

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA
zwana dalej **(SWZ)**

Zakup, dostawa i wdrożenie systemu kopii zapasowej oraz systemu ochrony poczty elektronicznej.

Postępowanie o udzielenie zamówienia prowadzone jest na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2023 r. poz. 1605), zwanej dalej "ustawą Pzp". Wartość szacunkowa zamówienia jest niższa od progów unijnych określonych na podstawie art. 3 ustawy Pzp.

1. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Samodzielny Publiczny Wojewódzki Szpital Specjalistyczny w Chełmie, ul. Ceramiczna 1, 22-100 Chełm.

Tel.: 82 562 32 54

Adres poczty elektronicznej: przetarg@szpitalchelm.pl

Adres strony internetowej prowadzonego postępowania oraz strony, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z prowadzonym postępowaniem: e-propublico.pl.

2. TRYB UDZIELENIA ZAMÓWIENIA

- 2.1. Postępowanie o udzielenie zamówienia prowadzone jest w **trybie podstawowym z możliwością negocjacji**, o którym mowa w art. 275 pkt 2 ustawy Pzp.
- 2.2. Zamawiający, na podstawie art. 275 pkt. 2 ustawy Pzp, przewiduje w prowadzonym postępowaniu, możliwość przeprowadzenia negocjacji treści ofert, złożonych w odpowiedzi na ogłoszenie o zamówieniu, w celu ich ulepszenia, stosując zasady wskazane w pkt. 3 niniejszej SWZ.
- 2.3. W przypadku, gdy Zamawiający postanowi nie prowadzić negocjacji, dokona wyboru najkorzystniejszej oferty spośród niepodlegających odrzuceniu ofert, złożonych w odpowiedzi na ogłoszenie o zamówieniu.

3. ZASADY OBOWIĄZUJĄCE PRZY ZASTOSOWANIU PROCEDURY NEGOCJACJI TREŚCI ZŁOŻONYCH OFERT

- 3.1. W przypadku podjęcia przez Zamawiającego decyzji o przeprowadzeniu negocjacji, w celu ulepszenia treści ofert, Zamawiający nie przewiduje ograniczenia liczby Wykonawców, których zaprosi do negocjacji.
- 3.2. Zamawiający poinformuje równocześnie wszystkich Wykonawców, którzy w odpowiedzi na ogłoszenie o zamówieniu złożyli oferty, o Wykonawcach:
 - 1) których oferty nie zostały odrzucone oraz punktacji przyznanej ofertom w każdym kryterium oceny ofert i łącznej punktacji,
 - 2) których oferty zostały odrzucone,
- 3.3. Zamawiający w zaproszeniu do negocjacji wskaże miejsce, termin i sposób ich prowadzenia oraz kryteria oceny ofert, w ramach których negocjacje będą prowadzone.
- 3.4. Zamawiający podczas negocjacji ofert zapewnia równe traktowanie wszystkich Wykonawców. Zamawiający nie udziela informacji w sposób, który mógłby zapewnić niektórym Wykonawcom przewagę nad innymi Wykonawcami.
- 3.5. Prowadzone negocjacje mają charakter poufny, żadna ze stron nie może, bez zgody drugiej strony, ujawniać informacji technicznych i handlowych związanych z negocjacjami. Zgoda jest udzielana w odniesieniu do konkretnych informacji i przed ich ujawnieniem.
- 3.6. Zamawiający poinformuje Wykonawców o zakończeniu negocjacji oraz zaprosi ich do składania ofert dodatkowych podając:
 - 1) nazwę oraz adres Zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania,
 - 2) sposób i termin składania ofert dodatkowych oraz język lub języki, w jakich muszą być one sporządzone, oraz termin otwarcia tych ofert.
- 3.7. Wykonawca może złożyć ofertę dodatkową, która zawiera nowe propozycje w zakresie treści oferty podlegających ocenie w ramach kryteriów oceny ofert wskazanych przez Zamawiającego w zaproszeniu do negocjacji. W przypadku, gdy Wykonawca nie złoży oferty dodatkowej, wówczas wiążąca będzie oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.

- 3.8. Oferta dodatkowa nie może być mniej korzystna w żadnym z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.
- 3.9. Oferta przestaje wiązać Wykonawcę w takim zakresie, w jakim złoży on ofertę dodatkową zawierającą korzystniejsze propozycje w ramach każdego z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji.
- 3.10. Oferta dodatkowa, która jest mniej korzystna w którymkolwiek z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu, podlega odrzuceniu.

4. INFORMACJE OGÓLNE

- 4.1. Komunikacja w postępowaniu
- 4.2. W niniejszym postępowaniu komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej, za pośrednictwem platformy on-line działającej pod adresem <https://e-propublico.pl> (dalej jako: "Platforma").
- 4.3. Wizja lokalna
- 4.4. Zamawiający nie przewiduje obowiązku odbycia przez Wykonawcę wizji lokalnej lub sprawdzenia przez Wykonawcę dokumentów niezbędnych do realizacji zamówienia.
- 4.5. Zaliczki na poczet wykonania zamówienia
- 4.6. Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.
- 4.7. Katalogi elektroniczne
- 4.8. Zamawiający ☐ wymaga / ☒ nie wymaga złożenia ofert w postaci katalogów elektronicznych.
- 4.9. Do spraw nieuregulowanych w niniejszej SWZ mają zastosowanie przepisy ustawy z dnia 11 września 2019 r. roku Prawo zamówień publicznych (t.j. Dz. U. z 2023, POZ. 1605).

5. OPIS PRZEDMIOTU ZAMÓWIENIA

- 5.1. Przedmiotem zamówienia jest **zakup, dostawa i wdrożenie systemu kopii zapasowej oraz systemu ochrony poczty elektronicznej.**
- 5.2. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

A) Biblioteka taśmowa

Lp.	Nazwa parametru, elementu lub cechy	Wymagane parametry techniczne
	1	2
	TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Obudowa	Do zamontowania w szafie rack, maksymalnie 1U.
2.	Napęd	min. 1 x LTO9
3.	Interfejs	min. 1 x SAS min. 6Gb/s w napędzie
4.	Liczba slotów	Min. 9 slotów przeznaczonych na zestaw taśm. W komplecie 1 x taśma czyszcząca, 10 sztuk taśm LTO9.
5.	Dodatkowe	W komplecie 2 szt. kabla SAS umożliwiające podłączenie biblioteki do serwera o dł. min. 2 m.
6.	Warunki gwarancji	Przynajmniej 5 lat gwarancji z czasem reakcji do następnego dnia roboczego.

		<p>Możliwość zgłaszania awarii poprzez linię telefoniczną producenta.</p> <p>Wszystkie naprawy gwarancyjne realizowane w miejscu instalacji.</p> <p>Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.</p> <p>W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).</p>
--	--	---

B) Deduplikator 16TB

Lp.	Nazwa parametru, elementu lub cechy
	1
TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Urządzenie musi być przeznaczone do de-duplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
2.	Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.
3.	<p>Oferowane urządzenie musi posiadać minimum</p> <ul style="list-style-type: none"> • 4 porty Eth 10 Gb/s BaseT • 2 porty Eth 10Gb/s Eth OP <p>wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle;</p>
4.	Dostarczone urządzenie musi umożliwiać dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityką retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę (wymagane wsparcie dla AWS, Microsoft Azure, Google GCP). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Skalowanie w przypadku wykorzystywanej przestrzeni warstwy typu Cloud musi stanowić równoważność co najmniej dwukrotnej pojemności netto oferowanego urządzenia (bez uwzględnienia warstwy CLOUD), czyli 16TB x 2 = 32TB.
5.	<p>Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:</p> <ul style="list-style-type: none"> • CIFS, NFS, • zapewniającym deduplikację na źródle - wymagane wsparcie dla eksploatowanej przez Zamawiającego aplikacji Veeam Backup and Replication • VTL (po doposażeniu w porty FC)
6.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 3 TB/h (dane podawane przez producenta) oraz co

	najmniej 5 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta).
7.	<p>Urządzenie musi pozwalać na jednoczesną obsługę minimum 90 strumieni jednocześnie, w tym</p> <ul style="list-style-type: none"> • 30 dedykowanych do zapisu • 30 dedykowanych do odczytu • 30 dedykowanych do replikacji <p>wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.</p>
8.	<p>Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia, powyższe wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup'ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych interfejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backup'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiegokolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line</p>
9.	<p>Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.</p>
10.	<p>Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o długości nie większej niż 12 kB. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.</p>
11.	<p>Oferowane urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej przestrzeni urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może</p>

	zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
12.	Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych.
13.	Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
14.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
15.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru: gz, lz.
16.	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasta retencja powinny zostać usunięte podczas procesu czyszczenia tzw. cleaning, wymagane dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
17.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam, Oracle RMAN, Microsoft SQL Server Management Studio.
18.	W przypadku współpracy z każdą z poniższych aplikacji: <ul style="list-style-type: none"> • RMAN (dla ORACLE) • Microsoft SQL Server Management Studio (dla Microsoft SQL) • Veeam Backup and Replication urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwera do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu
19.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
20.	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta powinna być wspierana przez Veeam Backup and Replication. Spełnienie wymagania nie może być ograniczone dla wybranych grup danych ze względu na miejsce składowania czy konkretną retencję.
21.	Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku eksploatowanej aplikacji Veeam Backup and Replication.

22.	Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.
23.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: <ul style="list-style-type: none"> * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
24.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
25.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
26.	Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
27.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
28.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej.
29.	Oferowane urządzenie musi umożliwiać realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określonej chwili. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtworzenia backupów).
30.	Urządzenie musi pozwalać na realizację i przechowywanie minimum 300 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
31.	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).
32.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: <ul style="list-style-type: none"> • CIFS • NFS • zapewniającym deduplikację na źródle dla Veeam • VTL

33.	<p>Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.</p> <p>Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):</p> <ol style="list-style-type: none"> 1. Możliwość zdjęcia blokady przed upływem ważności danych 1. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE, wymagane wsparcie dla normy SEC 17a-4(f) lub ISO Standard 15489-1) <p>Licencje na blokadę skasowania/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.</p> <p>Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady, wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot.</p>
34.	<p>Urządzenie musi weryfikować ewentualne przekłamanie (zmianę danych) na poziomie systemu plików. Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu.</p>
35.	<p>Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych w trybie „end-to-end”). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności)</p>
36.	<p>Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.</p>
37.	<p>Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).</p>
38.	<p>Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).</p> <p>Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.</p>
39.	<p>Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.</p>
40.	<p>Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień -</p>

	minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie.
41.	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
42.	Urządzenie musi mieć możliwość zarządzania poprzez <ul style="list-style-type: none"> • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
43.	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.
44.	Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
45.	Oferowane urządzenie powinno być objęte wsparciem producenta w okresie min. 60 miesięcy, realizowanym w trybie NBD, uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
46.	Wymagane dołączenie do oferty oświadczenia producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym producenta. Zamawiający wymaga dołączenia do oferty oświadczenia producenta sprzętu potwierdzającego, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

C) Serwer kopii zapasowych

Lp.	Nazwa parametru, elementu lub cechy	Wymagane parametry techniczne
	1	2
	TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Obudowa	Obudowa Rack o wysokości maks. 2U z możliwością instalacji do min. 12 dysków 3,5". Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android i Apple iOS) przy użyciu jednego z protokołów BLE i WIFI.
2.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i

		oznaczona jego znakiem firmowym.
3.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
4.	Procesor	Zainstalowane dwa procesory min. ośmiordzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 130 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
5.	RAM	Min. 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.
6.	Zabezpieczenia pamięci RAM	Memory Health Check, Memory Page Retire
7.	Gniazda PCI	Min. pięć slotów PCIe x16 generacji 4 i jeden slot PCIe x4.
8.	Interfejsy sieciowe/FC	<p>Wbudowane dwa interfejsy sieciowe min. 25Gb Ethernet ze złączami SFP28.</p> <p>Możliwość instalacji wymiennie modułów udostępniających:</p> <ul style="list-style-type: none"> - dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ - dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ - cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 <p>Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.</p> <p>Dodatkowo zainstalowane:</p> <ul style="list-style-type: none"> - jedna karta dwuportowa SAS 12Gb/s ze złączami wyprowadzonymi na zewnątrz obudowy. <p>Dla każdego portu SFP28 należy dostarczyć moduł nadawczo-odbiorczy SFP+ SR 10GbE.</p>
9.	Dyski twarde	<p>Zainstalowane min. 6 x 20TB NearLine SAS 7.2k oraz min. 2 x 480GB SATA SSD, DWPD min. 1.</p> <p>Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość instalacji 2 jednakowych nośników typu flash o pojemności min. 64GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.</p>

		Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
10.	Kontroler RAID	Sprzętowy kontroler dyskowy z pojemnością cache min. 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60.
11.	System operacyjny	<p>Zakres Przedmiotu Zamówienia obejmuje dostarczenie i wdrożenie Oprogramowania Systemowego zwanego dalej SSO.</p> <p>Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.</p> <p>SSO musi posiadać następujące, wbudowane cechy:</p> <ul style="list-style-type: none"> a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

	<ul style="list-style-type: none"> • umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: <ul style="list-style-type: none"> • podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, • usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną; ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania; odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, • zdalna dystrybucja oprogramowania na stacje robocze, • praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, • centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: dystrybucję certyfikatów poprzez http;
--	---

		<p>konsolidację CA dla wielu lasów domen;</p> <p>automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,</p> <ul style="list-style-type: none"> • szyfrowanie plików i folderów, • szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), • możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, • serwis udostępniania stron WWW, • wsparcie dla protokołu IP w wersji 6 (IPv6), • wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: <ul style="list-style-type: none"> o dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, o obsługi ramek typu jumbo frames dla maszyn wirtualnych, o obsługi 4-KB sektorów dysków, o nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, o możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, o możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
12.	Wbudowane porty	min. port USB 2.0 oraz port USB 3.0, port VGA

13.	Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1600x1200.
14.	Wentylatory	Redundantne
15.	Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
16.	Bezpieczeństwo	Moduł TPM 2.0 V3. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą oraz blokada obudowy zamykana w sposób umożliwiający ochronę przed nieautoryzowanym dostępem do dysków twardych.
17.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows Server 2022
18.	Karta Zarządzania	Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającą: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich

	<p>komponentów serwera</p> <ul style="list-style-type: none"> • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. • Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe • monitorowanie przepływu powietrza na bieżąco • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, ElasticSearch, Grafana • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe • monitorowanie przepływu powietrza na bieżąco
--	---

19.	Dodatkowe oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniające poniższe wymagania: • wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • szczegółowy opis wykrytych systemów oraz ich komponentów • możliwość eksportu raportu do CSV, HTML, XLS, PDF • możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • grupowanie urządzeń w oparciu o kryteria użytkownika • tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • szybki podgląd stanu środowiska • podsumowanie stanu dla każdego urządzenia • szczegółowy status urządzenia/elementu/komponentu • generowanie alertów przy zmianie stanu urządzenia. • filtry raportów umożliwiające podgląd najważniejszych zdarzeń • integracja z service desk producenta dostarczonej platformy sprzętowej • możliwość przejęcia zdalnego pulpitu • możliwość podmontowania wirtualnego napędu • kreator umożliwiający dostosowanie akcji dla wybranych alertów • możliwość importu plików MIB • przesyłanie alertów „as-is” do innych konsol firm trzecich • możliwość definiowania ról administratorów • możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta
-----	--	---

		<p>oferowanego rozwiązania)</p> <ul style="list-style-type: none"> • możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • zdalne uruchamianie diagnostyki serwera. • dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. <p>oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</p>
20.	Warunki gwarancji	<p>Min. 60 miesięcy gwarancji producenta lub autoryzowanego partnera serwisowego producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta.</p> <p>W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Do oferty Wykonawca dołączy oświadczenie, że:</p> <ul style="list-style-type: none"> • Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta, • sprzęt pochodzi z oficjalnego kanału

		dystrybucyjnego producenta Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
21.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

D) System ochrony poczty elektronicznej

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane parametry techniczne
	1	2
	TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Zakres i jakość ochrony	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń
2.	Tryby pracy	Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: <ul style="list-style-type: none"> • Tryb Gateway. • Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). • Serwer
3.	Wypożazenie	System musi być wyposażony w 4 porty Gigabit Ethernet RJ-45 System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB z możliwością obsługi mechanizmu RAID 0, 1 System musi posiadać wbudowany port konsoli szeregowej Zasilanie z sieci 230V/50Hz <ul style="list-style-type: none"> • 2 zasilacze redundantne
4.	Funkcja serwera poczty	systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi

		integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.
5.	Funkcja serwera poczty	<p>W tym zakresie dostarczony system musi zapewniać:</p> <ul style="list-style-type: none"> • Obsługę serwisów pocztowych: SMTP, POP3, IMAP. • Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2). • Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników. • Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3). • Polski interfejs użytkownika przy dostępie przez WebMail. • Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP. • Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
6.	Funkcja systemu ochrony poczty	<p>Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:</p> <ul style="list-style-type: none"> • Wsparcie dla co najmniej 100 domen pocztowych. • System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 150 tys. wiadomości/godzinę. • Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). • Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. • Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). • Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. • Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. • Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. • Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z

		<p>zewnętrznego serwera LDAP.</p> <ul style="list-style-type: none"> • Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. • Możliwość poddania ponownemu skanowaniu (antyvirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. • Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. • Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. • Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. • Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. • Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. • Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). • Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
7.	Funkcje kontroli antywirusowej i ochrony przed malware	<p>dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> • Skanowanie antywirusowe wiadomości SMTP. • Kwarantannę dla zainfekowanych plików. • Skanowanie załączników skompresowanych. • Definiowanie komunikatów powiadomień w języku polskim. • Blokowanie załączników w oparciu o typ pliku. • Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. • Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. • Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject,

		<p>dostarczenie do innego serwera, powiadomienie administratora.</p> <ul style="list-style-type: none"> • Ochronę typu wirus outbrake. • Ochronę przed zagrożeniami zawartymi w wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.
8.	Funkcje kontroli antyspamowej	<p>System musi zapewniać poniższe funkcje i metody filtrowania spamu:</p> <ul style="list-style-type: none"> • Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. • Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. • Szczegółowa kontrola nagłówka wiadomości. • Analiza Heurystyczna. • Współpraca z zewnętrznymi serwerami RBL, SURBL. • Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. • Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. • Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. • Kontrola w oparciu o Greylisting oraz SPF. • Filtrowanie treści wiadomości i załączników. • Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. • Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. • Ochrona typu outbrake. • Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). • Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. • Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level) • Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9.	Funkcje ochrony przed atakami na usługę poczty	<p>System musi zapewniać poniższe funkcje i metody filtrowania:</p> <ul style="list-style-type: none"> • Ochrona przed atakami na adres odbiorcy

		<p>(m.in. email bombing).</p> <ul style="list-style-type: none"> • Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. • Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. • Kontrola Reverse DNS (ochrona przed Anty-Spoofing). • Weryfikacja poprawności adresu e-mail nadawcy.
10.	Funkcje logowania i raportowania	<p>Dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> • Logowanie do zewnętrznego serwera SYSLOG. • Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. • Logowanie informacji na temat spamu oraz niedozwolonych załączników. • Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. • Możliwość analizy przebiegu sesji SMTP. • Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. • Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. • Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
11.	Funkcje pracy w trybie wysokiej dostępności (HA)	<p>System ochrony poczty musi zapewniać poniższe funkcje:</p> <ul style="list-style-type: none"> • Konfigurację HA w każdym z trybów: gateway, transparent, serwer • Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. • Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. • Monitorowanie stanu pracy klastra.
12.	Aktualizacje sygnatur, dostęp do bazy spamu	<p>Dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> • Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. • Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
13.	Zarządzanie	<p>System ochrony poczty musi zapewniać poniższe funkcje:</p> <ul style="list-style-type: none"> • System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. • Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.

		<ul style="list-style-type: none"> • Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
14.	Certyfikaty	<p>Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:</p> <ul style="list-style-type: none"> • VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
15.	Serwisy i licencje	<p>Dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:</p> <ul style="list-style-type: none"> • Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbreak, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 60 miesięcy.
16.	Gwarancja oraz wsparcie	<ul style="list-style-type: none"> • Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7
		<ul style="list-style-type: none"> • Wykonawca musi zapewnić wdrożenie oraz szkolenie z oferowanego produktu • System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

- 5.3. Wspólny Słownik Zamówień: 32420000-3 – urządzenia sieciowe; dodatkowy kod CPV: 48710000-8 - pakiety oprogramowania do kopii zapasowych i odzyskiwania, 48223000-7 – pakiety oprogramowania do poczty elektronicznej, 72265000-0 - usługi konfiguracji oprogramowania, 79632000-3 – szkolenia pracowników.
- 5.4. Oferty nie zawierające pełnego zakresu przedmiotu zamówienia zostaną odrzucone.
- 5.5. Przedmiot zamówienia dostarczony będzie Zamawiającemu na koszt i ryzyko Wykonawcy. W szczególności Wykonawca ponosi pełną odpowiedzialność za szkody wynikłe w czasie transportu oraz spowodowane niewłaściwym oznakowaniem. Opakowanie winno posiadać oryginalną etykietę w języku polskim. Naklejanie, przeklejanie etykiety na obcojęzyczne opakowanie nie będą akceptowane.
- 5.6. Miejsce realizacji:

5.7. Serwerownia SPWSzS w Chełmie**6. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 7 I 8 USTAWY PZP.**

- 6.1. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.

7. TERMIN WYKONANIA ZAMÓWIENIA

- 7.1. Zamówienie musi zostać zrealizowane w terminie:
do 18 października 2023 r.

8. INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU

- 8.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu oraz spełniają warunki udziału w postępowaniu i wymagania określone w niniejszej SWZ.
- 8.2. Zamawiający, na podstawie art. 112 ustawy Pzp określa następujące warunki udziału w postępowaniu:
- 8.3. Zamawiający nie określa warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 ustawy Pzp.

9. PODSTAWY WYKLUCZENIA WYKONAWCY Z POSTĘPOWANIA

- 9.1. Zamawiający wykluczy z postępowania o udzielenie zamówienia Wykonawcę:
- 9.2. wobec którego zachodzą podstawy wykluczenia określone w art. 108 ustawy Pzp;
- 9.3. wobec którego zachodzą podstawy wykluczenia określone w 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 2022 r., poz. 835).
- 9.4. Zamawiający, na podstawie art. 109 ust. 1 ustawy Pzp, wykluczy z postępowania o udzielenie zamówienia Wykonawcę:
- 9.5. 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.
- 9.6. Wykluczenie Wykonawcy nastąpi w przypadkach, o których mowa w art. 111 ustawy Pzp.
- 9.7. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2–5 i 7–10 ustawy Pzp, jeżeli udowodni Zamawiającemu, że spełnił łącznie przesłanki określone w art. 110 ust. 2 ustawy Pzp.
- 9.8. Zamawiający oceni, czy podjęte przez Wykonawcę czynności, o których mowa w art. 110 ust. 2 ustawy Pzp, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, a jeżeli uzna, że nie są wystarczające, wykluczy Wykonawcę.
- 9.9. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania, ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

10. INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH

- 10.1. Wykonawca wraz z ofertą zobowiązany jest złożyć:

Lp.	Wymagany dokument
1	Formularz ofertowo-cenowy – załącznik nr 1 do SWZ (arkusze: "formularz oferty" i "szczegóły")

2	Wykaz wymaganych parametrów technicznych – załącznik nr 4 do SWZ
3	Oświadczenie producenta sprzętu potwierdzającego, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego - dotyczy części B
	Oświadczenie Wykonawcy, że: 1) Serwis urządzeń będzie realizowany bezpośrednio przez producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym producenta, 2) sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – dotyczy części C
3	Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału Aktualne na dzień składania ofert oświadczenie Wykonawcy stanowiące wstępne potwierdzenie spełniania warunków udziału w postępowaniu oraz brak podstaw wykluczenia

10.2. 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:

10.3. W celu potwierdzenia braku podstaw wykluczenia Wykonawcy z udziału w postępowaniu:

Lp.	Wymagany dokument
1	Odpis lub informacja z KRS lub CEIDG Odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzone nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

10.4. Dokumenty podmiotów zagranicznych:

Lp.	Wymagany dokument
1	Dokument potwierdzający, że nie otwarto likwidacji wykonawcy Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast "Odpisu lub informacji z KRS lub CEIDG" składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, 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, wystawione nie wcześniej niż 3 miesiące przed ich złożeniem.

10.5. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się ww. dokumentów, zastępuje się je 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, z uwzględnieniem terminów ważności tych dokumentów.

- 10.6. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania, wezwać Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
- 10.7. Jeżeli zajądą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, Zamawiający może w każdym czasie wezwać Wykonawcę do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
- 10.8. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
- 10.9. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:
- 1) może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 Pzp dane umożliwiające dostęp do tych środków;
 - 2) podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1.
- 10.10. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia Wykonawca składa, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
- 10.11. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

11. INFORMACJA O PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH

- 11.1. Zamawiający żąda złożenia przez Wykonawcę wraz z ofertą następujących, przedmiotowych środków dowodowych:
- 11.2. Zamawiający nie wymaga dołączenia do oferty przedmiotowych środków dowodowych

12. INFORMACJA DLA WYKONAWCÓW ZAMIERZAJĄCYCH POWIERZYĆ WYKONANIE CZĘŚCI ZAMÓWIENIA PODWYKONAWCOM

- 12.1. Wykonawca może powierzyć wykonanie części zamówienia Podwykonawcom.
- 12.2. Zamawiający żąda wskazania przez Wykonawcę, w ofercie, części zamówienia, których wykonanie zamierza powierzyć Podwykonawcom oraz podania nazw ewentualnych Podwykonawców, jeżeli są już znani.
- 12.3. Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, podał nazwy, dane kontaktowe oraz przedstawicieli, Podwykonawców zaangażowanych w realizację zamówienia, jeżeli są już znani.
- 12.4. Wykonawca jest obowiązany zawiadomić Zamawiającego o wszelkich zmianach w odniesieniu do informacji, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazać wymagane informacje na temat nowych Podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację zamówienia.

13. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

- 13.1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
- 13.2. Pełnomocnictwo należy dołączyć do oferty i powinno ono zawierać w szczególności wskazanie:
- 13.3. postępowania o udzielenie zamówienia publicznego, którego dotyczy;
- 13.4. wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia;
- 13.5. ustanowionego pełnomocnika oraz zakresu jego umocowania.

- 13.6. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, dokument "Oświadczenia o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału", o którym mowa w pkt. 10.1.2 SWZ, składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

14. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI

- 14.1. W niniejszym postępowaniu komunikacja Zamawiającego z Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej, za pośrednictwem Platformy on-line działającej pod adresem <https://e-propublico.pl>.
- 14.2. Korzystanie z Platformy przez Wykonawcę jest bezpłatne.
- 14.3. Na Platformie postępowanie prowadzone jest pod nazwą: **"Zakup, dostawa, wdrożenie systemu kopii zapasowej oraz systemu ochrony poczty elektronicznej."** – znak sprawy: **ZP.3311.33.2023**.
- 14.4. Wykonawca przystępując do postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z Platformy określone w Regulaminie zamieszczonym na stronie internetowej <https://e-propublico.pl> oraz uznaje go za wiążący.
- 14.5. Wykonawca zamierzający wziąć udział w postępowaniu musi posiadać konto na Platformie.
- 14.6. Do złożenia oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy ważnego kwalifikowanego podpisu elektronicznego, podpisu zaufanego lub podpisu osobistego.
- 14.7. Ilekroć w niniejszej SWZ jest mowa o:
- 14.8. podpisie zaufanym – należy przez to rozumieć podpis, o którym mowa art. 3 pkt 14a ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U.2020 poz. 346);
- 14.9. podpisie osobistym – należy przez to rozumieć podpis, o którym mowa w art. z art. 2 ust. 1 pkt 9 ustawy z 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz.U.2020 poz. 332).
- 14.10. Zalecenia Zamawiającego odnośnie kwalifikowanego podpisu elektronicznego:
- 14.11. dokumenty sporządzone i przesyłane w formacie .pdf zaleca się podpisywać kwalifikowanym podpisem elektronicznym w formacie PAdES;
- 14.12. dokumenty sporządzone i przesyłane w formacie innym niż .pdf (np.: .doc, .docx, .xlsx, .xml) zaleca się podpisywać kwalifikowanym podpisem elektronicznym w formacie XAdES;
- 14.13. do składania kwalifikowanego podpisu elektronicznego zaleca się stosowanie algorytmu SHA-2 (lub wyższego).
- 14.14. Zamawiający określa następujące wymagania sprzętowe – aplikacyjne pozwalające na korzystanie z Platformy:
- 14.15. stały dostęp do sieci Internet;
- 14.16. posiadanie dowolnej i aktywnej skrzynki poczty elektronicznej (e-mail),
- 14.17. komputer z zainstalowanym systemem operacyjnym Windows 7 (lub nowszym) albo Linux,
- 14.18. zainstalowana dowolna przeglądarka internetowa - Platforma współpracuje z najnowszymi, stabilnymi wersjami wszystkich głównych przeglądarek internetowych (Internet Explorer 10+, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera),
- 14.19. włączona obsługa JavaScript oraz Cookies.
- 14.20. Zamawiający dopuszcza następujący format przesyłanych danych:
- 14.21. pliki w formatach określonych w załączniku nr 2 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i

- wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, przy czym zaleca się wykorzystywanie plików w formacie **.pdf, .doc, .docx, .xls, .xlsx**;
- 14.22. w celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z rozszerzeń: **.zip** lub **.7z**;
- 14.23. maksymalny rozmiar pojedynczego pliku to **80 MB**, przy czym nie określa się limitu liczby plików.
- 14.24. Zamawiający określa następujące informacje na temat kodowania i czasu odbioru danych:
- 14.25. załączony i przesłany przez Wykonawcę za pomocą Platformy plik oferty wraz z załącznikami, nie jest dostępny dla Zamawiającego i przechowywany jest na serwerach Platformy w formie zaszyfrowanej. Zamawiający otrzyma dostęp do pliku dopiero po upływie terminu otwarcia ofert;
- 14.26. oznaczenie czasu odbioru danych przez Platformę stanowi przyporządkowaną do dokumentu elektronicznego datę oraz dokładny czas (hh:mm:ss), widoczne przy wysłanym dokumencie w kolumnie "Data przesłania";
- 14.27. o terminie przesłania decyduje czas pełnego przeprocesowania transakcji pliku na Platformie.
- 14.28. W postępowaniu, wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje przekazywane są za pośrednictwem Platformy (karta "Wiadomości"). Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przesłanych za pośrednictwem Platformy, przyjmuje się datę ich zamieszczenia na Platformie.
- 14.29. Ofertę, wraz ze stanowiącymi jej integralną część załącznikami, składa się pod rygorem nieważności w formie elektronicznej lub postaci elektronicznej za pośrednictwem Platformy, podpisaną kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
- 14.30. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
- 14.31. Osobami uprawnionymi do kontaktu z Wykonawcami są: Urszula Sobocińska – st. specjalista ds. zamówień publicznych, tel. (82) 562 32 47, e-mail: urszula.sobocinska@szpitalchelm.pl.

15. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ TREŚCI SWZ

- 15.1. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ, przekazany za pośrednictwem Platformy (karta "Zapytania/Wyjaśnienia").
- 15.2. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
- 15.3. Jeżeli wniosek o wyjaśnienie treści SWZ nie wpłynie w terminie, o którym mowa w punkcie powyżej, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ.
- 15.4. Przedłużenie terminu składania ofert, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
- 15.5. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępni na stronie internetowej prowadzonego postępowania, bez ujawniania źródła zapytania.
- 15.6. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej prowadzonego postępowania.

16. WYMAGANIA DOTYCZĄCE WADIUM

- 16.1. W postępowaniu nie jest przewidziane składanie wadium.

17. TERMIN ZWIĄZANIA OFERTĄ

- 17.1. Wykonawca pozostaje związany ofertą **do dnia 2 listopada 2023 r.**
- 17.2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

- 17.3. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, Zamawiający przed upływem tego terminu zwróci się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie terminu związania ofertą o wskazywany przez niego okres, nie dłuższy niż 30 dni.

18. OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

- 18.1. Wykonawca może złożyć tylko jedną ofertę.
- 18.2. Treść oferty musi być zgodna z wymaganiami Zamawiającego określonymi w niniejszej SWZ.
- 18.3. Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy, powinny być sporządzone zgodnie z tymi wzorami.
- 18.4. Oferta wraz ze stanowiącymi jej integralną część załącznikami musi być sporządzona w języku polskim i złożona pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej, za pośrednictwem Platformy oraz podpisana kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
- 18.5. Zamawiający informuje, iż zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), zwanej dalej „ustawą o zwalczaniu nieuczciwej konkurencji” jeżeli Wykonawca:
- 18.6. wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane;
- 18.7. wykazał, załączając stosowne uzasadnienie, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
- 18.8. Zaleca się, aby uzasadnienie o którym mowa powyżej było sformułowane w sposób umożliwiający jego udostępnienie pozostałym uczestnikom postępowania.
- 18.9. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp.
- 18.10. Opis sposobu przygotowania oferty składanej w formie elektronicznej lub w postaci elektronicznej:
- 18.11. Wykonawca, chcąc przystąpić do udziału w postępowaniu, loguje się na Platformie, w menu „Ogłoszenia” wyszukuje niniejsze postępowanie, otwiera je klikając w jego temat, a następnie korzysta z funkcji **”Zgłoś udział w postępowaniu”** na karcie Informacje ogólne”;
- 18.12. w przypadku, gdy Wykonawca nie posiada konta na Platformie, należy skorzystać z funkcji **”Zarejestruj”**. Po wypełnieniu Formularza rejestracyjnego Wykonawca otrzyma wiadomość e-mail na zdefiniowany adres poczty elektronicznej, z opcją aktywacji konta. Aktywacja konta jest konieczna do zakończenia procesu rejestracji i umożliwia zalogowanie się na Platformie;
- 18.13. oferta wraz ze stanowiącymi jej integralną część załącznikami, powinna być podpisana ważnym kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, przez osobę (osoby) uprawnione do reprezentowania Wykonawcy, zgodnie z formą reprezentacji określoną w dokumentach rejestrowych, a następnie przesłana Zamawiającemu za pośrednictwem Platformy, poprzez dodanie dokumentów na karcie ”Oferta/Załączniki”, za pomocą opcji **”Załącz plik”** i użycie przycisku **”Załącz”**;
- 18.14. jeżeli umocowanie dla osób podpisujących ofertę nie wynika z dokumentów rejestrowych, Wykonawca do oferty powinien dołączyć dokument pełnomocnictwa udzielonego przez osoby uprawnione i obejmujące swym zakresem umocowanie do złożenia oferty lub do złożenia oferty i podpisania umowy. Pełnomocnictwo powinno zostać złożone w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym albo w elektronicznej kopii dokumentu poświadczonej notarialnie za zgodność z oryginałem przy użyciu kwalifikowanego podpisu elektronicznego;
- a) wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji, które Wykonawca chce zastrzec jako tajemnicę przedsiębiorstwa, powinny zostać przesłane za pośrednictwem Platformy, w osobnym pliku, na karcie ”Oferta/Załączniki”, w tabeli ”Część oferty stanowiąca tajemnicę przedsiębiorstwa”, za pomocą opcji **”Załącz plik”** i użycie przycisku **”Załącz”**;

- a) potwierdzeniem prawidłowo załączonego pliku jest automatyczne wygenerowanie przez Platformę komunikatu systemowego o treści "Plik został poprawnie przesłany na platformę;
 - b) ostateczne złożenie oferty wraz z załącznikami Wykonawca musi potwierdzić klikając w przycisk "**Złóż ofertę**";
 - c) złożenie oferty zostanie potwierdzone komunikatem systemowym z podaniem terminu jej złożenia oraz aktywowana zostanie dla Wykonawcy możliwość pobrania, w stosunku do każdego z przesłanych plików, automatycznie wystawionego przez Platformę dokumentu EPO (Elektroniczne Potwierdzenie Odbioru), będącego dowodem potwierdzającym fakt i czas dostarczenia Zamawiającemu pliku za pośrednictwem Platformy.
- 18.15. Do upływu terminu składania ofert, Wykonawca, za pośrednictwem Platformy, może wycofać złożoną ofertę, używając opcji "**Wycofaj ofertę**" (karta Oferta/Załączniki). Po wycofaniu oferty Wykonawca może usunąć załączone pliki, zaznaczając pozycje do usunięcia i klikając w przycisk "**Usuń zaznaczone**".
- 18.16. Szczegółowa instrukcja korzystania z Platformy znajduje się na stronie internetowej <https://e-ProPublico.pl/>, przycisk "**Instrukcja Wykonawcy**".
- 18.17. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

19. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

- 19.1. Ofertę, wraz z załącznikami, należy złożyć za pośrednictwem Platformy w terminie **do dnia 4 października 2023 r. do godz. 9:00**.

20. TERMIN OTWARCIA OFERT

- 20.1. Otwarcie ofert nastąpi w dniu **4 października 2023 r. o godz. 9:30**, za pośrednictwem Platformy, na karcie "Oferta/Załączniki", poprzez ich odszyfrowanie, które jest jednoznaczne z ich upublicznieniem.
- 20.2. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
- 20.3. Niezwłocznie po otwarciu ofert, Zamawiający zamieści na stronie internetowej prowadzonego postępowania informacje o:
- 20.4. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej bądź miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
- 20.5. cenach lub kosztach zawartych w ofertach.

21. OPIS SPOSOBU OBLICZENIA CENY

- 21.1. W ofercie Wykonawca zobowiązany jest podać cenę za wykonanie całego przedmiotu zamówienia w złotych polskich (PLN), z dokładnością do 1 grosza, tj. do dwóch miejsc po przecinku.
- 21.2. W cenie należy uwzględnić wszystkie wymagania określone w niniejszej SWZ oraz wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia, a także wszystkie potencjalne ryzyka ekonomiczne, jakie mogą wystąpić przy realizacji przedmiotu zamówienia.
- 21.3. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich z dokładnością do dwóch miejsc po przecinku.
- 21.4. Wykonawca zobowiązany jest zastosować stawkę VAT zgodnie z obowiązującymi przepisami ustawy z 11 marca 2004 r. o podatku od towarów i usług.
- 21.5. Jeżeli złożona zostanie oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2021 r. poz. 685), dla celów zastosowania kryterium ceny Zamawiający doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.

- 21.6. Wykonawca składając ofertę zobowiązany jest:
- 21.7. poinformować Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
- 21.8. wskazać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
- 21.9. wskazać wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;
- 21.10. wskazać stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

22. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

- 22.1. Przy dokonywaniu wyboru najkorzystniejszej oferty Zamawiający stosować będzie niżej podane kryteria:

Zadanie	Nazwa kryterium - waga [%]
1	1 - Cena - 100

- 22.2. Punkty przyznawane za podane kryteria będą liczone według następujących wzorów:

Zadanie	Wzór
1	<p>1 - Cena</p> <p>Liczba punktów = $(C_{min}/C_{of}) * 100 * waga$</p> <p>gdzie:</p> <ul style="list-style-type: none"> - C_{min} - najniższa cena spośród wszystkich ofert - C_{of} - cena podana w ofercie

- 22.3. Po dokonaniu oceny punkty przyznane przez każdego z członków Komisji przetargowej zostaną zsumowane dla każdego z kryteriów oddzielnie. Suma punktów uzyskanych za wszystkie kryteria oceny stanowić będzie końcową ocenę danej oferty.
- 22.4. Zamawiający poprawi w ofercie:
- 22.5. oczywiste omyłki pisarskie,
- 22.6. oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
- 22.7. inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty
- 22.8. - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
- 22.9. Jeżeli zaoferowana cena, lub jej 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 w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, Zamawiający zażąda od Wykonawcy wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny, lub jej istotnych części składowych. Wyjaśnienia mogą dotyczyć zagadnień wskazanych w art. 224 ust. 3 ustawy Pzp.
- 22.10. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy.
- 22.11. Zamawiający odrzuci ofertę Wykonawcy, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdzi, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

- 22.12. Zamawiający odrzuci ofertę Wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają rażąco niskiej ceny tej oferty.

23. UDZIELENIE ZAMÓWIENIA

- 23.1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszej SWZ i została oceniona jako najkorzystniejsza w oparciu o podane w niej kryteria oceny ofert.
- 23.2. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający poinformuje równocześnie Wykonawców, którzy złożyli oferty, przekazując im informacje, o których mowa w art. 253 ust. 1 ustawy Pzp oraz udostępni je na stronie internetowej prowadzonego postępowania e-propublico.pl.
- 23.3. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może dokonać ponownego badania i oceny ofert, spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

24. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

- 24.1. Zamawiający zawrze umowę w sprawie zamówienia publicznego, w terminie i na zasadach określonych w art. 308 ust. 2 i 3 ustawy Pzp.
- 24.2. Zamawiający poinformuje Wykonawcę, któremu zostanie udzielone zamówienie, o miejscu i terminie zawarcia umowy.
- 24.3. Przed zawarciem umowy Wykonawca, na wezwanie Zamawiającego, zobowiązany jest do podania wszelkich informacji niezbędnych do wypełnienia treści umowy.
- 24.4. W przypadku wyboru oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Wykonawcy ci, na wezwanie Zamawiającego, zobowiązani będą przed zawarciem umowy w sprawie zamówienia publicznego przedłożyć kopię umowy regulującej współpracę tych Wykonawców.
- 24.5. Jeżeli Wykonawca nie dopełni ww. formalności w wyznaczonym terminie, Zamawiający uzna, że zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy i będzie upoważniony do zatrzymania wadium na podstawie art. 98 ust. 6 pkt 3 ustawy Pzp.

25. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

- 25.1. W danym postępowaniu wniesienie zabezpieczenie należytego wykonania umowy nie jest wymagane.

26. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

- 26.1. Wzór umowy stanowi załącznik nr 3 do niniejszej SWZ.

27. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

- 27.1. Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy Pzp, przysługują środki ochrony prawnej na zasadach przewidzianych w art. 505 – 590 ustawy Pzp.

28. AUKCJA ELEKTRONICZNA

- 28.1. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej, o której mowa w art. 308 ust. 1 ustawy Pzp.

29. OCHRONA DANYCH OSOBOWYCH

- 29.1. Zamawiający oświadcza, że spełnia wymogi określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 4 maja 2016 r.), dalej: RODO,

- tym samym dane osobowe podane przez Wykonawcę będą przetwarzane zgodnie z RODO oraz zgodnie z przepisami krajowymi.
- 29.2. Zamawiający informuje, że:
- 29.3. administratorem danych osobowych Wykonawcy jest **Samodzielny Publiczny Wojewódzki Szpital Specjalistyczny w Chełmie**, Ceramiczna 1, 22-100 Chełm.
- 29.4. Tel.: 82 562 32 54, e-mail: przetarg@szpitalchelm.pl;
- 29.5. w sprawach związanych z przetwarzaniem danych osobowych, można kontaktować się z Inspektorem Ochrony Danych, e-mail: inspektor@ethna.pl;
- 29.6. dane osobowe Wykonawcy będą przetwarzane w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego pn. **Zakup, dostawa i wdrożenie systemu kopii zapasowej oraz systemu ochrony poczty elektronicznej.** – znak sprawy: **ZP.3311.33.2023** oraz w celu archiwizacji dokumentacji dotyczącej tego postępowania;
- 29.7. odbiorcami przekazanych przez Wykonawcę danych osobowych będą osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy Pzp;
- 29.8. dane osobowe Wykonawcy będą przechowywane, zgodnie z art. 78 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli okres obowiązywania umowy w sprawie zamówienia publicznego przekracza 4 lata, okres przechowywania obejmuje cały okres obowiązywania umowy.
- 29.9. Wykonawca jest zobowiązany, w związku z udziałem w przedmiotowym postępowaniu, do wypełnienia wszystkich obowiązków formalno-prawnych wymaganych przez RODO i związanych z udziałem w przedmiotowym postępowaniu o udzielenie zamówienia. Do obowiązków tych należą:
- 29.10. obowiązek informacyjny przewidziany w art. 13 RODO względem osób fizycznych, których dane osobowe dotyczą i od których dane te Wykonawca bezpośrednio pozyskał i przekazał Zamawiającemu w treści oferty lub dokumentów składanych na żądanie Zamawiającego;
- 29.11. obowiązek informacyjny wynikający z art. 14 RODO względem osób fizycznych, których dane Wykonawca pozyskał w sposób pośredni, a które to dane Wykonawca przekazuje Zamawiającemu w treści oferty lub dokumentów składanych na żądanie Zamawiającego.
- 29.12. Zamawiający informuje, że;
- 29.13. udostępnia dane osobowe, o których mowa w art. 10 RODO (dane osobowe dotyczące wyroków skazujących i czynów zabronionych) w celu umożliwienia korzystania ze środków ochrony prawnej, o których mowa w dziale IX ustawy Pzp, do upływu terminu na ich wniesienie;
- 29.14. udostępnianie protokołu i załączników do protokołu ma zastosowanie do wszystkich danych osobowych, z wyjątkiem tych, o których mowa w art. 9 ust. 1 RODO (tj. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby), zebranych w toku postępowania o udzielenie zamówienia;
- 29.15. w przypadku korzystania przez osobę, której dane osobowe są przetwarzane przez Zamawiającego, z uprawnienia, o którym mowa w art. 15 ust. 1–3 RODO (związanych z prawem Wykonawcy do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jego dotyczące, prawem Wykonawcy do bycia poinformowanym o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem jego danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz prawem otrzymania przez Wykonawcę od administratora kopii danych osobowych podlegających przetwarzaniu), Zamawiający może żądać od osoby występującej z żądaniem wskazania dodatkowych informacji, mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia;
- 29.16. skorzystanie przez osobę, której dane osobowe są przetwarzane, z uprawnienia, o którym mowa w art. 16 RODO (uprawnienie do sprostowania lub uzupełnienia danych osobowych), nie może naruszać integralności protokołu postępowania oraz jego załączników;

- 29.17. w postępowaniu o udzielenie zamówienia zgłoszenie żądania ograniczenia przetwarzania, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia tego postępowania;
- 29.18. w przypadku, gdy wniesienie żądania dotyczącego prawa, o którym mowa w art. 18 ust. 1 RODO 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. 2 rozporządzenia 2016/679.

29.19. Załączniki do SWZ:

Nr	Nazwa załącznika
1	Formularz ofertowo-cenowy
2	Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału
3	Wzór umowy
4	Wykaz wymaganych parametrów technicznych

Dyrektor
Samodzielnego Publicznego
Wojewódzkiego Szpitala Specjalistycznego
w Chełmie

dr Kamila Ćwik
/podpis/