



Wykonanie usługi konfiguracji, zabezpieczenia i obsługi informatycznej jednostek oświatowych obsługiwanych przez TCUW, w zakresie hostingu i dostępu do poczty elektronicznej

Gmina Miasta Toruń z siedzibą w Toruniu, ul. Wały gen. Sikorskiego 8, posiadająca NIP 879-000-10-14, działająca poprzez Toruńskie Centrum Usług Wspólnych, plac św. Katarzyny 9, 87-100 Toruń, zaprasza w formie Zapytania Ofertowego do złożenia oferty w postępowaniu o udzielenie zamówienia o wartości mniejszej niż 130.000 zł.

KOD CPV:

72412000-1 Dostawcy usług poczty elektronicznej

72417000 - Nazwy domen internetowych

I. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest usługa konfiguracji, zabezpieczenia i obsługi informatycznej jednostek oświatowych obsługiwanych przez Zamawiającego, w zakresie hostingu i dostępu do poczty elektronicznej.

Wykonawca będzie oferował usługi w oparciu o własne zasoby osobowe oraz własną infrastrukturę technologiczną ośrodka centrum przetwarzania danych zlokalizowanego na terytorium Unii Europejskiej lub Lichtensteinu, Islandii, Norwegii zgodnie z określonymi przez Zamawiającego wymaganiami.

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

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

II. Termin świadczenia usługi

Od dnia podpisania umowy przez okres 12 miesięcy zgodnie z terminami określonymi w opisie przedmiotu zamówienia.

III. Miejsce i termin składania ofert

Wykonawca może złożyć tylko jedną ofertę w jednej z podanych form: w sekretariacie TCUW, pl. Św. Katarzyny 9, 87-100 Toruń, na adres e-mail sekretariat@tcuw.torun.pl lub przesłać na adres Toruńskie Centrum Usług Wspólnych, pl. św. Katarzyny 9, 87-100 Toruń. Oferty prosimy składać w terminie do **31.10.2022 r. do godz. 10:00**.

III. Sposób obliczania ceny

1. Wykonawca poda cenę netto i brutto oferty w Formularzu Ofertowym, sporządzonym według wzoru stanowiącego Załącznik Nr 1.
2. Wykonawca poda cenę za całość usługi.
3. Ceny muszą być wyrażone w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca musi uwzględnić w cenie oferty wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania zamówienia oraz wszelkie opłaty i podatki wynikające z obowiązujących przepisów. Cena musi zawierać



Zamówienie publiczne nr 15/2022

wszystkie koszty przygotowania i złożenia oferty, a także koszty świadczenie usługi przez okres wskazany w przedmiocie zamówienia.

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

IV. Badanie ofert

1. Niespełnienie lub niewykazanie spełnienia któregośkolwiek warunku lub braku podstaw do wykluczenia będzie przyczyną wykluczenia Wykonawcy i uznania jego oferty za odrzuconą.
2. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert. Zamawiający zastrzega możliwość weryfikacji i wizytacji wskazanego w ofercie ośrodka centrum przetwarzania danych, w tym złożenia dowodów dotyczących spełnienia wskazanych w zapytaniu wymagań.
3. Zamawiający w celu ustalenia, czy oferta zawiera rażąco niską cenę lub części składowe ceny wydają się rażąco niskie w stosunku do przedmiotu zamówienia, zwróci się do wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Zamawiający zwraca się o wyjaśnienia w szczególności w przypadku, gdy cena całkowita oferty jest niższa o co najmniej 30% od:
 - a) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania lub średniej arytmetycznej cen wszystkich złożonych ofert, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia.
 - b) wartości zamówienia powiększonej o należny podatek od towarów i usług, zaktualizowanej z uwzględnieniem okoliczności, które nastąpiły po wszczęciu postępowania, w szczególności istotnej zmiany cen rynkowych.

Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na Wykonawcy. Zamawiający odrzuca ofertę Wykonawcy, który nie udzielił wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.

4. Zamawiający poprawi w ofercie:
 - a) oczywiste omyłki pisarskie,
 - b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
 - c) inne omyłki polegające na niezgodności oferty z SWZ, niepowodujące istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.

W przypadku, o którym mowa w zdaniu poprzedzającym lit. c) powyżej, Zamawiający wyznacza wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.

5. Zamawiający zastrzega sobie, że może najpierw dokonać oceny ofert, a następnie zbadać, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

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



Zamówienie publiczne nr 15/2022

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

Lp.	Nazwa kryterium	Waga kryterium (w %)
1	Cena netto za całość usługi	60
2	Ośrodek przetwarzania danych	30
3	Dostępność usługi – SLA	10

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

$$\frac{\text{oferty najtańszej}}{\text{oferty badanej}} \times 60 = \text{LP}$$

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

4. Punkty za kryterium „Ośrodek przetwarzania danych” zostaną przyznane w skali punktowej od 0 do 30 pkt, wg poniższej zasady:
- Posiadany aktualny certyfikat ISO 27001 na usługi cloud computing: 5 pkt
 - Posiadany aktualny certyfikat ISO 27017 na usługi cloud computing: 5 pkt
 - Posiadany aktualny certyfikat ISO 22301 na usługi cloud computing: 5 pkt
 - Posiadany aktualny certyfikat ANSI-TIA RATED 3: 5 pkt
 - Posiadany certyfikat TIER III dokumentacji centrum przetwarzania danych: 5 pkt
 - Posiadany certyfikat TIER III infrastruktury centrum przetwarzania danych: 5 pkt
5. Punkty za kryterium „Dostępność usługi – SLA” zostaną przyznane w skali punktowej do 10 pkt. wg poniższej zasady ramach:
- Gwarancja dostępności usługi poniżej 99,99% SLA w skali roku – 0 pkt
 - Gwarancja dostępności usługi 99,99% i powyżej SLA w skali roku – 10 pkt
6. Liczby punktów, o których mowa w pkt 3 do 5 po zsumowaniu stanowić będą końcową ocenę oferty.
7. Za najkorzystniejszą zostanie uznana oferta z największą liczbą punktów, tj. przedstawiająca najkorzystniejszy bilans kryteriów oceny ofert.
8. Zamawiający nie dopuszcza składania ofert wariantowych.

VI. Warunki udziału w postępowaniu

1. Wykonawca musi być zarejestrowanym operatorem telekomunikacyjnym nie krócej niż 3 lata od dnia złożenia oferty. Warunek zostanie oceniony na podstawie złożonych dokumentów w postaci potwierdzenia wpisu do właściwego rejestru.



Zamówienie publiczne nr 15/2022

2. Wykonawca musi dysponować ośrodkiem danych, z którego będzie świadczona usługa, spełniającym wymagania określone w części VIII.

VII. Opis przedmiotu zamówienia

Zakres prac do wykonania przez Wykonawcę

1. Wykonawca zobowiązany jest:
 - a. w terminie do 2 dni roboczych od zawarcia umowy:
 - i. powołać dla 69 jednostek obsługiwanych przez Zamawiającego indywidualne domeny internetowe o ustandaryzowanym adresie i nazwie (w konsultacji z Zamawiającym na etapie realizacji) dla poszczególnych grup wskazanych przez Zamawiającego;
 - ii. przygotować i przeprowadzić konfigurację serwerów DNS, kierując ruch z nowo powołanych domen internetowych na wskazane przez Zamawiającego adresy internetowe;
 - iii. przygotować i zabezpieczyć odpowiednią infrastrukturę teleinformatyczną, zabezpieczającą prawidłowe i bezprzerwowe działanie nowo skonfigurowanego przekierowania adresów internetowych. Wykonawca musi zapewnić środowisko wirtualne oraz oprogramowanie systemowe i narzędziowe niezbędne do prawidłowej i bezprzerwowej realizacji usługi automatycznego przekierowywania adresów internetowych, o których mowa w lit. a) powyżej. Wykonawca musi zapewnić niezawodność i ciągłość działania środowiska wirtualnego w ramach rozwiązania HA (wysoka dostępność), gdzie w przypadku awarii pojedynczego komponentu infrastruktury teleinformatycznej musi następować automatyczne bezprzerwowe przełączenie urządzeń na zapasowe komponenty w celu utrzymania ciągłości pracy dostarczonych zasobów.
 - b. przeszkolić 69 osób wskazanych przez Zamawiającego w zakresie powoływania i uruchamiania indywidualnych kont pocztowych w domenie internetowej tożsamej z domeną danej jednostki (w oparciu o licencje Office 365 A1 dla edukacji);
 - c. opracować instrukcję postępowania dla czynności wskazanych w lit. b) powyżej;
 - d. świadczyć roczną usługę wsparcia IT w zakresie konfiguracji czynności opisanych w lit. b) powyżej w trybie 24/7;
 - e. zapewnić roczne utrzymanie przekierowania opisanego w lit a) powyżej;
 - f. zapewnić na czas realizacji usługi oprogramowanie do ochrony antywirusowej dla 69 użytkowników końcowych. Szczegółowa specyfikacja oprogramowania została przedstawiona poniżej;

Lp.	Minimalne wymagania
1	<p>Systemy Operacyjne Komputerów</p> <ul style="list-style-type: none">● Windows 11● Windows 10● Windows 8.1● Windows 8● Windows 7● Windows Vista z dodatkiem Service Pack 1● Windows XP z Service Pack 2 64 bit● Windows XP z Service Pack 3 <p>Tablety i Wbudowane Systemy Operacyjne</p> <ul style="list-style-type: none">● Windows Embedded 8.1 Industry● Windows Embedded 8 Standard● Windows Embedded Standard 7● Windows Embedded Compact 7● Windows Embedded POSReady 7



Zamówienie publiczne nr 15/2022

	<ul style="list-style-type: none">● Windows Embedded Enterprise 7● Windows Embedded POSReady 2009● Windows Embedded Standard 2009● Windows XP z wbudowanym Service Pack 2● Windows XP Tablet PC Edition
2	<p>Systemy Operacyjne Mac OS X</p> <ul style="list-style-type: none">● Mac OS X Sierra (10.12.x)● Mac OS X El Capitan (10.11.x)● Mac OS X Yosemite (10.10.5)● Mac OS X Mavericks (10.9.5)● Mac OS X Mountain Lion (10.8.5)
3	<p>Wymagania Ochrony Mobile</p> <ul style="list-style-type: none">● Apple iPhone i tablety iPad (iOS 5.1+)● Smartfony i tablety z Google Android (2.3+)
4	<p>Obsługiwane Środowiska Microsoft Exchange</p> <ul style="list-style-type: none">● Exchange Server 2016 z rolą Edge Transport lub Mailbox● Exchange Server 2013 z rolą Edge Transport lub Mailbox● Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox● Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox
5	<p>Wymagania funkcjonalno-użytkowe:</p> <ol style="list-style-type: none">1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.4. Wbudowana technologia do ochrony przed rootkitami.5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.8. Możliwość skanowania dysków sieciowych i dysków przenośnych.9. Skanowanie plików spakowanych i skompresowanych.10. Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.11. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.12. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).13. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.



Zamówienie publiczne nr 15/2022

16. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
17. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
20. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
21. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
22. Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze.
23. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
24. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.
25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
27. Praca programu musi być niezauważalna dla użytkownika.
28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
30. Oprogramowanie klienckie posiada wbudowaną funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
31. Możliwość odblokowania ustawień programu po wpisaniu hasła
32. Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika
33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)
34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.
35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
37. Jedna wersja instalacyjna na stacje robocze i serwery plików.
38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
39. Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa.
40. Możliwość tworzenia list sieci zaufanych.
41. Możliwość dezaktywacji funkcji zapory sieciowej.
42. Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików.



Zamówienie publiczne nr 15/2022

	<p>43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.</p> <p>44. Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware</p>
6	<p>Urządzenia Mobilne</p> <ol style="list-style-type: none"> 1. Dla systemu Android możliwość blokowania stron internetowych. 2. Możliwość szyfrowania urządzenia opartego o system android. 3. Możliwość pobrania wersji instalacyjnej ze sklepu iOS oraz Android 4. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android 5. Posiadać możliwość szyfrowania urządzenia dla systemu Android 6. Ochrona stron internetowych dla androida pod kontem malware, exploit, phishing 7. Możliwość blokowania ekranu głównego hasłem. 8. Możliwość definiowania i zabezpieczania połączeń WiFi 9. Dla systemu Android moduł odpowiedzialny za blokowanie stron. 10. Kontrola przeglądarki Safari dla urządzeń z systemem iOS

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

1. Wymagania obligatoryjne dla ośrodka centrum przetwarzania danych.

OBIEKT I LOKALIZACJA			
L.p.	Parametry lub kryterium	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1	Centrum przetwarzania danych zlokalizowane na terenie UE lub Lichtensteinu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Lichtensteinu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.	
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.	
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury.	
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.	
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko).	



Zamówienie publiczne nr 15/2022

6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.	
7	Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni.	Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw.	
8	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).	
9	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN).	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pól zakłócających pracę urządzeń elektrycznych i magnetycznych.	
10	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.	
11	Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.	
12	Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1.	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.	
13	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.	
WĘZŁY TELEKOMUNIKACYJNE			
1	Podłączenie w pełni niezależnymi drogami światłowodowymi do co	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia	



Zamówienie publiczne nr 15/2022

	najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym.	usług transmisji danych przez operatora.	
2	Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.	
3	Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.	
4	Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.	
5	Węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.	
6	Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.	
ZASILANIE			
1	Dostępność roczna systemu zasilania 99,99%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.	
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.	
3	System zasilania awaryjnego UPS osobno na każdą linię zasilającą .	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.	
4	Redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.	
5	System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną.	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.	

A



Zamówienie publiczne nr 15/2022

6	<p>Agregat prądowórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.</p>	<p>Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.</p>	
BEZPIECZEŃSTWO			
1	<p>Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD).</p>	<p>Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń.</p>	
2	<p>Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.</p>	<p>Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.</p>	
3	<p>Ochrona przez zewnętrzną licencjonowaną firmę.</p>	<p>Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.</p>	
4	<p>System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.</p>	<p>Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.</p>	
5	<p>System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 21 dni.</p>	<p>Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.</p>	
6	<p>System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I.</p>	<p>Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku.</p>	
7	<p>Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).</p>	<p>Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.</p>	



Zamówienie publiczne nr 15/2022

8	Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urzędzeń lub w pobliże urzędzeń.	
9	Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urzędzeń lub w pobliże urzędzeń.	
10	Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urzędzeń lub w pobliże urzędzeń.	
11	System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.	
12	Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.	
MONITOROWANIE			
1	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.	
2	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urzędzeń komputerowych udostępnianej Zamawiającemu. Pomiar mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urzędzeń.	

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

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Izolacja sprzętu krytycznego	
2	Ochrona przed uszkodzeniem	



Zamówienie publiczne nr 15/2022

3	Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego	
4	Ochrona przed dostępem dla osób nieupoważnionych	

VIII. Wymagania SLA i czas reakcji

- a. SLA dla świadczonej usługi musi wynosić minimum 99,9% w skali roku.
- b. Obsługa zarządzania środowiskiem teleinformatycznym i wsparcia musi być realizowana w trybie 24/7.
- c. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w systemie online Wykonawcy, który umożliwi podgląd wszystkich zgłoszeń, czas ich realizacji oraz bieżący status.
- d. Czas reakcji na zgłoszenie musi wynosić do 15 minut od przyjęcia zgłoszenia.
- e. Czas realizacji zgłoszenia musi wynosić do 6 h od przyjęcia zgłoszenia.

XIII. Obowiązek zatrudnienia na umowę o pracę osób

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

- a) administrowanie serwerami w środowisku wirtualnym,
- b) administrowanie systemami operacyjnymi.

XIV. Podstawy wykluczenia

1. Zamówienie może zostać udzielone Wykonawcy, który:

- a) nie podlega wykluczeniu na podstawie art. 108 ust. 1 Ustawy Prawo zamówień publicznych
- b) nie podlega wykluczeniu na podstawie art.109 ust 1 pkt 4) Ustawy prawo zamówień publicznych:

Zamawiający wykluczy z udziału w postępowaniu Wykonawców, w stosunku do których 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

- c) 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 2022r. poz. 835 z późn. zm.).
2. Wykluczeniu z postępowania z przyczyn określonych w ust. 1 powyżej nie mogą podlegać również podwykonawcy ani podmioty, na zasobach których polega Wykonawca.

XV. Osoba wyznaczona do kontaktowania się z Oferentami: Magdalena Lorenc, tel. 56 611-79-30, m.lorenc@tcuw.torun

XVI. Pozostałe postanowienia

1. Zamawiający nie dopuszcza możliwości składania ofert wariantowych i częściowych.
2. Zamawiający zastrzega sobie prawo do rezygnacji z realizacji zadania bez wyboru którejkolwiek ze złożonych ofert bez podania przyczyny.
3. Oferty niespełniające wymogów zapytania ofertowego zostaną odrzucone i nie będą brane pod uwagę przy wyborze Wykonawcy.
4. Zamawiający zastrzega sobie prawo unieważnienia zapytania ofertowego bez podania przyczyny, w szczególności w przypadku, gdy kwoty przedstawione w ofertach na zapytanie będą wyższe od zaplanowanych w budżecie na ww. zadanie. Oferenci uczestniczą w postępowaniu ofertowym na własne ryzyko i koszt, nie przysługują im żadne roszczenia w przypadku unieważnienia lub z tytułu odstąpienia przez Zamawiającego od



Zamówienie publiczne nr 15/2022

postępowania ofertowego. Zamawiający może odstąpić od podpisania umowy bez podawania uzasadnienia tej decyzji.

5. Zamawiający jest uprawniony do wyboru kolejnej najkorzystniejszej oferty w przypadku, gdy Wykonawca, którego oferta została uznana za najkorzystniejszą, odmówił podpisania umowy lub gdyby podpisanie umowy z takim Wykonawcą stało się niemożliwe z innych przyczyn.
6. **O wyborze najkorzystniejszej oferty** Zamawiający powiadomi niezwłocznie Oferentów zamieszczając informację o wyborze na swojej stronie internetowej (www.tcuw.torun.pl zakładka BIP, „Zamówienia publiczne”).

DYREKTOR
TORUŃSKIEGO CENTRUM USŁUG WSPÓLNYCH

Łukasz Nowak

**1. Informacje o Wykonawcy**

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

2. Informacje o ofercie

Opis przedmiotu zamówienia/zakres oferty	
Cena netto całości zamówienia w PLN	
Cena brutto całości zamówienia w PLN	

Treść oświadczeń:

- oświadczam, że zapoznałem się z opisem przedmiotu zamówienia i nie wnoszę do niego zastrzeżeń,
- oświadczam, że spełniam warunki określone przez Zamawiającego,
- oświadczam, że w razie wyboru mojej oferty podpiszę umowę z Zamawiającym wg załączonego wzoru.

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

1. Wymagania obligatoryjne dla ośrodka.

OBIEKT I LOKALIZACJA			
L.p.	Parametry lub kryterium	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1	Centrum przetwarzania danych zlokalizowane na terenie UE lub Lichtensteinu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak	



Zamówienie publiczne nr 15/2022

	gromadzone i przetwarzane na terenie UE lub Lichtensteinu, Islandii, Norwegii.	spełnienie wymagań RODO / GDPR.	
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.	
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury.	
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.	
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko).	
6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.	
7	Minimum 200 m oddalenie od linii wysokiego napięcia i elektrowni.	Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw.	
8	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).	
9	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN).	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pól zakłócających pracę urządzeń elektrycznych i magnetycznych.	



Zamówienie publiczne nr 15/2022

10	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.	
11	Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.	
12	Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1.	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.	
13	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.	
WĘZŁY TELEKOMUNIKACYJNE			
1	Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora.	
2	Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.	
3	Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.	
4	Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.	
5	Węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.	



Zamówienie publiczne nr 15/2022

6	Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.	
ZASILANIE			
1	Dostępność roczna systemu zasilania 99,99%	Zagrożenie ciągłości pracy urzędów i dostępności urzędów.	
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.	
3	System zasilania awaryjnego UPS osobno na każdą linię zasilającą .	Zagrożenie dla zachowania nieprzerwanego zasilania urzędów lub skrócenia pracy urzędów na zasilaniu awaryjnym poniżej czasu bezpiecznego.	
4	Redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.	
5	System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną.	Zagrożenie ciągłości pracy urzędów 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 urzędów do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.	
6	Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.	
BEZPIECZEŃSTWO			
1	Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD).	Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urzędów. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urzędów.	
2	Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.	



Zamówienie publiczne nr 15/2022

3	Ochrona przez zewnętrzną licencjonowaną firmę.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.	
4	System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.	
5	System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.	
6	System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku.	
7	Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
8	Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
9	Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
10	Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	



Zamówienie publiczne nr 15/2022

11	System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.	
12	Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.	
MONITOROWANIE			
	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.	
	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.	

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

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

4. Lokalizacja (adres) centrum przetwarzania danych:

5. Posiadane certyfikaty:

1. _____
2. _____
3. _____



Zamówienie publiczne nr 15/2022

4. _____
5. _____
6. _____

5. Gwarantowana w ofercie „Dostępność usługi – SLA w skali roku” wyrażona w %

1. _____

6. Załącznik wymagane do formularza ofertowego:

- 1) Kopie certyfikatów wymienionych w pkt. 5 i potwierdzonych za zgodność z oryginałem
- 2) Oświadczenie o braku podstaw wykluczenia
- 3) Pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy - jeżeli umocowanie tej osoby do reprezentowania podmiotu nie wynika z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.



UMOWA nr

zawarta w Toruniu, w dniu _____ r. pomiędzy:

_____, reprezentowany przez:

zwaną dalej **Wykonawcą**,

a

_____, reprezentowany przez:

zwanym dalej **Zamawiającym**,

zwane dalej **Stronami**.

§1

Przedmiot Umowy

1. Przedmiotem Umowy jest świadczenie przez Wykonawcę na rzecz Zamawiającego usługi informatycznej polegającej na konfiguracji, zabezpieczeniu i obsłudze informatycznej jednostek oświatowych obsługiwanych przez Zamawiającego, w zakresie hostingu i dostępu do poczty elektronicznej, zwanej dalej **Usługą**.
2. Szczegółowy zakres Usługi tj. zakres prac do wykonania oraz sposób ich realizacji został zawarty w cz. VII zapytania ofertowego nr 15/2022 (dalej Zapytanie) i ofercie Wykonawcy z dnia, które stanowią załączniki do niniejszej umowy.
3. Wykonawca przystąpi do realizacji Usługi, zgodnie z terminem określonym w cz. VII zapytania ofertowego liczonego od dnia zawarcia umowy.

§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 jednorazowego wynagrodzenia w wysokości zł brutto (słownie:).
2. Płatność Wynagrodzenia, o którym mowa w ust.1 nastąpi na podstawie faktur VAT wystawianej przez Wykonawcę i doręczonej Zamawiającemu.
3. Zamawiający wyraża zgodę na otrzymanie faktury Vat drogą elektroniczną w formacie PDF, na adres email sekretariat@tcuw.torun.pl.



Zamówienie publiczne nr 15/2022

4. Za dzień dokonania zapłaty Strony uznają dzień, w którym zostanie obciążony rachunek bankowy Zamawiającego.
5. Strony zgodnie oświadczają, że wynagrodzenie określone w niniejszej Umowie wyczerpuje całkowicie zobowiązania Zamawiającego względem Wykonawcy z tytułu świadczenia usług objętych niniejszą umową.

§4

Prawa i obowiązki Stron

1. Zamawiający na podstawie niniejszej Umowy otrzymuje możliwość korzystania z Usługi w okresie ustalonym w Umowie, a Wykonawca ma obowiązek świadczyć Usługę zgodnie z ustalonymi warunkami i parametrami.
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. Wykonawca zobowiązuje się do świadczenia Usługi będącej przedmiotem Umowy z najwyższą starannością. W szczególności zobowiązuje się zapewnić ciągłą dostępność Usługi w granicach i na warunkach określonych w Zapytaniu ofertowym, z zastrzeżeniem ust.6 poniżej.
4. Wykonawca w ramach zapewnienia dostępności Usługi zobowiązuje się do utrzymywania prawidłowego działania i sprawności urządzeń i zasobów sieciowych w ramach sieci wewnętrznej Wykonawcy.
5. Wykonawca zapewnia Zamawiającemu dostępność Usługi na poziomie SLA w skali roku podczas trwania Umowy.
6. 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 30 min jednorazowo i 1 h w miesiącu. O planowanych przerwach technicznych Wykonawca poinformuje Zamawiającego nie później niż na 48h przed planowaną przerwą. Informacja zostanie przekazana drogą elektroniczną na adres email Zamawiającego wskazany w paragrafie §2, ust. 1, lit. b) oraz zamieszczona na stronie internetowej Wykonawcy w zakładce
7. Wykonawca zobowiązuje się do zapewnienia ciągłości funkcjonowania Usługi, w szczególności do usuwania awarii, błędów, ograniczeń w dostępności Usługi. Czas reakcji na zgłoszenie wynosi do 15 minut od przyjęcia zgłoszenia. Czas realizacji zgłoszenia nastąpi w terminie do 6 h od przyjęcia zgłoszenia.
8. Zgłaszanie błędów następować będzie w następujący sposób:
9. Wykonawca jest zobowiązany do zapewnienia odpowiednich zabezpieczeń swojej sieci wewnętrznej przed wirusami komputerowymi, atakami hakerskimi lub utratą danych.
10. Zamawiający, w związku z korzystaniem z Usługi, będzie przysyłać, przechowywać lub rozpowszechniać jedynie takie dane, do korzystania z których jest uprawniony i których umieszczenie w zasobach Wykonawcy nie stanowi naruszenia obowiązującego prawa, praw osób trzecich lub zobowiązań umownych Zamawiającego.
11. Wykonawca zobowiązuje się przyznać Zamawiającemu dostęp do indywidualnego konta użytkownika w portalu z narzędziami i dokumentacją dotyczącą Usługi. Dostęp do panelu (login i hasło) zostaną przekazane Zamawiającemu w dniu zawarcia niniejszej Umowy.
12. Wykonawca dokona przekierowania zasobów Zamawiającego bez jakiegokolwiek przerwy w dostępie do Usługi ani jakiegokolwiek utraty danych. Przygotowanie i zabezpieczenie odpowiedniej infrastruktury teleinformatycznej zabezpieczającej prawidłowe i bezprzerwowe działanie skonfigurowanego przekierowania adresów internetowych zostanie zrealizowane w ciągu 2 dni roboczych.
13. Dostęp do urządzeń, systemów oraz oprogramowania w ramach świadczonej Usługi uzyskiwać będą wyznaczeni pracownicy Wykonawcy oraz pracownicy serwisu zewnętrznego pod nadzorem Wykonawcy.
14. Wykonawca nie sprawdza, nie rozpowszechnia, ani też w żaden sposób nie wykorzystuje treści danych przechowywanych lub przesyłanych przez Zamawiającego.
15. Wykonawca obowiązany jest do samodzielnego wykonywania przedmiotu Umowy i nie jest uprawniony do powierzenia jej realizacji innym podmiotom bez uprzedniej pisemnej (pod rygorem nieważności) zgody Zamawiającego.



Zamówienie publiczne nr 15/2022

§ 5

Odpowiedzialność Stron

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

§ 6

Prawa autorskie

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

§ 7

Ochrona danych osobowych

1. Zamawiający może w związku z korzystaniem z Usługi przechowywać lub przeprowadzać operacje (przetwarzać) na danych osobowych.
2. Zamawiający jest administratorem danych osobowych, o których mowa w ust. 1 lub ich procesorem (przetwarzającym powierzone dane osobowe). Wykonawca nie decyduje o celach i środkach przetwarzania tych danych osobowych, a jedynie udostępnia w ramach świadczenia usług zasoby pozwalające na przechowywanie danych. Wykonawca stosuje środki techniczne i organizacyjne zapewniające ochronę danych przechowywanych i przetwarzanych przez Zamawiającego zgodnie z odpowiednimi przepisami ustawy o ochronie danych osobowych oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem



Zamówienie publiczne nr 15/2022

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – zwane dalej RODO.

- Wykonawca oświadcza, że serwery fizyczne, za pomocą których świadczone są Usługi, będące przedmiotem Umowy, znajdują się na terenie Unii Europejskiej/EOG, a przechowywane dane w żadnym przypadku w toku świadczenia Usługi nie są przesyłane poza obszar Unii Europejskiej/EOG.
- Strony zobowiązują się do zawarcia odrębnej umowy o powierzeniu przetwarzania danych osobowych, najpóźniej w dniu rozpoczęcia świadczenia usługi będącej przedmiotem niniejszej Umowy.

§ 8

Wymagania techniczne korzystania z Usług

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

§ 9

Wsparcie techniczne

- Wykonawca zobowiązuje się do usuwania awarii, błędów urządzeń, za prawidłowe działanie, których ponosi odpowiedzialność, zgodnie z postanowieniami Umowy. Za awarię, błąd uważa się nieprawidłowe działanie urządzenia, powodujące przerwę w świadczeniu Usług, trwające dłużej niż 15 minut w ciągu doby.
- Zamawiający może zgłaszać awarie, błędy pocztą elektroniczną na adres: W przypadku otrzymania zgłoszenia awarii, błędu Wykonawca w najkrótszym możliwym czasie nie dłuższym niż 15 minut dokona analizy zasadności zgłoszenia oraz usunie błąd lub awarię w terminach określonych w § 4 ust. 7 Umowy.
- Jeżeli w wyniku analizy zasadności zgłoszenia nie zostanie potwierdzone istnienie awarii lub jeśli ustalona przyczyna awarii Wykonawca powiadomi Zamawiającego o braku podstaw do interwencji.
- Jeżeli w wyniku analizy zasadności zgłoszenia zostanie ustalona przyczyna awarii, mieszcząca się w zakresie odpowiedzialności Wykonawcy, Wykonawca niezwłocznie przystąpi do usuwania awarii i powiadomi Zamawiającego o przewidywanym terminie jej usunięcia, nie dłuższym niż termin określony w §4 ust. 7, przy czym Wykonawca zobowiązuje się do usuwania awarii w najwcześniejszym możliwym terminie w normalnym toku czynności, z uwzględnieniem charakteru i rozmiaru awarii.
- W przypadkach wskazanych w niniejszym paragrafie zastosowanie znajdują terminy określone w § 4 ust. 7 Umowy.
- Czas prowadzenia analizy zasadności zgłoszenia awarii i sposobu usuwania awarii jest wliczany do czasu dostępności Usługi dla Zamawiającego.

§ 10

Ochrona Informacji Poufnych

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



Zamówienie publiczne nr 15/2022

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

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



Zamówienie publiczne nr 15/2022

§ 11

Kary umowne

1. W przypadku wystąpienia przerw bądź utrudnień w dostępności Usługi, których łączny czas spowoduje spadek dostępności Usługi poniżej gwarantowanego poziomu, o którym mowa w §4 ust. 5 umowy Zamawiający jest uprawniony do naliczenia kary umownej w wysokości:
 - 1) za spadek dostępności Usługi o każde 0,01 % poniżej gwarantowanego w Umowie poziomu , o którym mowa w § 4 ust. 6 wynosi 5% wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy, łącznie nie więcej niż 60% wartości wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy.
2. Strony przewidują zapłatę kar umownych również w następujących przypadkach i wysokościach:
 - a) za zwłokę Wykonawcy w zareagowaniu na awarie (błędy), w stosunku do terminu określonego w § 9 ust. 2 umowy w wysokości 0,5% wynagrodzenia brutto określonego w § 3 ust. 1 za każdą rozpoczętą godzinę zwłoki.
 - b) za zwłokę Wykonawcy w usunięciu awarii, w stosunku do terminu określonego w § 4 ust. 7 Wykonawca zapłaci karę umowną w wysokości 0,5% wynagrodzenia brutto określonego w § 3 ust. 1 za każdą rozpoczętą godzinę zwłoki.
 - c) za zwłokę Wykonawcy w powołaniu indywidualnych domen i realizacji przekierowania dla każdej wskazanej przez Zamawiającego jednostki w stosunku do terminu, o którym mowa w § 4 ust. 12 Umowy, w wysokości 0,5% wynagrodzenia brutto określonego w § 3 ust. 1 za każdy rozpoczęty dzień zwłoki.

Suma kar umownych za zwłokę nie może przekroczyć 60% wartości wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy.
3. W przypadku wystąpienia okoliczności uzasadniających zapłatę przez Wykonawcę kar umownych, Zamawiający może według własnego wyboru:
 - a) potrącać kary umowne z wynagrodzenia należnego Wykonawcy;
 - b) wezwać Wykonawcę do zapłaty kar umownych w terminie 14 dni od daty otrzymania pisemnego wezwania do ich zapłaty.
4. Zastrzeżenie kar umownych nie wyłącza możliwości dochodzenia przez Zamawiającego odszkodowania na zasadach ogólnych za szkodę przewyższającą wartość zastrzeżonych kar.

§ 12

Ograniczenie, zawieszenie Usług, Reklamacje

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

§ 13

Okres obowiązywania Umowy

1. Niniejsza Umowa została zawarta na czas określony od dnia do dnia roku.



Zamówienie publiczne nr 15/2022

2. Zamawiający ma prawo rozwiązać Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca.
3. Wykonawca ma prawo do natychmiastowego zaprzestania świadczenia Usługi oraz do rozwiązania Umowy bez zachowania okresu wypowiedzenia, jeżeli pomimo pisemnego wezwania do przywrócenia stanu zgodnego z prawem lub umową w wyznaczonym, nie krótszym niż 7 dni terminie Zamawiający:
 - a) narusza przepisy prawa w związku z realizacją Umowy lub narusza postanowienia Umowy;
4. Zamawiający ma prawo do natychmiastowego rozwiązania Umowy bez zachowania okresu wypowiedzenia, jeśli
 - a) przerwa w dostępie do Usługi, niezależnie od jej przyczyny, trwa dłużej niż 3 dni,.
 - b) w przypadku powtarzających się opóźnień w obsłudze zgłoszeń awarii określonych § 9 umowy lub ich usuwaniu,
 - c) w przypadku, gdy dostępność Usługi spada poniżej zaoferowanego poziomu SLA i utrzymuje się przez okres 7 dni.
5. Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy.
6. Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o okolicznościach uzasadniających odstąpienie.
7. W przypadku odstąpienia od umowy Wykonawca może żądać wynagrodzenia jedynie za część umowy należycie wykonaną do dnia ustania obowiązywania umowy.
8. Oświadczenie o odstąpieniu, wypowiedzeniu lub rozwiązaniu Umowy powinno zostać złożone na piśmie pod rygorem nieważności.
9. Po zakończeniu obowiązywania Umowy, Wykonawca zobowiązany jest w terminie do 7 dni od zakończenia obowiązywania Umowy, zapisać dane zgromadzone na udostępnionych przez Operatora serwerach na nośniku fizycznym w powszechnie obsługiwanym formacie umożliwiającym edycję i przekazać je Zamawiającemu lub, w przypadku otrzymania od Zamawiającego zgody, dane umieścić na serwerze ftp i udostępnić Zamawiającemu. Następnie Wykonawca, po potwierdzeniu przez Zamawiającego otrzymania zapisanych danych, zobowiązany jest usunąć dane z serwerów Wykonawcy. Wykonawca z chwilą wydania i w ramach wynagrodzenia określonego w niniejszej Umowie przenosi na zamawiającego prawo własności nośnika fizycznego, na którym utrwalono dane.

§ 14

Postanowienia końcowe

1. Wszelkie zmiany Umowy wymagają formy pisemnego aneksu pod rygorem nieważności.
2. Prawem właściwym dla zobowiązań wynikających z Umowy jest prawo polskie.
3. Wszelkie spory wynikające z Umowy będą rozstrzygane przez sąd właściwy dla siedziby Zamawiającego. Strony zobowiązują się w każdym przypadku dążyć do ugodowego rozstrzygnięcia sporu powstałego na gruncie stosowania niniejszej Umowy.
4. Żadna ze Stron Umowy nie może przenieść praw lub obowiązków z niej wynikających na osobę trzecią bez uprzedniej pisemnej zgody drugiej Strony.
5. Zapytanie ofertowe nr z dnia i oferta Wykonawcy z dnia, stanowią załączniki nr i do niniejszej umowy i stanowią jej integralną część..
6. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Wykonawca

Zamawiający



Zamówienie publiczne nr 15/2022

Załącznik nr 1 - Lista oprogramowania koniecznego do prawidłowej realizacji usługi:

Lp.	Nazwa oprogramowania	Zastosowanie



.....
.....
.....
Pełne dane oferenta

OŚWIADCZENIE

o braku podstaw do wykluczenia

Nawiązując do zapytania ofertowego na wykonanie usługi konfiguracji, zabezpieczenia i obsługi informatycznej jednostek oświatowych obsługiwanych przez Zamawiającego, w zakresie hostingu i dostępu do poczty elektronicznej (postępowanie nr 15/2022) oświadczam(y), że:

1. nie podlegamy wykluczeniu z postępowania na podstawie art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4) ustawy Prawo Zamówień Publicznych w zw. z postanowieniami cz. XIV Zapytania ofertowego.
2. nie podlegamy wykluczeniu 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 2022r. poz. 835 z późn. 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 2022 r. poz. 593 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 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 2021 r. poz. 217, 2105 i 2106), 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.

Podpisy (pieczętki) osób, upoważnionych do reprezentowania Wykonawcy

.....
miejsce i data

.....
imię i nazwisko, pieczętką



Zamówienie publiczne nr 15/2022

Załącznik nr 4 - Informacja o zasadach przetwarzania danych

Klauzula informacyjna o przetwarzaniu danych osobowych - Zamówienie publiczne, do którego nie stosuje się przepisów ustawy Prawo zamówień publicznych

Zgodnie z art. 13 oraz 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 17 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) informuję, że:

1. Administrator danych osobowych

a. Administratorem Pani / Pana danych jest Gmina Miasta Toruń z siedzibą w Toruniu działająca przez Toruńskie Centrum Usług Wspólnych (dalej: Administrator).

b. Z Administratorem można kontaktować się listownie na adres: pl. Św. Katarzyny 9, 87-100 Toruń, poprzez e-mail: sekretariat@tcuw.torun.pl lub dzwoniąc pod numer: 56 611-89-91

2. Inspektor Ochrony Danych

a. Administrator powołał Inspektora Ochrony Danych (dalej: IOD).

b. Z IOD można kontaktować się we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych pisząc e-mail na adres: m.lorenc@tcuw.torun.pl lub pisząc na adres siedziby Administratora.

3. Cel i podstawa prawna przetwarzania danych osobowych

Pani/i dane osobowe będą przetwarzane na podstawie art. 6 ust.1 lit. b i c RODO w celu związanym z procedurą przeprowadzenia postępowania oraz zawarcia umowy w sprawie zamówienia, do którego nie stosuje się przepisów ustawy Prawa zamówień publicznych. Procedura jest prowadzona w związku z zapewnieniem wydatkowania środków publicznych w sposób oszczędny i z zachowaniem zasad uzyskiwania najlepszych efektów z danych nakładów, co stanowi obowiązek Gminy jako jednostki sektora finansów publicznych, określony w przepisach ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

4. Okres przechowywania danych

a. Pani/Pana dane osobowe będą przechowywane w Urzędzie przez okres 4 lat od dnia zakończenia procedury oraz przez cały czas obowiązywania umowy zawartej w wyniku rozstrzygnięcia procedury.

b. Dane osobowe zebrane na podstawie Pani / Pana zgody będą przechowywane do momentu wycofania tej zgody lub do momentu realizacji celu określonego w zgodzie.

c. Okres przetwarzania może być przedłużony w granicach prawa w przypadku, gdy przetwarzanie danych osobowych niezbędne jest do dochodzenia lub obrony przed roszczeniami.

5. Informacja o wymogu podania danych

Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących wynika z Pani/Pana dobrowolnego uczestnictwa w procedurze oraz jest warunkiem zawarcia umowy w sprawie zamówienia. Konsekwencją niepodania danych osobowych będzie niemożliwość weryfikacji spełnienia warunków udziału w procedurze i dokonania oceny ofert, a także niemożność zawarcia umowy

6. Prawa osób, których dane dotyczą

Z zastrzeżeniem sytuacji określonych w przepisach prawa Pani / Panu przysługują następujące uprawnienia:

a. Prawo dostępu do treści swoich danych oraz otrzymania ich kopii.

b. Prawo do sprostowania (poprawienia) swoich danych.

c. Prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej.

d. Prawo do ograniczenia przetwarzania danych (przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego prawa).

e. Prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa (w przypadku podejrzenia, że przetwarzanie narusza przepisy prawa dotyczącego ochrony danych osobowych).

7. Obowiązki Oferentów w związku z przekazaniem danych osobowych

a. W przypadku udostępnienia Administratorowi przez Oferenta danych osobowych swojego personelu niezależnie od podstawy dysponowania, pełnomocników, członków organów, prokurentów, współników, kontrahentów, współpracowników, osób do kontaktu, Administrator zobowiązuje Oferentów do poinformowania osób, których dane zostały przekazane o fakcie i zakresie przekazania danych, o danych kontaktowych do Administratora oraz zasadach przetwarzania danych wskazanych w niniejszej informacji.

8. Odbiorcy danych

Dane osobowe mogą zostać przekazane zewnętrznym podmiotom:



Zamówienie publiczne nr 15/2022

- a. Dane Oferenta pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego przekazywane będą wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia publicznego jest jawne.
 - b. Instytucje i organy uprawnione do uzyskania danych na podstawie obowiązujących przepisów prawa, np. organy kontrolujące Administratora, Krajowa Izba Odwoławcza.
 - c. Podmioty zewnętrzne wspierające Administratora, np. podmiot świadczący usługę poczty elektronicznej (wszystkie podmioty biorą udział w procesie przetwarzania danych osobowych na podstawie upoważnienia lub zawartych umów powierzenia przetwarzania danych z Administratorem i zapewniają odpowiedni poziom ochrony danych osobowych).
9. Dane osobowe nie będą przekazywane poza Europejski Obszar Gospodarczy ani do organizacji międzynarodowych.
10. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą przedmiotem profilowania.

