SP ZOZ Sanatorium Uzdrowiskowe MSWiA „AGAT” w Jeleniej Górze

SPECYFIKACJA
WARUNKÓW ZAMÓWIENIA

Postępowanie o udzielenie zamówienia publicznego na podstawie
ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych
(t.j. Dz. U. z 2024 r. poz. 1320 – dalej „PZP”).
Tryb postępowania: podstawowe oparte na art. 275 pkt 1 (bez negocjacji).

Zamawiający oczekuje, że Wykonawcy zapoznają się dokładnie z treścią niniejszej SWZ.
Wykonawca ponosi ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów,
oraz przedłożenia oferty nieodpowiadającej wymaganiom określonym przez Zamawiającego.
Zamawiający po terminie składania ofert nie będzie miał możliwości zmiany zasad
postępowania wskazanych w niniejszej SWZ.

Przedmiot zamówienia: „ZAKUP I DOSTAWA SPRZĘTU INFORMATYCZNEGO, OPROGRAMOWANIA WRAZ Z LICENCJAMI”

Składanie ofert następuje za pośrednictwem platformy e-Zamówienia dostępnej pod adresem internetowym: https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e

Nr postępowania: **1/2026**

Kierownik Zamawiającego

Signature Not Verified
Dokument podpisany przez
KATARZYNA NIEWĘGŁOWSKA
Data: 2026.05.05 12:26:39 CEST

/podpisano kwalifikowanym podpisem elektronicznym/

Spis treści

I. NAZWA I ADRES ZAMAWIAJĄCEGO.

1. NAZWA (FIRMA) ORAZ ADRES ZAMAWIAJĄCEGO

Zamawiający:	Samodzielny Publiczny Zakład Opieki Zdrowotnej Sanatorium Uzdrowiskowego MSWiA „Agat” w Jeleniej Górze
Adres :	Ul. Cervi 14, 58-560 Jelenia Góra
NIP:	6112223263
Numer telefonu:	75 75 520 64 do 68

2. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

   Postępowanie prowadzone jest przy użyciu środków komunikacji elektronicznej z wykorzystaniem Platformy **https://ezamowienia.gov.pl/pl/**
   Zamawiający informuje, że informacje dotyczące prowadzonego postępowania udostępnione stronie internetowej prowadzonego postępowania będą także udostępnione na stronie Zamawiającego (Biuletyn Informacji Publicznej): www.sanatorium-agat.pl

   Kanał komunikacji elektronicznej:
   https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e

   Identyfikator postępowania: ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e

II. TRYB UDZIELENIA ZAMÓWIENIA.

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest zgodnie z przepisami ustawy z dnia 24 października 2019 roku Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320) oraz aktów wykonawczych do tej ustawy, w trybie podstawowym, o którym mowa w art. 275 pkt 1 ustawy PZP, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji.
2. Realizacja zamówienia podlega prawu polskiemu, w tym w szczególności: ustawie PZP oraz ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061 z późn. zm.) zwanej dalej "Kc".
3. Postępowanie prowadzone jest z uwzględnieniem przepisów właściwych dla zamówień klasycznych o wartości mniejszej niż progi unijne określone w przepisach wskazanych w art. 3 ust. 1 ustawy PZP.
4. Postępowanie, którego dotyczy niniejsza SWZ, oznaczone jest znakiem**: 1/2026** i Wykonawcy zobowiązani są do powoływania się na podane oznaczenie we wszelkich kontaktach z Zamawiającym.
5. Postępowanie prowadzone jest w języku polskim. Wszelkie oświadczenia, zawiadomienia i inne dokumenty sporządzane w postępowaniu, jak również umowa w sprawie zamówienia publicznego, sporządzone będą w języku polskim.
6. W sprawach nie uregulowanych niniejszą Specyfikacją Warunków Zamówienia zwaną dalej „SWZ”, mają zastosowanie przepisy ustawy PZP oraz akty wykonawcze wydane na jej podstawie.
7. Rodzaj zamówienia: **dostawy**

III. INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PRZEPROWADZENIA NEGOCJACJI.

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA.

Przedmiot zamówienia:

ZAKUP I DOSTAWA SPRZĘTU INFORMATYCZNEGO, OPROGRAMOWANIA WRAZ Z LICENCJAMI.

NAZWY I KODY ZAMÓWIENIA WEDŁUG WSPÓLNEGO SŁOWNIKA ZAMÓWIEŃ (CPV):

48821000-9 Serwery sieciowe

48823000-3 Serwery plików

32420000-3 Urządzenia sieciowe

48000000-8 Pakiety oprogramowania i systemy informatyczne

48223000-7 Pakiety oprogramowania do poczty elektronicznej

48761000-0 Pakiety oprogramowania antywirusowego

1) Zamawiający informuje, że zamówienie zostało podzielone na 6 (sześć) części.

   Wykonawcy uprawnieni są do złożenia oferty na dowolną liczbę części zamówienia.

2) Wykonawca zobowiązany jest w szczególności dostarczyć przedmiot zamówienia Zamawiającemu na własny koszt do SP ZOZ Sanatorium Uzdrowiskowego MSWiA „Agat" w Jeleniej Górze przy ul. Cervi 14.
3) Przedmiot zamówienia musi być fabrycznie nowy, wolny od wad, wykonany z materiałów spełniających wymogi bezpieczeństwa użytkowania i ochrony zdrowia oraz posiadać wymagane certyfikaty, atesty i deklaracje zgodności – w zakresie wynikającym z obowiązujących przepisów prawa dla danego rodzaju produktu.

CZĘŚĆ 1- SERWER WIRTUALIZACYJNY – 1 SZTUKA

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max. 1U z możliwością instalacji min. 8 dysków 2,5" SATA z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 304 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla jednego procesora. Dla oferowanego serwera.

RAM	Min. 256GB DDR5 RDIMM 6400MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 2TB pamięci RAM.
Zabezpieczenia pamięci RAM	Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection
Gniazda PCIe	- minimum dwa sloty PCIe x16 generacji 5 i jeden slot OCP 3.0 x16.
Interfejsy sieciowe/FC/SAS	Dwa interfejsy sieciowe 10/25GbE SFP28, cztery interfejsy sieciowe 1GbE Base-T
Dyski twarde	Zainstalowane 5 x 1.92TB SSD SATA 6Gbps 512e 2.5in Hot-plug skonfigurowane fabrycznie w RAID 5. Zainstalowane dwa dyski 480GB SSD SATA 6Gbps 512e 2.5in Hot-plug z możliwością konfiguracji RAID 1.
Kontroler RAID	Główny kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Dodatkowy Kontorler typu BOSS.
Wbudowane porty	min. port USB 2.0 oraz 2 x USB 3.1, port VGA,
System operacyjny	Windows Server 2025 Standard na odpowiadającą ilość rdzeni procesora.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne.
Zasilacze	Min. dwa zasilacze Hot-Plug min. 800W Titanium każdy wraz z kablami zasilającymi o długości min. 2m.
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Możliwość integracji z RSA SecurID. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.
Karta Zarządzania	Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej:

	• zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje 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 podłączenia lokalnego poprzez złącze RS-232. • 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 komponentów serwera • 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 odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. Karta powinna umożliwiać rozszerzenie funkcjonalności o: • 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 **Na wezwanie Zamawiającego należy przedłożyć oświadczenie producenta serwera potwierdzające spełnienie powyższych wymagań.**

Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta serwera 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 oferowanego rozwiązania) • 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. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Normy Środowiskowe	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - ***Wykonawca złoży dokument na wezwanie Zamawiającego potwierdzający spełnianie* wymogu.** Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera.**
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2022, Microsoft Windows 2025 x64.
Warunki gwarancji	Zamawiający wymaga min. 60 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***wykonawcy / producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następny dzień roboczy od zakończenia

	diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu przedłożenia na wezwanie oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.** **Wymagane na wezwanie przez Zamawiającego oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.** **Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.**
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.

CZĘŚĆ 2- MACIERZ NAS – 1 sztuka

Nazwa komponentu	Opis minimalnych wymagań technicznych
Typ	Sieciowy serwer plików NAS
Obudowa	Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.
Procesor	Procesor klasy ARM, min. 4-rdzeniowy. Procesor osiągający w teście PassMark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 1100 pkt. według wyników publikowanych na stronie https://www.cpubenchmark.net/cpu-list/all
Pamięć RAM	2 GB UDIMM DDR4
Wewnętrzna pamięć masowa	3 dyski 8TB 3,5-calowe SATA 6 Gb/s, Zainstalowane dyski muszą znajdować się na liście kompatybilnych urządzeń publikowanej przez producenta serwera NAS. Możliwość dołożenia czwartego dysku.
Kompatybilność dysków	3,5-calowe wnęki: 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA
Interfejsy sieciowe	Min. 2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M), 2 x 10GbE SFP+
Złącza dodatkowe	Min. 2 porty typu A USB 3.2,
Gniazdo M.2	Opcjonalne, poprzez kartę PCIe
Szyfrowanie	AES 256bit

Zasilacz	250 W PSU, 100–240 V
Certyfikaty	Producent serwera NAS musi posiadać certyfikat jakości według normy ISO 9001 na produkcję oferowanego asortymentu lub równoważny certyfikat jakości oraz certyfikat według normy ISO 14001 Systemu Zarządzania Środowiskowego lub równoważną normę zarządzania środowiskowego.
Gwarancja producenta	5 lat gwarancji Next Business Day Onsite na serwer. 5 lat gwarancji Next Business Day na dyski.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej.

CZĘŚĆ 3-ZAAWANSOWANY FIREWALL NOWEJ GENERACJI (NGFW) – 2 sztuki

Wymagania ogólne:

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
5. System ma pracować w postaci redundantnego klastra.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 8 portami Gigabit Ethernet RJ-45.

- 2 gniazdami SFP 1 Gbps.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1.3 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall:

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN:

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN:

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.

2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN:

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem:

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware:

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami:

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji:

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW:

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji:

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie:

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie:

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne:

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

Serwisy i licencje:

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 60 miesięcy.

Gwarancja oraz wsparcie:

System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

CZĘŚĆ 4 –SCENTRALIZOWANY SYSTEM GROMADZENIA, ANALIZY I RAPORTOWANIA LOGÓW 1-sztuka

Wymagania Ogólne:

W ramach postępowania wymaganym jest dostarczenie systemu do zbierania, analizy i raportowania zdarzeń sieciowych i systemowych. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na Microsoft Hyper-V wersje 2019 i nowsze;

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 wirtualne interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.

2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie:

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie:

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów:

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.

- Email.
- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

Zarządzanie:

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje:

Wsparcie: System musi być objęty serwisem producenta przez okres min. 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

CZĘŚĆ 5 - SYSTEM OCHRONY POCZTY – 1 SZTUKA

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware-ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na Microsoft Hyper-V wersje 2019 i nowsze;

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego:

1. System musi obsługiwać co najmniej 4 wirtualne interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne funkcje systemu ochrony poczty:

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. 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.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware:

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.

6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. 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.
8. 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, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi 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.

Kontrola antyspamowa:

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. 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.

Ochrona przed atakami na usługę poczty:

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania:

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA):

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu:

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie:

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Certyfikaty:

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria evaluation in process (NIAP), FIPS 140-3 Certified.

Serwisy i licencje:

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres min. 60 miesięcy.

Gwarancja oraz wsparcie:

System musi być objęty serwisem producenta przez okres min. 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych:

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

CZEŚĆ 6- PROGRAM ANTYWIRUSOWY – 35 LICENCJI NA 3 LATA.

Centralne zarządzanie:

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).
2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim.
3. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID. 6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
5. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
6. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej:

- Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.
- Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
- Buforowanie ruchu HTTPS.

7. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
8. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
9. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe.
10. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
11. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie.
13. Rozwiązanie musi udostępniać możliwość tagowania obiektów.

14. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

Ochrona stacji roboczych - Windows :

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia sumy kontrolnej (SHA1).
12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
- Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
- Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
- Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

14. Rozwiązanie musi udostępniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi udostępniać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji.
18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

- tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:

- Antywiruzs
- Zapora osobista.
- Sandbox.
- Antyspyware.
- Metody heurystyczne.

20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
21. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
22. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    a. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - Skanowanie portów TCP oraz UDP,
        - Wykrywanie duplikacji adresu IP,
        - Atak zatruwania ARP,
        - Nieprawidłowa długość pakietu TCP oraz UDP.
    b. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        - RDP,
        - SMB,
        - My SQL, ➢ MS SQL.
    c. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
23. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    a. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    b. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        - tryb automatyczny
        - tryb interaktywny
        - tryb oparty na regułach
        - tryb uczenia się
24. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
    - Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
    - Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

- W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

25. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.

Ochrona serwera – Windows Server:

1. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft WS 2022, Microsoft WS 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia sumy kontrolnej (SHA1). Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
11. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
    B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. C. Raport musi posiadać co najmniej:
        - Listę zainstalowanych aplikacji,
        - Listę usług systemowych,
        - informacje o systemie operacyjnym i sprzęcie,

- Listę aktywnych procesów i połączeń sieciowych,
- harmonogram systemu operacyjnego,
- Szczegóły pliku hosts,
- Informacje o sterowników.

12. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
    - antywirus,
    - zapora osobista
    - sandbox,
    - antyspyware, ➢ metody heurystyczne.
13. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
14. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
15. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników.
16. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
    - MS SQL.
    - Active Directory.
    - IIS.
    - Sysvol.
    - DNS.
    - DHCP.
    - Hyper-V.
    - Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
17. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:

    - Skanowanie portów TCP oraz UDP,
    - Wykrywanie duplikacji adresu IP,
    - Atak zatruwania ARP,
    - Nieprawidłowa długość pakietu TCP oraz UDP.

    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:

    - RDP,
    - SMB,
    - My SQL, ➢ MS SQL.

    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

18. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
19. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

    A. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

    - tryb automatyczny
    - tryb interaktywny

- tryb oparty na regułach
- tryb uczenia się

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy w tym co najmniej:
   - Microsoft Windows 10 oraz 11,
   - Microsoft Windows Server,
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
   - archiwa,
   - skrypty,
   - pliki wykonywalne,
   - pliki rejestru systemowego (.reg), ➢ możliwy spam, ➢ dokumenty.
7. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
8. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
9. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
10. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
    - czysty,
    - podejrzany,
    - bardzo podejrzany,
    - szkodliwy.
13. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

Endpoint Detection and Response / eXtended Detection and Response:

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
   - Tworzenie procesów.
   - Uruchamianie, zatrzymanie i modyfikacja usług.

- Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym.
- Usuwanie oraz zmiana nazw plików.
- Tworzenie i usuwanie kluczy rejestru systemowego.
- Ładowanie bibliotek DLL.
- Zalogowanie użytkowników.

A. elementy sieciowe, w tym co najmniej:

- Pobranie plików wykonywalnych.
- Zestawienie połączeń TCP/IP.
- Zapytania http.
- Zapytania DNS.

4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.
   A. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
      - Blokowanie pliku wykonywalnego.
      - Blokowanie pliku wykonywalnego i poddanie go kwarantannie.
      - Blokowanie podejrzanej biblioteki DLL.
      - Zakończenie procesu.
      - Skanowanie komputera w poszukiwaniu zagrożeń.
      - Wyłączenie komputera.
      - Izolacja sieciowa hosta dla systemów Windows oraz Linux. ➢ Wylogowanie użytkownika.

   B. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
   A. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
   B. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:
      - Proces.
      - Proces nadrzędny (proces rodzica).
      - Nazwę procesu.
      - Ścieżkę procesu.
      - Wiersz polecenia.
      - Wydawcę.
      - Typ podpisu cyfrowego.
      - SHA-1.
      - SHA-2.
      - Użytkownika.

   C. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.

6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
   A. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
   B. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):

- SHA-1.
- SHA-256.

7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
    - Hash pliku SHA-1.
    - Hash pliku SHA-256.
    - Hash pliku MD5.
    - Typ sygnatury podpisu cyfrowego.
    - Wydawcę certyfikatu.
    - Wersję pliku.
    - Oryginalną nazwę pliku.
    - Rozmiar pliku.
    - Reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego.
    - Pierwsze uruchomienie pliku w środowisku. ➢ Ostatnie uruchomienie pliku w środowisku.
8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
    - Oznaczania ich jako bezpieczne lub niebezpieczne.
    - Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, ➢ Zablokowania wykonywania i wykorzystania pliku.
    - Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
    - Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
    - Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, ➢ Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
    - Administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
    - Administrator musi posiadać możliwość odczytania informacji o języku skryptu.
10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
    ➢ Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.
13. Rozwiązanie musi umożliwiać moduł zaawansowanego wyszukiwania, które umożliwia badanie wskaźników danych zawartych w XDR.

<u>Ochrona serwerów w chmurze AWS, Microsoft Azure i Google Cloud Platform:</u>

1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
2. Rozwiązanie musi udostępniać możliwość integracji przynajmniej z rozwiązaniami: Microsoft Azure, Google Cloud Platform. ➢ Amazon Web Services.

3. Rozwiązanie powinno zapewniać możliwość zarówno automatycznego uruchamiania ochrony dla nowych i już istniejących maszyn wirtualnych, jak i ręcznego wskazania wybranych zasobów do objęcia ochroną.

Wsparcie techniczne czas licencji oraz Gwarancja

1. System musi być objęty licencją i serwisem producenta przez okres min. 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
2. Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.
3. Licencja będzie obowiązywać od 05.11.2026 r. , tj od zakończenia licencji dotychczasowego oprogramowania.

V. TERMIN WYKONANIA ZAMÓWIENIA

1. Zamawiający określa następujący termin realizacji Przedmiotu Umowy:
   Przedmiot umowy zostanie zrealizowany przez Wykonawcę w terminie:

   Do 90 dni od dnia podpisania umowy.

2. Zamawiający nie dopuszcza zmiany terminu realizacji zamówienia.

VI. WARUNKI UDZIAŁU W POSTEPOWANIU.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

1. spełniają warunki udziału w postępowaniu dotyczące:
   a) zdolności do występowania w obrocie gospodarczym:
   Zamawiający nie określa warunku w tym zakresie.

   b) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:
   Zamawiający nie określa warunku w tym zakresie.

   c) sytuacji finansowej lub ekonomicznej:
   Zamawiający nie określa warunku w tym zakresie.

   d) zdolności technicznej lub zawodowej:

Wykonawca spełni warunek, jeżeli w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – wykonał co najmniej 1 dostawę (zawartą umowę na dostawę), oraz załączy na wezwanie dowody określające, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane co najmniej 12 miesięcy.

Dla części nr 1 i 5:

polegające na dostawie sprzętu informatycznego np. zestawów komputerowych, sprzętu multimedialnego, urządzeń wielofunkcyjnych, sprzętu i osprzętu informatycznego oraz oprogramowania o wartości co najmniej 50 000,00 zł brutto**.**

Dla części nr 2, 3, 4, 6:

polegające na dostawie sprzętu informatycznego np. zestawów_komputerowych, sprzętu multimedialnego, urządzeń wielofunkcyjnych, sprzętu i osprzętu informatycznego oraz oprogramowania o wartości co najmniej 17 000,00 zł brutto**.**

VII. PODSTAWY WYKLUCZENIA.

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych:
   1) w art. 108 ust. 1 PZP.;
   2) w art. 109 ust. 1 pkt. 4, PZP., tj.:
   a) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
   3) art. 7 ust. 1 pkt 1-3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz. U. z 2025 r. poz. 514).
   4) art. 5k Rozporządzenia Rady (UE) 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz.U. L 111/1 z 8.4.2022).
2. Wykluczenie Wykonawcy następuje zgodnie z art. 110 i 111 PZP
3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2, 5 PZP lub art. 109 ust. 1 pkt 4 PZP, jeżeli udowodni Zamawiającemu, że spełnił łącznie przesłanki wskazane w art. 110 ust. 2 PZP.
4. Zamawiający oceni, czy podjęte przez Wykonawcę czynności, o których mowa w art. 110 ust. 2 PZP, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy. Jeżeli podjęte przez Wykonawcę czynności nie są wystarczające do wykazania jego rzetelności, Zamawiający wyklucza Wykonawcę.

VIII. DOKUMENTY I OŚWIADCZENIA JAKIE SA ZOBOWIĄZANI DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTEPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA (W TYM PODMIOTOWE ŚRODKI DOWODOWE).

Na ofertę składają się następujące dokumenty i oświadczenia:

1. Formularz ofertowy wypełniony i podpisany przez Wykonawcę wg wzoru stanowiącego **załącznik nr 1 do SWZ.**
2. Oświadczenie o braku podstaw do wykluczenia, sporządzone zgodne ze wzorem stanowiącym **załącznik nr 2 do SWZ.**
3. Oświadczenia o aktualności informacji podanych w oświadczeniu z art. 125 ust. 1 PZP **załącznik nr 3 do SWZ.**
   W przypadku wspólnego ubiegania się o zamówienie przez wielu Wykonawców, oświadczenie składa każdy z Wykonawców, oświadczenia te potwierdzają brak podstaw wykluczenia.
4. **W przypadku gdy oferta nie została podpisana przez osobę uprawnioną do reprezentacji Wykonawcy określoną w odpowiednim rejestrze lub innym dokumencie właściwym dla danej formy organizacyjnej**

Wykonawcy, <u>do oferty należy dołączyć pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy</u> w formie elektronicznej.

5. **Załącznik nr 4 do SWZ.** Oświadczenie o udostępnieniu zasobów (podpisuje podmiot udostępniający zasoby). Dokument należy dołączyć do oferty - jeżeli ma zastosowanie.
6. **Załącznik nr 5 do SWZ -** Oświadczenie Wykonawców składający ofertę wspólnie (gdy ma zastosowanie).
7. Oświadczenia, o których mowa wyżej stanowią dowód potwierdzający brak podstaw wykluczenia na dzień składania ofert. Oświadczenie te składa się, pod rygorem nieważności, w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
8. Jeżeli złożone przez wykonawcę oświadczenie, o którym mowa w art. 125 ust. 1 PZP, lub podmiotowe środki dowodowe budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełniania przez Wykonawcę warunków udziału w postępowaniu lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.
9. W przypadku oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum, spółka cywilna):

- w formularzu oferty należy wskazać firmy (nazwy) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
- oferta musi być podpisana w taki sposób, by wiązała prawnie wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Osoba podpisująca ofertę musi posiadać umocowanie prawne do reprezentacji. Umocowanie musi wynikać z treści pełnomocnictwa załączonego do oferty – treść pełnomocnictwa powinna dokładnie określać zakres umocowania;
- wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia będą ponosić odpowiedzialność solidarną za wykonanie umowy.

10. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
11. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 PZP, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
12. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 PZP, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.

Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych jeśli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005r. informatyzacji działalności podmiotów realizujących zadnia publiczne (tekst jedn. Dz. U. z 2023 r. poz. 57 z późn. zm.), o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 PZP, dane umożliwiające dostęp do tych środków

Dokumenty składane na wezwanie przez Zamawiającego:

13. **Załącznik nr 6_wez - Wykaz dostaw** – wzór (dołączyć referencje).
14. Oświadczenie o spełnieniu norm środowiskowych - dotyczy części 1 (pierwszej) przedmiotu zamówienia.
15. Oświadczenie potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta- dotyczy części 1 (pierwszej) przedmiotu zamówienia.
16. Oświadczenie potwierdzające spełnienie wymagań Karty Zarządzania- dotyczy części 1 (pierwszej) przedmiotu zamówienia.
17. Oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta - dotyczy części 1 (pierwszej) przedmiotu zamówienia.

Wykaz dostaw (odrębnie do każdej części zamówienia na którą wykonawca złożył ofertę) porównywalnych z dostawami stanowiącymi przedmiot zamówienia, wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy – zgodnie z warunkiem postawionym w rozdziale VI - wg **Załącznika nr 6_wez do SWZ**,

IX. ŚRODKI KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIĘ KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ WYMAGANIA TECHNICZNE DLA DOKUMENTÓW ELEKTRONICZNYCH ORAZ ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ.

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem https://ezamowienia.gov.pl.
2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
3. Adres strony internetowej prowadzonego postępowania (link prowadzący bezpośrednio do widoku postępowania na Platformie e-Zamówienia) podany jest w rozdziale I. Postępowanie można wyszukać również ze strony głównej Platformy e-Zamówienia (przycisk „Przeglądaj postępowania/konkursy").
4. Identyfikator (ID) **postępowania na Platformie e-Zamówienia**: ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e
5. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca" na Platformie e- Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej https://ezamowienia.gov.pl oraz informacje zamieszczone w zakładce „Centrum Pomocy".
6. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
7. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w Rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub w konkursie (Dz. U. z 2020 r. poz. 2452).
8. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia, o którym mowa w ust. 7, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773), z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki. W przypadku formatów, o których mowa w art. 66 ust. 1 Ustawy, ww. regulacje nie będą miały bezpośredniego zastosowania.
9. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych (wskazanego w ust. 7), przekazywane w postępowaniu sporządza się w postaci elektronicznej:
    1) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (i przekazuje się jako załącznik), lub

2) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji").

10. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2022 r. poz. 1233) wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa".
11. Komunikacja w postępowaniu, z wyłączeniem składania ofert o dopuszczenie do udziału w postępowaniu, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze" („Formularze do komunikacji"). Za pośrednictwem „Formularzy do komunikacji" odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik"). W przypadku załączników, które są zgodnie z Ustawą lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym mogą być opatrzone, zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem zewnętrznym lub wewnętrznym. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się do przesyłanej wiadomości uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
12. Możliwość korzystania w postępowaniu z „Formularzy do komunikacji" w pełnym zakresie wymaga posiadania konta „Wykonawcy" na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji" służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.
13. Wszystkie wysłane i odebrane w postępowaniu przez Wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja".
14. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji" wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
15. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
16. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (22) 458 77 99 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce „Zgłoś problem".
17. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: sekretariat@sanatorium-agat.pl (nie dotyczy składania ofert/wniosków o dopuszczenie do udziału w postępowaniu).

X. SPOSÓB OBLICZANIA CENY OFERTY.

1. Cena oferty zostanie wyliczona przez Wykonawcę na załączonym Formularzu oferty, zgodnie z treścią niniejszej Specyfikacji.
2. Cena oferty powinna zawierać wszystkie koszty i składniki związane z wykonaniem zamówienia.
3. Podana wycena będzie stanowić o podstawie rozliczenia realizacji przedmiotu zamówienia.
4. Wykonawca oszacuje wszystkie koszty związane z realizacją przedmiotu umowy, a także oddziaływania innych czynników mających lub mogących mieć wpływ na koszty.
5. W Formularzu oferty należy podać cenę netto, określić procentowo wysokość podatku VAT i podać cenę brutto, z dokładnością do 0,01 zł.
6. Obowiązuje zasada zaokrąglania „w górę" liczby „5" występującej na trzecim miejscu po przecinku np. 4,375 =4,38

7. Cena oferty określona przez Wykonawcę zostanie ustalona na okres ważności umowy wg zasad wskazanych w projekcie umowy – **Załącznik nr 7 do SWZ.**
8. Rozliczenia pomiędzy Zamawiającym a Wykonawcą będą prowadzone w walucie PLN.
9. Cena musi być wyrażona w złotych polskich niezależnie od wchodzących w jej skład elementów. Tak obliczona cena będzie brana pod uwagę przez Zamawiającego w trakcie wyboru najkorzystniejszej oferty.
10. Cena oferty musi zawierać wszystkie koszty związane z realizacją zadania, zgodnie z opisem przedmiotu zamówienia. Ceny jednostkowe wskazane w wypełnionym przez Wykonawcę formularzu ofertowym w ofercie muszę uwzględniać wszystkie upusty, rabaty oraz opłaty mające wpływ na cenę oferty. Zamawiający nie dopuszcza możliwości wprowadzenia do oferty dodatkowych metod rozliczeń mających wpływ na cenę oferty lub sposób realizacji umowy.
11. Wykonawca ponosi wyłączną odpowiedzialność za zastosowane przez niego stawki podatku VAT niezgodnej z obowiązującymi przepisami.
12. Umowna cena musi zawierać wszelkie wydatki oraz ryzyko związane z koniecznością zrealizowania przedmiotu zamówienia, wszystkie koszty związane z wykonaniem przedmiotu zamówienia oraz koszty robót, usług i czynności nie wymienionych, a których wykonanie, wg Wykonawcy, jest niezbędne do prawidłowego wykonania przedmiotu zamówienia i uzyskania założonego efektu końcowego zadania.

XI. OPIS SPOSOBU PRZYGOTOWANIA I SKŁADANIA OFERTY.

1. Wykonawca ma prawo złożyć tylko jedną ofertę na daną część zamówienia, zawierającą jedną, jednoznacznie opisaną propozycję cenową. Złożenie większej liczby ofert w danej części zamówienia spowoduje odrzucenie wszystkich ofert złożonych w danej części przez danego Wykonawcę. Formularz oferty stanowi **Załącznik do SWZ nr 1 formularz oferty.**
2. Oferta musi być sporządzona pod rygorem nieważności w formie elektronicznej (w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Po podpisaniu nie należy zmieniać nazwy pliku formularza. W przypadku kwalifikowanego podpisu elektronicznego zaleca się korzystanie z opcji znacznika czasu.
3. Wszystkie oświadczenia i dokumenty składane wraz z ofertą muszą być sporządzone w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym (formie elektronicznej), w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
4. Oferta musi być napisana w języku polskim oraz podpisana przez osobę(y) upoważnioną do reprezentowania Wykonawcy i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty. Zamawiający wymaga, aby ofertę oraz wszystkie dokumenty składane wraz z ofertą podpisano zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub ewidencji działalności gospodarczej. Jeżeli osoby podpisujące ofertę działają na podstawie pełnomocnictwa, to pełnomocnictwo to musi obejmować uprawnienie do podpisania oferty.
5. Oferta musi być złożona w oryginale.
6. Oferta musi być sporządzona zgodnie z treścią formularza „Oferta Wykonawcy". Integralną część oferty stanowi opis oferowanego przedmiotu
7. Wraz z ofertą musi zostać złożone oświadczenia i dokumenty wskazane **w SWZ.**
8. Ofertę należy złożyć zgodnie z przepisami prawa oraz niniejszą specyfikacją, tj. zgodnie z treścią formularza oferty, z podaniem ceny netto, stawki i wartości podatku VAT oraz ceny brutto za wykonanie przedmiotu zamówienia.
9. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom). Zamawiający wymaga wskazania przez Wykonawcę, w ofercie, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.
10. Oferta musi być czytelna, spełniająca wymagania SWZ oraz treści aktów wykonawczych do ustawy PZP.
11. Gdy w składanych dokumentach, oświadczeniach pojawiają się informacje stanowiące tajemnicę przedsiębiorstwa:

1) Wykonawca powinien wskazać w sposób nie budzący wątpliwości, które informacje stanowią tajemnicę przedsiębiorstwa oraz powinien zastrzec, wraz z przekazaniem tych informacji, że nie mogą one być udostępniane. Wykonawca dla skuteczności wniesionego zastrzeżenia ma jednocześnie obowiązek wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. 2020 r. poz. 1913). Wykonawca musi zatem wykazać, iż zastrzeżone informacje, jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne i są to informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, oraz że uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp.
2) Powyższe informacje powinny zostać złożone w osobnym odpowiednio oznaczonym, jako tajemnica przedsiębiorstwa, pliku. Proponuje się, aby w nazwie pliku pojawił się opis, przykładowo: TP, tajemnica, ….
3) Powyższe zasady mają również zastosowanie do informacji stanowiących tajemnicę przedsiębiorstwa, zawartych w szczególności w oświadczeniach lub dokumentach oraz ich wyjaśnieniach lub uzupełnieniach, składanych przez Wykonawcę w toku postępowania o udzielenie zamówienia publicznego, przy czym wskazanie tych informacji oraz wykazanie, że stanowią one tajemnicę przedsiębiorstwa powinno nastąpić najpóźniej wraz z ich przekazaniem przez Wykonawcę.

12. Koszty związane z przygotowaniem oferty ponosi Wykonawca składający ofertę.

13. Wykonawca może – przed upływem terminu składania ofert - wprowadzić zmiany, poprawki, modyfikacje i uzupełnienie do złożonej oferty.
14. Wykonawca ma prawo, przed upływem terminu składania ofert wycofać złożoną przez siebie ofertę. W przypadku złożenia przez Wykonawcę dwóch lub więcej ofert na jedną część, oferty te zostaną odrzucone.
15. Zamawiający odrzuci ofertę gdy zajdą przesłanki opisane w art. 226 ustawy Pzp.
16. Postanowienia dotyczące prowadzenia przez Zamawiającego wyjaśnień w toku badania i oceny ofert:
    1) Zamawiający może wezwać Wykonawców do złożenia, uzupełnienia, poprawienia lub uzupełnienia oświadczenia wykonawcy, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń na zasadach określonych w art. 128 ustawy Pzp.
    2) Zamawiający poprawia w ofercie oczywiste omyłki pisarskie oraz oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
    3) Zamawiający poprawia w ofercie inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona, wyznaczając jednocześnie Wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie sposobu jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.
    4) Jeżeli zaoferowana cena lub koszt, lub ich istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia lub budzą wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w niniejszej specyfikacji lub wynikającymi z odrębnych przepisów, Zamawiający zażąda od Wykonawcy wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu, lub ich istotnych części składowych. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na Wykonawcy. Odrzuceniu, jako oferta z rażąco niską ceną lub kosztem, podlega oferta Wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają rażąco niskiej ceny lub kosztu tej oferty.
17. Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop („przeciągnij” i „upuść”) służące do dodawania plików.
18. Wykonawca dodaje wybrany z dysku i uprzednio podpisany „Formularz oferty” w pierwszym polu (Wypełniony formularz oferty”). W kolejnym polu („Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”) Wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
19. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” dodaje się uprzednio podpisane dokumenty wraz

z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny). W przypadku przekazywania dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

20. System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym Wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce „Oferty/Wnioski".
21. Oferta może być złożona tylko do upływu terminu składania ofert.
22. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski" używając przycisku „Wycofaj ofertę".
23. Sposób złożenia oferty oraz załączników został opisany w interaktywnej instrukcji „Oferty, wnioski i prace konkursowe", zamieszczonej na platformie e-zamówienia.
24. Maksymalny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250MB.

XII. WADIUM.

1. Zamawiający nie wymaga wniesienia wadium.

XIII. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI.

1. Zamawiający nie dopuszcza niżej wymienionych środków porozumiewania się czy komunikacji w postępowaniu:
   - za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012r. - Prawo pocztowe (t.j. Dz. U. z 2025 r. poz. 366).w jakiejkolwiek formie,
   - za pośrednictwem posłańca,
   - telefonicznie,
   - osobiste doręczenie przesyłki, zapytania, dokumentów, oświadczeń, wyjaśnień lub oferty.

2. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
3. Zamawiający jest obowiązany udzielić 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.
4. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w pkt 3, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych Wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.
5. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w pkt 3, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
6. Przedłużenie terminu składania ofert, o których mowa w pkt 5, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
7. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępnia, bez ujawniania źródła zapytania, na stronie internetowej prowadzonego postępowania.

Zmiany w treści SWZ

1. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę Zamawiający zamieści na stronie internetowej, na której udostępniono SWZ. Odpowiedzi na pytania oraz zmiany stanowią integralną treść SWZ.

2. W przypadku gdy zmiana treści SWZ jest istotna dla sporządzenia oferty lub wymaga od Wykonawców dodatkowego czasu na zapoznanie się ze zmianą treści SWZ i przygotowanie ofert, Zamawiający przedłuża termin składania ofert o czas niezbędny na ich przygotowanie. Zamawiający informuje Wykonawców o przedłużonym terminie składania odpowiednio ofert przez zamieszczenie informacji na stronie internetowej prowadzonego postępowania, na której została udostępniona SWZ oraz zamieszczenie ogłoszenia o zmianie ogłoszenia w Biuletynie Zamówień Publicznych.

Osobą wyznaczoną do kontaktu i porozumiewania się z wykonawcami jest:

Stanowisko: Kierownik działu organizacyjno-kadrowego
Imię i nazwisko: Paweł Lewandowski
W godzinach 7:30-14.30 od poniedziałku do piątku poza dniami wolnymi od pracy.

Zamawiający nie przewiduje:
- „obowiązkowej" wizji lokalnej wynikającej z art. 131 ust. 2 pkt 1 ustawy PZP,
- zebrania wykonawców.

XIV. TERMIN SKŁADANIA i OTWARCIA OFERT.

1. Oferty wraz z wymaganymi załącznikami należy złożyć w sposób opisany w niniejszej SWZ **w terminie do dnia 18.05.2026 r. do godziny: 09.00**
2. **Otwarcie ofert w dniu 18.05.2026 r. o godzinie 10:00.**
3. Oferta może być złożona tylko do upływu terminu składania ofert.
4. Przed terminem otwarcia ofert na stronie prowadzonego postępowania udostępniona informacja o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Oferty złożone po terminie wskazanym w ust. 1 zostaną odrzucone.
6. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii. Informacja o ostatecznym terminie otwarcia ofert zostanie udostępniona na stronie internetowej prowadzonego postępowania.

XV. TERMIN ZWIĄZANIA OFERTĄ.

1. Wykonawca będzie związany ofertą do upływu następującego terminu: 16.06.2026 r. .
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w ust. 1, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, **nie dłuższy niż 30 dni.**
3. Przedłużenie terminu związania ofertą wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

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

1. Kryteria oceny ofert - zamawiający uzna oferty za spełniające wymagania i przyjmie do szczegółowego rozpatrywania, jeżeli:
   1) oferta, spełnia wymagania określone niniejszą specyfikacją,
   2) oferta została złożona, w określonym przez Zamawiającego terminie,
   3) Wykonawca przedstawił ofertę zgodną co do treści z wymaganiami Zamawiającego.

1. Przy wyborze oferty Zamawiający będzie się kierował kryterium cenowym w części nr 1, w części nr 2 i 3 kryterium cenowym oraz czasowym (tj. z uwzględnieniem terminu dostawy przedmiotu zamówienia), w części nr 4, części nr 5 i części nr 6 kryterium cenowym i czasowym (tj. wydłużeniem wsparcia oraz licencji aktualizacyjnej).
2. Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu oraz dane – ceny wskazane jej treści.
3. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.
4. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą, określonym w SWZ.
5. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
6. W przypadku braku zgody, o której mowa w ust. 7 oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.
7. **Za najkorzystniejszą ofertę uznana zostanie oferta, która uzyska największą ilość punktów.**
8. Przy wyborze i ocenianiu ofert uznanych za ważne Zamawiający będzie się kierował następującym kryteriami:

1) Dotyczy części 1

Kryterium	Waga [%]	Liczba punktów	Sposób oceny wg wzoru
Łączna ofertowa cena brutto	**100%**	**100**	**CN Cena najtańszej oferty nie podlegającej odrzuceniu** **C = ---------- x 100pkt** **CB Cena badanej oferty**
RAZEM	**100%**	**100**	———————————

Cena oferty (C) za realizację całego zamówienia według następującego wzoru:

C- liczba punktów otrzymanych przez ofertę badaną w kryterium „Cena oferty”
CN - najniższa cena spośród wszystkich ofert podlegających ocenie
CB - cena w ofercie badanej

1. Do oceny oferty w tym kryterium Zamawiający przyjmie cenę brutto oferty zaoferowaną przez
2. Wykonawcę w Formularzu oferty.
3. Dla kryteriów oceny ofert przyjmuje się, iż 1% wagi kryterium = 1 pkt i tak zostanie przeliczona liczba punktów.
4. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą liczbę punktów wyliczoną w zaokrągleniu do dwóch miejsc po przecinku.
5. Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

2) <u>Dotyczy części 2, części 3</u>

Kryterium	Waga [%]	Liczba punktów	Sposób oceny wg wzoru
Łączna ofertowa cena brutto	**60%**	**60**	**Cena najtańszej oferty nie podlegającej odrzuceniu** **C = ---------- x 60pkt** **Cena badanej oferty**
Termin dostawy	**40%**	**40**	**P=** 1) Termin dostawy do 60 dni od podpisania umowy-40 pkt; 2) Termin dostawy 61-90 dni od podpisania umowy-20 pkt. 3) Termin dostawy powyżej 90 dni -0 pkt.
RAZEM	**100%**	**100**	———————————

1. **Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:**

L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Termin dostawy”

2. Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
3. Ocena punktowa w kryterium „Termin dostawy”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
4. Ocena ofert w oparciu o kryterium „Termin dostawy” klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:

- Termin dostawy do 60 dni od podpisania umowy **40 pkt;**
- Termin dostawy 61-90 dni od podpisania umowy **20 pkt;**
- Termin dostawy powyżej 90 dni od podpisania umowy **0 pkt;**

5. Ocena ofert w oparciu o kryterium „Termin dostawy” rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
6. Najkrótszy możliwy czas dostawy towaru to termin do 60 dni od podpisania umowy.
7. Najdłuższy możliwy czas dostawy towaru to termin powyżej 90 dni.
8. Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu dostawy zamawiający przyjmie do oceny maksymalny możliwy czas (czyli 90 dni), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
9. Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
10. W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
11. Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

3) Dotyczy części 4, części 5

Kryterium	Waga [%]	Liczba punktów	Sposób oceny wg wzoru
Łączna ofertowa cena brutto	**60%**	**60**	**Cena najtańszej oferty nie podlegającej odrzuceniu** **C = ---------- x 60pkt** **Cena badanej oferty**
Wydłużenie wsparcia oraz licencji aktualizacyjnej	**40%**	**40**	**P=** 1. Wydłużenie wsparcia do 66 miesięcy - 40 pkt; 2. Wydłużenie wsparcia od 61 do 65 miesięcy -20 pkt. 3. Wydłużenie wsparcia do 60 miesięcy -0 pkt.
RAZEM	**100%**	**100**	———————————

1. **Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:**

L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”

2. Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
3. Ocena punktowa w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
4. Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:
   - Wydłużenie wsparcia do 66 miesięcy - 40 pkt;
   - Wydłużenie wsparcia od 61 do 65 miesięcy -20 pkt.
   - Wydłużenie wsparcia do 60 miesięcy -0 pkt
5. Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
6. Najkrótszy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 60 miesięcy.
7. Najdłuższy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 66 miesięcy.
8. Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu na wydłużenie wsparcia oraz licencji aktualizacyjnej zamawiający przyjmie do oceny minimalny możliwy czas (czyli 60 miesięcy), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
9. Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
10. W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
11. Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4) Dotyczy części 6.

Kryterium	Waga [%]	Liczba punktów	Sposób oceny wg wzoru
Łączna ofertowa cena brutto	**60%**	**60**	**Cena najtańszej oferty nie podlegającej odrzuceniu** **C = ---------- x 60pkt** **Cena badanej oferty**
Wydłużenie wsparcia oraz licencji aktualizacyjnej	**40%**	**40**	**P=** 1. Wydłużenie wsparcia do 42 miesięcy - 40 pkt; 2. Wydłużenie wsparcia od 37 do 41 miesięcy - 20 pkt. 3. Wydłużenie wsparcia do 36 miesięcy -0 pkt.
RAZEM	**100%**	**100**	———————————

1. **Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:**

L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”

2. Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
3. Ocena punktowa w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
4. Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:
   - Wydłużenie wsparcia do 42 miesięcy - 40 pkt;
   - Wydłużenie wsparcia od 37 do 41 miesięcy -20 pkt.
   - Wydłużenie wsparcia do 36 miesięcy -0 pkt
5. Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
6. Najkrótszy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 36 miesięcy.
7. Najdłuższy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 42 miesięcy.
8. Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu na wydłużenie wsparcia oraz licencji aktualizacyjnej zamawiający przyjmie do oceny minimalny możliwy czas (czyli 36 miesięcy), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
9. Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
10. W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
11. Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

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

1. Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę.
2. Zamawiający niezwłocznie poinformuje wszystkich Wykonawców o wyborze najkorzystniejszej oferty.
3. Zawiadomienie o wyborze najkorzystniejszej oferty zawierać będzie uzasadnienie faktyczne i prawne oraz zamieszczone zostanie na stronie prowadzonego postępowania e-zamówienia.
4. O unieważnieniu postępowania o udzielenie zamówienia Zamawiający zawiadamia równocześnie Wykonawców, którzy złożyli oferty lub wnioski o dopuszczenie do udziału w postępowaniu lub zostali zaproszeni do negocjacji - podając uzasadnienie faktyczne i prawne.
5. W przypadku unieważnienia postępowania o udzielenie zamówienia, zamawiający na wniosek wykonawcy, który ubiegał się o udzielenie zamówienia, zawiadomi o wszczęciu kolejnego postępowania, które dotyczy tego samego przedmiotu zamówienia lub obejmuje ten sam przedmiot zamówienia.
6. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni - jeżeli zostało przesłane w inny sposób.

Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 6, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę.

7. O miejscu i terminie podpisania umowy Zamawiający powiadomi wybranego Wykonawcę.
8. W przypadku, gdy okaże się, że Wykonawca, którego oferta została wybrana będzie uchylał się od zawarcia umowy Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny, chyba, że zachodzi jedna z przesłanek unieważnienia postępowania.

XVIII. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY.

1. Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XIX. INNE POSTANOWIENIA ZAMAWIAJĄCEGO.

1. Zamawiający nie wymaga przedłożenia przedmiotowych środków dowodowych.
2. Zamawiający nie przewiduje zawarcia umowy ramowej.
3. Zamawiający nie dopuszcza składania ofert wariantowych.
4. Zamawiający nie przewiduje rozliczenia w walutach obcych.
5. Zamawiający nie przewiduje aukcji elektronicznej.
6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
7. Uczestnicy postępowania mają prawo wglądu do treści protokołu postępowania oraz do załączników do protokołu. Protokół postępowania jest jawny i udostępniany na wniosek.
8. Załącznikami do protokołu postępowania są w szczególności: Oferty, opinie biegłych, oświadczenia, informacja z zebrania z wykonawcami, zawiadomienia, wnioski, dowód przekazania ogłoszenia do BZP, inne dokumenty i informacje składane przez zamawiającego i wykonawców oraz umowa w sprawie zamówienia publicznego.
9. Załączniki do protokołu postępowania udostępnia się po dokonaniu wyboru najkorzystniejszej oferty albo unieważnieniu postępowania, z tym że oferty wraz z załącznikami, udostępnia się niezwłocznie po otwarciu ofert, nie później jednak niż w terminie 3 dni od dnia ich otwarcia.
10. Wymagania w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art.95 ustawy – nie dotyczy.
11. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 ustawy PZP.

12. Zamawiający nie przewiduje wymagań w zakresie zatrudniania osób, o których mowa w art. 96 ust.2 pkt.2 ustawy PZP.
13. Przedmiot zamówienia został podzielony na 6 (sześć) części.

XX. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANA WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO,OGÓLNE WARUNKI UMOWY ALBO WZÓR UMOWY.

1. Umowa w sprawie realizacji zamówienia publicznego zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszej specyfikacji istotnych warunków zamówienia oraz zawartych w ofercie.
2. Postanowienia umowy – zawiera projekt umowy stanowiący **Załącznik nr 7 do SWZ**.

XXI. PODWYKONAWSTWO

1. Wykonawca może powierzyć wykonanie zamówienia podwykonawcom.
2. Powierzenie realizacji części zamówienia podwykonawcom nie zwalnia wykonawcy z odpowiedzialności za prawidłową realizację zamówienia.
3. Wykonawca wskaże w Formularzu oferty części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i poda nazwy ewentualnych podwykonawców, jeżeli są już znani.

XXII. PRZETWARZANIE DANYCH OSOBOWYCH.

Klauzula informacyjna dla uczestników postępowań w ramach prawa zamówień publicznych

Zgodnie z art. 13 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest **Samodzielny Publiczny Zakład Opieki Zdrowotnej Sanatorium Uzdrowiskowe MSWiA "AGAT",** z siedzibą w 58-560 Jelenia Góra ul. Cervi 14 adres e-mail: **sekretariat@sanatorium-agat.pl** , tel. **+48 75 75 520 64** .
2. Może Pan/Pani kontaktować się w sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących na mocy RODO z Administratorem z wykorzystaniem powyższych danych teleadresowych lub z wyznaczonym u Administratora Inspektorem ochrony danych na adres e-mail: iod@sanatorium-agat.pl
3. Pani/Pana dane niezbędne do udziału w postępowaniu będą przetwarzane w celu związanym z realizacją postępowania o udzielenie zamówienia publicznego na podstawie ustawy Prawo zamówień publicznych oraz działanie przez administratora w interesie publicznym [PZP], zgodnie z art. 6 ust. 1 lit. c, e oraz art. 10 RODO[1].
4. Pani/Pana dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymywania na podstawie przepisów prawa lub umowy, w tym: podwykonawcom, firmom zapewniającym niszczenie dokumentów i nośników danych, biurom obsługi prawnej, itp.
5. Ze względu na jawność postępowania o udzielenie zamówienia publicznego, odbiorcami Pani/Pana danych osobowych mogą być wszystkie zainteresowane osoby lub podmioty. Ograniczenie dostępu do danych może wystąpić jedynie w szczególnych przypadkach, jeśli jest to uzasadnione ochroną prywatności, interesem publicznym lub informacja stanowi tajemnicę przedsiębiorstwa.
6. W związku z jawnością postępowania o udzielenie zamówienia publicznego Pani/a dane mogą być także przekazywane do państw trzecich.
7. Podanie przez Panią/Pana danych osobowych jest wymagane przepisami PZP do wzięcia udziału w postępowaniu.

[1] *Wskazano art. 10 RODO, ponieważ od niektórych osób jest wymagane oświadczenie o niekaralności, interes publiczny odnosi się do ewentualnego dochodzenia roszczeń*

8. Posiada Pani/Pan prawo do wniesienia skargi do Prezesa UODO (www.uodo.gov.pl) w razie uznania, że przetwarzanie danych przez Administratora narusza przepisy prawa.
9. Pani/Pana dane osobowe w przypadku postępowań o udzielenie zamówienia publicznego będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt , który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164) został przygotowany w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych. Dla dokumentów wytworzonych w ramach zamówień publicznych krajowych jest to okres 5 lat, dla zamówień publicznych unijnych jest to okres 10 lat. Natomiast umowy cywilno-prawne wraz z dokumentacją dotyczącą ich realizacji, niezależnie od trybu w jakim zostały zawarte, przechowywane są przez okres 10 lat. Okres przechowywania liczony jest od 1 stycznia roku następnego od daty zakończenia sprawy. Po upływie okresu przechowywania dokumentacja niearchiwalna podlega, po uzyskaniu zgody dyrektora właściwego archiwum państwowego, brakowaniu;

Posiada Pan/Pani: na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

- na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą PZP oraz nie może naruszać integralności protokołu postępowania oraz jego załączników;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO

XXIII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJACEGO WYKONAWCY.

1. Środki ochrony prawnej określone w niniejszym dziale przysługują Wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Postępowanie odwoławcze jest prowadzone w języku polskim.
4. Wszystkie dokumenty przedstawia się w języku polskim, a jeżeli zostały sporządzone w języku obcym, strona oraz uczestnik postępowania odwoławczego, który się na nie powołuje, przedstawia ich tłumaczenie na język polski. W uzasadnionych przypadkach Izba może żądać przedstawienia tłumaczenia dokumentu na język polski poświadczonego przez tłumacza przysięgłego.
5. Odwołanie przysługuje na:

1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania wykonawców lub konkursie, w tym na projektowane postanowienie umowy;
2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania wykonawców lub konkursie, do której zamawiający był obowiązany na podstawie ustawy;
3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.

6. Odwołanie wnosi się do Prezesa Izby.
7. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
8. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
9. Odwołanie zawiera:

1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);
2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;
3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;
4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku - numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;
5) określenie przedmiotu zamówienia;
6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;
7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy;
8) zwięzłe przedstawienie zarzutów;
9) żądanie co do sposobu rozstrzygnięcia odwołania;
10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;
11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
12) wykaz załączników.

10. Do odwołania dołącza się:

1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
2) dowód przesłania kopii odwołania zamawiającemu;
3) dokument potwierdzający umocowanie do reprezentowania odwołującego.

11. Odwołanie podlega rozpoznaniu, jeżeli:

1) nie zawiera braków formalnych;
2) uiszczono wpis w wymaganej wysokości.

12. Wpis uiszcza się najpóźniej do dnia upływu terminu do wniesienia odwołania.
13. Odwołanie wnosi się w przypadku zamówień, których wartość jest mniejsza niż progi unijne, w terminie:

1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.

14. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.
15. Odwołanie w przypadkach innych niż określone powyżej wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach

stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.

16. Zamawiający przesyła niezwłocznie, nie później niż w terminie 2 dni od dnia otrzymania, kopię odwołania innym wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli odwołanie dotyczy treści ogłoszenia o zamówieniu lub dokumentów zamówienia, zamieszcza ją również na stronie internetowej, na której jest zamieszczone ogłoszenie o zamówieniu lub są udostępniane dokumenty zamówienia, wzywając wykonawców do przystąpienia do postępowania odwoławczego.
17. Wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje, i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje.
18. Zgłoszenie przystąpienia doręcza się Prezesowi Izby, a jego kopię przesyła się zamawiającemu oraz wykonawcy wnoszącemu odwołanie. Do zgłoszenia przystąpienia dołącza się dowód przesłania kopii zgłoszenia przystąpienia zamawiającemu oraz wykonawcy wnoszącemu odwołanie.
19. Wykonawcy, którzy przystąpili do postępowania odwoławczego, stają się uczestnikami postępowania odwoławczego, jeżeli mają interes w tym, aby odwołanie zostało rozstrzygnięte na korzyść jednej ze stron.
20. Czynności uczestnika postępowania odwoławczego nie mogą pozostawać w sprzeczności z czynnościami i oświadczeniami strony, do której przystąpił, z wyjątkiem przypadku zgłoszenia sprzeciwu, o którym mowa w art. 523 ust. 1, przez uczestnika, który przystąpił do postępowania po stronie zamawiającego.

XXIV. ZAŁĄCZNIKI DO SWZ.

Załączniki wypełnione przez Wykonawcę, składane z ofertą:

1. **Załącznik nr 1** - FORMULARZ OFERTOWY.
2. **Załącznik nr 2** - OŚWIADCZENIE WYKONAWCY O BRAKU PODSTAW DO WYKLUCZENIA.
3. **Załącznik nr 3** – OŚWIADCZENIE O AKTUALNOŚCI INFORMACJI PODANYCH W OŚWIADCZENIU z art. 125 ust. 1 PZP
4. **Załącznik nr 4 do SWZ.** Oświadczenie o udostępnieniu zasobów (podpisuje podmiot udostępniający zasoby). Dokument należy dołączyć do oferty - jeżeli ma zastosowanie.
5. **Załącznik nr 5 -** Oświadczenie Wykonawców składający ofertę wspólnie (gdy ma zastosowanie).

Załączniki wypełnione przez wykonawcę – składane na wezwanie.

1. **Załącznik nr 6_wez** - Wykaz dostaw – wzór (dołączyć referencje).
2. Oświadczenie o spełnieniu norm środowiskowych - dotyczy części 1 przedmiotu zamówienia.
3. Oświadczenie potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta - dotyczy części 1 przedmiotu zamówienia.
4. Oświadczenie potwierdzające spełnienie wymagań Karty Zarządzania - dotyczy części 1 przedmiotu zamówienia.
5. Oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta - dotyczy części 1 przedmiotu zamówienia.

Wymagania związane z realizacją zamówienia.

1. **Załącznik nr 7** – Projekt Umowy