjno-prawne lub zmiana lokalizacji **Zamawiającego**, niezależnej od **Zamawiającego,**
   c) konieczność rezygnacji z części przedmiotu zamówienia np. w przypadku braku środków finansowych na kontynuowanie umowy czy też zmiany obowiązującego prawa.
2. Zamawiający przewiduje zmiany umowy oraz waloryzację wynagrodzenia Wykonawcy również w przypadkach i na zasadach opisanych w pkt. 43 SWZ.
3. Prawem właściwym dla zobowiązań wynikających z Umowy jest prawo polskie.
4. Wszelkie spory wynikające z Umowy będą rozstrzygane przez sąd powszechny właściwy miejscowo dla Zamawiającego. Strony zobowiązują się w każdym przypadku dążyć do ugodowego rozstrzygnięcia sporu powstałego na gruncie stosowania niniejszej Umowy.
5. Wszelkie zawiadomienia i oświadczenia związane z Umową 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.
6. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy Kodeksu cywilnego i ustawy Prawo Zamówień Publicznych.
7. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Wykonawca	**Zamawiający**

Załączniki:
nr 1 - Szczegółowy Opis Przedmiotu Zamówienia
nr 2 - Oferta Wykonawcy wraz z załącznikami
nr 3 – Klauzula informacyjna CRU

Toruńskie Centrum Usług Wspólnych
87-100 Toruń, pl. św. Katarzyny 9, tel. +48 56 611 89 91
e-mail: sekretariat@tcuw.torun.pl, www.tcuw.torun.pl

Załącznik nr 3 - do umowy

Klauzula informacyjna dotycząca przetwarzania danych osobowych w Centralnym Rejestrze Umów dla Wykonawców, z którymi zawarto umowę w wyniku postępowania będącymi osobami fizycznymi

Wykonując obowiązek wynikający z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE. L. z 2016 r., poz. 119) – dalej: ogólne rozporządzenie o ochronie danych, informujemy, że:

1. Administratorem danych osobowych udostępnianych w Centralnym Rejestrze Umów JSFP (dalej: CRU) jest: Gmina Miasta Toruń działająca przez Toruńskie Centrum Usług Wspólnych z siedzibą w Toruniu przy pl. Św. Katarzyny 9, tel. 56 611 89 81, zwany dalej administratorem.
2. Administrator wyznaczył inspektora ochrony danych, z którym można skontaktować się z wykorzystaniem następujących danych kontaktowych: Plac św. Katarzyny 9, 87-100 Toruń, e-mail: iod@tcuw.torun.pl.
3. Dane osobowe będą przetwarzane w celu udostępniania i aktualizacji w CRU informacji o umowach zawartych przez jednostkę sektora finansów publicznych lub na jej rzecz.
Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit c ogólnego rozporządzenia o ochronie danych (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) w zw. z art. 34a ust. 1 ustawy z 27.08.2009 r. o finansach publicznych (Dz.U. z 2025 r., poz. 1483 ze zm.),
4. Dane osobowe będą udostępniane podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa. Dane będą udostępniane Ministrowi Finansów prowadzącemu CRU. Dane osobowe udostępniane i aktualizowane w CRU, który jest rejestrem jawnym i dostępnym w Internecie, będą jawne i powszechnie dostępne.
5. Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
6. Dane osobowe będą przechowywane w CRU przez okres pięciu lat, licząc od końca roku, w którym umowa zawarta z administratorem przestała obowiązywać. Po upływie tego okresu dane będą usuwane z CRU.
7. Przysługuje Pani/Panu prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, zgodnie z przepisami ogólnego rozporządzenia o ochronie danych.
8. Przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli sądzi Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza ogólne rozporządzenie o ochronie danych.
9. Podanie Pani/Pana danych osobowych (jako strony umowy będącej osobą fizyczną) jest niezbędne do zawarcia i wykonania umowy, z czym wiąże się obowiązek udostępniania i aktualizacji informacji o umowie w CRU. Konsekwencją niepodania danych jest brak możliwości zawarcia umowy.
10. Pani/Pana dane osobowe nie będą wykorzystywane do podejmowania zautomatyzowanych decyzji ani profilowania.

Toruńskie Centrum Usług Wspólnych
87-100 Toruń, pl. św. Katarzyny 9, tel. +48 56 611 89 91
e-mail: sekretariat@tcuw.torun.pl, www.tcuw.torun.pl

Załącznik nr 5 do SWZ
Oświadczenie o przynależności do grupy kapitałowej

Dane Wykonawcy:

Nazwa: .....
Siedziba i adres: .....
Numer telefonu: .....
Numer REGON:.....
Numer NIP:.....

O Ś W I A D C Z E N I E

My, niżej podpisani

.....
(osoba reprezentująca wykonawcę)

działając w imieniu

.....
(nazwa wykonawcy)

Oświadczamy, że Wykonawca.....

(* niewłaściwe skreślić)

*** nie przynależę** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2025 r. poz. 1714 z późn. zm.), o której mowa w art. 108 ust. 1 pkt 5 i 6 ustawy PZP **z innymi wykonawcami**, którzy złożyli odrębne oferty w niniejszym Postępowaniu o udzielenia zamówienia.

*** przynależę** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2025 r. poz. 1714 z późn. zm.), o której mowa w art. 108 ust. 1 pkt 5 i 6 ustawy PZP z następującymi **wykonawcami**, którzy złożyli odrębne oferty w niniejszym postępowaniu o udzielenia zamówienia:

.....

Przedstawiam w załączeniu następujące dokumenty lub informacje potwierdzające, że przygotowanie oferty nastąpiło niezależnie od ww. wykonawcy/wykonawców oraz że powiązania z ww. wykonawcą/wykonawcami nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie niniejszego zamówienia:

.....

Toruńskie Centrum Usług Wspólnych
87-100 Toruń, pl. św. Katarzyny 9, tel. +48 56 611 89 91
e-mail: sekretariat@tcuw.torun.pl, www.tcuw.torun.pl

Załącznik nr 6 do SWZ
Oświadczenie składane na wezwanie Zamawiającego

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko /podstawa do reprezentacji)

Oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych w zakresie podstaw wykluczenia z postępowania

Na potrzeby postępowania o udzielenie zamówienia publicznego:

nr 45/2026 Postępowanie na: Zapewnienie dla TCUW infrastruktury teleinformatycznej o wysokiej dostępności w modelu chmury obliczeniowej wraz z usługami towarzyszącymi

Oświadczam, że podane informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp w zakresie podstaw wykluczenia z postępowania **są aktualne.**

……
(elektroniczny podpis osoby uprawnionej do reprezentowania Wykonawcy)