Nazwa i adres zamawiającego: Samodzielny Publiczny Zakład Opieki Zdrowotnej Wojewódzka Stacja Pogotowia Ratunkowego w Białymstoku 15 - 874 Białystok, ul. Poleska 89 NIP: 542-25-03-045, KRS: 0000179636, BDO: 000159464	Białystok 01.04.2026 r. ……..……., dn. …….. (miejscowość) data – dzień/m-c/rok
Znak sprawy	**EOP.334.6.26**

ZAPYTANIE OFERTOWE
NA DOSTAWĘ

SP ZOZ WSPR w Białymstoku, ul. Poleska 89, 15 - 874 Białystok zwraca się do Państwa z prośbą o przedstawienie swojej oferty poprzez wypełnienie formularza załączonego do niniejszego zapytania ofertowego zgodnie z poniższymi wymaganiami:

1. Przedmiot zamówienia:

1.a) Szczegółowy opis - specyfikacja cech towaru
(należy podać co najmniej: parametry zamawianego towaru, surowce, materiały, sposób wykonania, określić standard towaru)

Przedmiotem postępowania jest dostawa sprzętu informatycznego i urządzeń peryferyjnych o parametrach nie gorszych niż:

Część 1: : Drukarka a4 – 5 sztuk

Parametr	**Minimalna wymagana wartość parametru**
Rodzaj urządzenia	Jednofunkcyjne - tylko funkcja druku
Technologia druku	Monochromatyczna Laserowa/LED
Format	A4
Rozdzielczość druku mono	Min. 600x600 dpi
Szybkość drukowania mono	20 stron A4/min
Automatyczny druk dwustronny	tak
Czas do wydruku pierwszej strony	Do 8 sekund
Standardowa pojemność podajników	Min. 350 arkuszy
Standardowe rozwiązania komunikacyjne	USB (2.0 Hi-Speed)/ LAN
Gwarancja	Minimalnie 24 m-ce producenta
Eksploatacja	Dostępne na rynku zamienniki materiałów eksploatacyjnych

Część 2: Firewall Next Generation – 1 sztuka

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+ 10 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 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 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 4 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 2 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps. 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

1. 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 12 miesięcy. Gwarancja oraz wsparcie System jest objęty serwisem gwarancyjnym producenta przez okres 12 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. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. Zamawiający dopuszcza składnie ofert częściowych. Wszystkie ewentualnie użyte nazwy własne w niniejszym zapytaniu ofertowym mają charakter poglądowy i zamawiający dopuszcza zastosowanie rozwiązań zamiennych (równoważnych) o nie gorszych parametrach. Zamawiający dopuszcza możliwość składania ofert równoważnych. Jeżeli w opisie przedmiotu zamówienia użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty, pochodzenie, źródło lub szczegółowy proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę, normy, aprobaty, specyfikacje techniczne i systemy odniesienia, Zamawiający dopuszcza zastosowanie produktów i rozwiązań równoważnych do opisanych w opisie przedmiotu zamówienia, tj. o właściwościach funkcjonalnych i jakościowych takich samych lub zbliżonych do tych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. W celu udowodnienia Zamawiającemu równoważności zaproponowanego rozwiązania wykonawca zobowiązany jest, załączyć do oferty dokumenty z których jednoznacznie będzie wynikał fakt równoważności rozwiązania.
	Kody wg Wspólnego Słownika Zamówień (CPV)
	30232100 - 5 Drukarki i plotery 32420000 - 3 Urządzenia sieciowe
1.b)	**Warunki realizacji dostawy** (należy podać w zależności od rodzaju zamówienia: warunki płatności, sposób rozliczenia, miejsce dostawy, sposób realizacji dostawy-jednorazowo, sukcesywnie lub ciągle)
	1. Jednorazowa dostawa do siedziby Zamawiającego (ul. Poleska 89, 15 – 874 Białystok) w terminie 5 dni roboczych od dnia zawarcia umowy. 2. Wynagrodzenie będzie płatne przelewem na rachunek bankowy Wykonawcy wskazany w treści umowy, w terminie 30 dni od daty wystawienia prawidłowej faktury VAT, uwzględniającej obowiązującą stawkę podatku VAT.
1.c)	**Ilość towaru (szt., op. itp)**
	Część 1: Drukarka a4 – 5 szt. Cześć 2: Next Generation Firewall – 1 szt.
1.d)	**Termin realizacji zamówienia**
	Jednorazowa dostawa do siedziby Zamawiającego (ul. Poleska 89, 15 – 874 Białystok) w terminie 5 dni roboczych dni od zawarcia umowy

1.e)	**Do formularza dołączono wzór umowy**	
	TAK	~~**NIE**~~
2.	**Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami** (w szczególności: cena, koszt, jakość, funkcjonalność, parametry techniczne, kwalifikacje zawodowe i doświadczenie osób kierowanych do realizacji zamówienia, termin dostawy, serwis posprzedażowy)	
	KRYTERIUM	**WAGA**
	Cena	**100%**
3.	**Osoba uprawniona do kontaktu ze strony Zamawiającego** (nazwisko i imię - nr telefonu – godz. kontaktu)	
	W kwestiach formalnych: **Katarzyna Zalewska** **tel. 85 66 37 344 godz. kontaktu: 8^{00} - 14^{00}** **W kwestiach merytorycznych:** **Maciej Cylwik** **tel. 85 66 37 369 godz. kontaktu: 8^{00} - 14^{00}**	
	Adres e-mail, fax do kontaktu z Zamawiającym	
	przetargi@wspr.bialystok.pl **85 66 37 302**	
4.	**Termin, do którego należy złożyć oferty** (data i godzina)	
	10.04.2026r., godz. 10:00	

UWAGA;

Prosimy o uzupełnienie i złożenie we wskazanym wyżej terminie załączonego FORMULARZA OFERTOWEGO

Formularz ofertowy można składać:

1. *Osobiście w siedzibie Zamawiającego: pokój nr 214 piętro 2*
2. *przesłać pocztą na adres: SP ZOZ WSPR w Białymstoku, 15-874 Białystok, ul. Poleska 89 (pok. Nr 214)*
3. *faksem na nr 85 66 37 302*
4. *pocztą elektroniczną na adres e-mail: przetargi@wspr.bialystok.pl*

…….	……..…	……..……
Podpis kierownika komórki wnioskującej	Akceptacja komórki ds. zamówień publicznych	Podpis DYREKTORA

Załącznik nr 1 do zapytania ofertowego – Formularz ofertowy

Nazwa i adres Wykonawcy: …… …… …… e-mail do kontaktu: ……	……..……., dn.…….. (miejscowość) data – dzień/m-c/rok
Znak sprawy	**EOP.334.6.26**

FORMULARZ OFERTOWY

Oferujemy następujące warunki dostawy:

Część 1:

Nazwa artykułu	Jm.	Ilość	Producent, symbol i model oferowanego sprzętu	Cena jednostkowa netto	Stawka podatku VAT %	Cena jednostkowa brutto	Wartość brutto (kol. 3 x 7)
1	2	3	4	5	6	7	8
Drukarka a4	szt.	5					

Oferowana gwarancja wynosi:……
(Gwarancja minimum 24 m-ce producenta)

Część 2:

Nazwa artykułu	Jm.	Ilość	Producent, symbol i model oferowanego sprzętu	Cena jednostkowa netto	Stawka podatku VAT %	Cena jednostkowa brutto	Wartość brutto (kol. 3 x 7)
1	2	3	4	5	6	7	8
Firewall Next Generation	szt.	1					

Oferowana gwarancja wynosi:……
(Gwarancja minimum 12 m-cy producenta)

Ponadto oświadczamy, że:

1. *Posiadam wymagane uprawnienia do wykonania niniejszego zamówienia (jeżeli dotyczy).*
2. *W cenie naszej oferty zostały uwzględnione wszystkie koszty związane z prawidłową realizacją zamówienia, a w szczególności koszty transportu, rozładunku itp.*
3. ***Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego[1] (Dz. U. poz. 835)***
   - ☐ ***POTWIERDZAM, nie zachodzą przesłanki wykluczenia;***
   - ☐ ***NIE POTWIERDZAM, zachodzą w stosunku do nas następujące przesłanki wykluczenia:***

   ……
   ……
   (zaznaczyć właściwą odpowiedź)
4. *Akceptujemy termin i warunki realizacji dostawy.*
5. *Akceptujemy warunki płatności zawarte w Zapytaniu ofertowym.*
6. *Nie wnosimy zastrzeżeń do wzoru umowy dołączonego do zapytania ofertowego.*
7. *Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres 30 dni od terminu składania ofert.*
8. *Posiadam uprawnienia wiedze i doświadczenie do wykonania przedmiotu zamówienia*
9. *Wykonawca oświadcza, że **jest/nie jest** czynnym podatnikiem podatku VAT (*niepotrzebne skreślić)*
10. *Jesteśmy świadomi, ze postępowanie może być unieważnione w każdym momencie bez podania przyczyny.*

[1] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą", z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.
Zamawiający odrzuci ofertę złożoną przez wykonawcę, który podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

11. Klauzula informacyjna:

1) Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO) informuję, że:

1. Administratorem Pani/Pana danych osobowych jest: SP ZOZ WSPR w Białymstoku, ul. Poleska 89, 15-874 Białystok;

2) Administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: iod@wspr.bialystok.pl tel. 85 663 73 01;

3) Państwa dane osobowe będą przetwarzane w celu związanym z wszczęciem postępowania w procedurze zapytania ofertowego o wartości mniejszej niż 170.000,00 zł netto wyłączonych z obowiązku stosowania ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 ze zm.) - na podstawie art. 6 ust. 1 lit. b i c RODO oraz w celu rozpatrzenia złożonej przez Państwa oferty i ewentualnego zawarcia umowy.

4) W szczególnych sytuacjach możemy przekazać/powierzyć Państwa dane osobowe innym podmiotom. Podstawą przekazania/powierzenia danych są przepisy prawa lub właściwie skonstruowane, zapewniające bezpieczeństwo danym osobowym oraz umowy powierzenia przetwarzania.

5) Jednocześnie odbiorcami Państwa danych osobowych mogą być osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o ustawę o dostępie do informacji publicznej z dnia 26 września 2001 r.;

6) Państwa dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych w postępowaniu o udzielenie zamówienia, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa w zakresie archiwizacji dokumentów.

7) Podanie przez Panią/Pana danych osobowych jest obowiązkowe. W przypadku niepodania danych nie będzie możliwy udział w postępowaniu o udzielenia zamówienia poniżej 170 000,00 zł. Podanie danych osobowych jest warunkiem ważności oferty i ewentualnego zawarcia umowy.

8) Posiadają Państwo:

a) na podstawie art. 15 RODO prawo żądania dostępu do danych osobowych Państwa dotyczących;

b) na podstawie art. 16 RODO prawo do sprostowania Państwa danych osobowych;

c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;

d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają Państwo, że przetwarzanie danych osobowych Państwa dotyczących narusza przepisy RODO;

9) Nie przysługuje Państwu:

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

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

c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Państwa danych osobowych jest art. 6 ust. 1 lit. c RODO;

10) Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

11) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji.

12) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania tzn. żadne decyzje wywołujące wobec osoby skutki prawne lub w podobny sposób na nią istotnie wpływające nie będą oparte wyłącznie na automatycznym przetwarzaniu danych osobowych i nie wiążą się z taką automatycznie podejmowaną decyzją

.....

/podpis Wykonawcy/

<u>Oświadczenie Oferenta w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO</u>

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu przedłożenia oferty w niniejszym postępowaniu.

……..

(data i podpis)

Załącznik nr 2 do zapytania ofertowego – projekt umowy

Umowa nr EOP.334.6.26 cz. 1, 2* - projekt

zawarta w dniu …….. r. w Białymstoku
pomiędzy:
Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Wojewódzką Stacją Pogotowia Ratunkowego w Białymstoku, ul. Poleska 89, 15 - 874 Białystok,
NIP: 542-25-03-045, KRS: 0000179636, BDO: 000159464
reprezentowanym przez:
……..
zwaną dalej **„Zamawiającym"**
a
……
……
reprezentowanym przez:
……
zwanym dalej „**Wykonawcą**"

§ 1

1. W wyniku przeprowadzonego postępowania w trybie zapytania ofertowego Wykonawca sprzedaje, a Zamawiający kupuje:
   w części 1: Drukarka A4;*
   w części 2: Firewall Next Generation;*
   zwane w dalszej części „towarem" na potrzeby SP ZOZ WSPR w Białymstoku, szczegółowo opisane w Załączniku nr 1 do Zapytania ofertowego - formularz ofertowy w części 1, 2*.
2. Wykonawca oświadcza, że dostarczony przez niego przedmiot umowy jest fabrycznie nowy i wolny od wad oraz posiada parametry techniczne i użytkowe zgodne z wymogami Zamawiającego określonymi w zapytaniu ofertowym.
3. Na zakupiony towar zostanie udzielona:
   w części 1 – gwarancja producenta …. miesięce/y;*
   w części 2 – gwarancja producenta …. miesięce/y.*

§ 2

1. Wykonawca zobowiązuje się na swój koszt i ryzyko dostarczyć towar w terminie 5 dni roboczych od dnia podpisania umowy. Dostawa towaru powinna nastąpić w dzień roboczy tj. od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy do siedziby Zamawiającego przy ul. Poleskiej 89 w Białymstoku (2 piętro) pokój 214 w godzinach od 7^{30} do 15^{05}.
2. Do dostarczonego przedmiotu umowy Wykonawca w dniu dostawy dodatkowo dołączy:
   a) dokumenty potwierdzające gwarancje na zakupiony towar zgodnie z kartami gwarancyjnymi (jeżeli takie karty występują). Dokumenty mogą być przekazane w formie papierowej, jak i elektronicznej. W formie elektronicznej dostarczone nie później niż w dniu dostawy na adres e-mail: informatyk@wspr.bialystok.pl.
   b) instrukcje (jeżeli dany przedmiot umowy taką instrukcję posiada), opisy techniczne, które będą w języku polskim.
3. W przypadku zwłoki w dostawie Zamawiający obciąży Wykonawcę karą umowną w wysokości określonej w §5 ust 1 pkt c).
4. Wszelkie inne koszty związane z dostarczeniem towaru do siedziby Zamawiającego, w szczególności koszty opakowania czy ubezpieczenia ponosi Wykonawca.
5. Po dostarczeniu towaru, Zamawiający dokona odbioru w ciągu maksymalnie 2 dni roboczych od dnia dostawy, w celu potwierdzenia zgodności przedmiotu umowy ze specyfikacją techniczną.

6. Potwierdzeniem wykonania umowy, którą uznaje się za zrealizowaną jest dzień podpisania protokołu odbioru, o którym mowa w § 2 ust. 5 z klauzulą „bez zastrzeżeń".

§ 3

1. Za przedmiot umowy Zamawiający zapłaci Wykonawcy przelewem na numer wskazany w §3 ust. 3 kwotę w wysokości:
   W części 1: ……zł brutto, (słownie:…….);*
   W części 2: ……zł brutto, (słownie:…….);*
2. Podstawą do wystawienia faktury VAT będzie podpisany przez Zamawiającego i Wykonawcę protokół odbioru, o którym mowa w §2 ust. 5-6 z klauzulą „bez zastrzeżeń".
3. Wynagrodzenie będzie płatne przelewem na rachunek bankowy Wykonawcy wskazany w treści niniejszej umowy, tj. ……, w terminie 30 dni od daty wystawienia prawidłowej faktury VAT, uwzględniającej obowiązującą stawkę podatku VAT.
4. Wykonawca oświadcza, iż wyżej wskazany rachunek bankowy jest zgłoszony we właściwym dla niego organie podatkowym w ramach zgłoszenia identyfikacyjnego lub zgłoszenia aktualizacyjnego, w szczególności w ramach uwidocznionych w „białej księdze podatników".
5. W przypadku zmiany wskazanego w umowie rachunku bankowego Wykonawca jest obowiązany poinformować Zamawiającego o powyższym, w terminie 7 dni od dnia dokonania zmiany na piśmie. Zmiana umowy w tym przedmiocie wymaga aneksu do umowy.
6. Strony umowy zastrzegają, iż w przypadku zmiany rachunku bankowego przez Wykonawcę, do czasu uwidocznienia nowego rachunku bankowego w „białej księdze podatników", termin płatności określony w §3 ust. 3 umowy ulega przesunięciu do dnia uwidocznienia nowego rachunku bankowego w „białej księdze podatników", bez możliwości naliczania kar umownych, odsetek za opóźnienie, czy też kierowania innych roszczeń odszkodowawczych w stosunku do Zamawiającego.
7. Zobowiązuje się Wykonawcę do przesłania faktur w formacie .pdf na adres faktury@wspr.bialystok.pl lub dostarczenia faktury w formie papierowej do dnia w którym Wykonawca zostanie zobowiązany do wystawiania i udostępnienia Zamawiającemu faktur ustrukturyzowanych przy użyciu Krajowego Systemu e-Faktur (dalej: KSeF) na podstawie przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.
8. W przypadku zmiany stawki podatku VAT w toku realizacji niniejszej umowy cena ofertowa brutto nie ulegnie wzrostowi.
9. Datą zapłaty będzie dzień obciążenia rachunku bankowego Zamawiającego.
10. W przypadku wystawienia przez Wykonawcę faktury VAT niezgodnej z umową lub obowiązującymi przepisami prawa, Zamawiający ma prawo do wstrzymania płatności do czasu wyjaśnienia oraz otrzymania faktury korygującej VAT bez obowiązku płacenia odsetek z tytułu niedotrzymania terminu zapłaty.
11. Wykonawca oświadcza, że **jest/nie jest*** czynnym podatnikiem podatku VAT. W przypadku zmiany statusu VAT Wykonawca zobowiązany jest niezwłocznie, powiadomić o tym Zamawiającego.

§ 4

1. Poniższe postanowienia będą miały zastosowanie od dnia, w którym Wykonawca zostanie zobowiązany do wystawiania i udostępnienia Zamawiającemu faktur ustrukturyzowanych przy użyciu Krajowego Systemu e-Faktur (dalej: KSeF) na podstawie przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (dalej: ustawa o VAT) i od tego dnia będą miały pierwszeństwo w przypadku rozbieżności z innymi postanowieniami niniejszej umowy.
2. Wykonawca wystawi i udostępni Zamawiającemu fakturę z wykorzystaniem KSeF, chyba że zaistnieją przypadki, o których mowa w ustawie o VAT uniemożliwiające takie działanie lub uprawniające Wykonawcę do innego działania – w takim przypadku faktura zostanie wystawiona i udostępniona Nabywcy z uwzględnieniem zasad określonych w ustawie o VAT i niżej wskazanych ustępów.
3. Zapłata należnego Wykonawcy wynagrodzenia nastąpi w oparciu o wystawioną na zasadach określonych w ust. 2 powyżej fakturę na numer rachunku bankowego wskazany w umowie w terminie, o którym mowa w § 3 ust. 3 umowy.

4. Za datę wystawienia faktury ustrukturyzowanej uznaje się datę przesłania faktury przez Wykonawcę do KSeF, a w przypadku faktury, o której mowa w art. 106 nda ust. 1 lub ust. 16 ustawy o VAT lub faktur wystawianych w okresie awarii lub niedostępności KSeF – datę wystawienia wskazaną przez Wykonawcę na tej fakturze.
5. Za dzień skutecznego doręczenia faktury uznaje się dzień jej otrzymania w rozumieniu przepisów ustawy o VAT; w przypadku faktury ustrukturyzowanej będzie to zatem dzień przydzielenia jej indywidualnego numeru identyfikującego tę fakturę w KSeF.
6. Jeżeli ustawa o VAT dopuszcza możliwość udostępnienia Zamawiającemu faktury w sposób inny niż przy użyciu KSeF, taka faktura może zostać doręczona Zamawiającemu na jeden z następujących adresów:
   a) ul. Poleska 89, 15-874 Białystok - za datę skutecznego doręczenia faktury w takim przypadku będzie uznawana data doręczenia Zamawiającemu przesyłki listowej zawierającej ww. fakturę, oznaczoną odpowiednimi kodami zgodnie z ustawą o VAT (z zastrzeżeniem, że w przypadku braku odbioru takiej przesyłki faktura będzie uznana za skutecznie doręczoną po upływie 14 dni od pozostawienia pierwszego zawiadomienia o próbie doręczenia takiej przesyłki) lub data nadania fakturze numeru identyfikującego KSeF – w zależności od tego, która z wymienionych sytuacji nastąpi pierwsza)
   b) e-mail: faktury@wspr.bialystok.pl (za datę skutecznego doręczenia faktury w takim przypadku będzie uznawana data wysłania przez Wykonawcę do Zamawiającego wiadomości e-mail zawierającej ww. fakturę, np. w formacie pdf, oznaczoną odpowiednimi kodami zgodnie z ustawą o VAT lub data nadania fakturze numeru identyfikującego w KSeF – w zależności od tego, która z wymienionych sytuacji nastąpi pierwsza).
7. Faktura będzie uznana za prawidłowo wystawioną, jeżeli zostanie wystawiona z uwzględnieniem zasad wystawiania faktur określonych w ustawie o VAT.
8. Zasady o których mowa w ust. 5 i 6 powyżej stosuje się odpowiednio do załączników ustrukturyzowanych.

§ 5

1. Strony ustalają następujące kary umowne:
   a) w wysokości 10% wartości umowy brutto dla danej części, w przypadku odstąpienia Wykonawcy od umowy z przyczyn niezależnych od Zamawiającego,
   b) w wysokości 10% wartości umowy brutto dla danej części, w przypadku odstąpienia Zamawiającego od umowy z przyczyn, za które odpowiedzialność ponosi Wykonawca,
   c) w wysokości 0,2% wartości umowy brutto dla danej części w przypadku zwłoki w dostawie towaru za każdy rozpoczęty dzień zwłoki,
   d) 0,5% wartości umowy brutto dla danej części w przypadku zwłoki w dostawie towarów reklamowanych za każdy dzień zwłoki.
2. Wykonawca wyraża zgodę na potrącanie kar umownych i innych należności względem Zamawiającego z należnego wynagrodzenia.
3. Jeżeli wysokość naliczonych przez Wykonawcę kar umownych nie pokryje szkody poniesionej przez Zamawiającego, Zamawiającemu przysługuje prawo dochodzenia odszkodowania uzupełniającego na zasadach ogólnych.
4. Kary, o których mowa w § 5 ustęp 1 nie wykluczają się wzajemnie.
5. W przypadku zwłoki w dostawie towaru, Zamawiającemu przysługuje uprawnienie do dokonania zakupu towaru na koszt i ryzyko Wykonawcy u innego dostawcy.

§6

1. W razie awarii zakupionego towaru przez Zamawiającego w okresie gwarancji:
   a) Wykonawca zobowiązuje się do naprawy/wymiany sprzętu w terminie 14 dni roboczych od dnia zgłoszenia;
   b) W przypadku gdy przewidywany czas naprawy sprzętu będzie dłuższy niż tydzień, Wykonawca dostarczy na własny koszt sprzęt zastępczy (o co najmniej tych samych parametrach i funkcjach użytkowych);
   c) W przypadku dokonania naprawy poprzez wymianę elementów w sprzęcie muszą zostać zainstalowane fabrycznie nowe, identyczne elementy, lub za zgodą Zamawiającego, fabrycznie nowe elementy o parametrach równoważnych lub lepszych tego samego producenta;

d) W przypadku naprawy lub wymiany sprzętu, jego części (podzespołu) gwarancja na ten sprzęt, część (podzespół) biegnie od dnia wymiany;
e) Czas naprawy wyłączony jest z okresu gwarancyjnego. Czas trwania gwarancji będzie automatycznie wydłużony o czas trwania naprawy;
f) Wszelkie koszty naprawy, w tym koszty transportu, ponosi Wykonawca;
g) W przypadku niewykonania naprawy w terminie 6 tygodni od daty zgłoszenia wady/awarii/usterki sprzętu Wykonawca zobowiązany jest do wymiany sprzętu na nowy, wolny od wad, o co najmniej takich samych parametrach i funkcjach użytkowych w terminie 3 dni od wystąpienia okoliczności powodujących wymianę;
h) W przypadku ponownego wystąpienia wady/awarii/usterki sprzętu po wykonaniu 3 napraw Wykonawca zobowiązany jest do wymiany sprzętu na nowy, wolny od wad, o co najmniej takich samych parametrach i funkcjach użytkowych w terminie 3 dni od dnia zgłoszenia. Na sprzęt ten okres gwarancji biegnie na nowo od chwili dostarczenia go, zainstalowania, uruchomienia oraz stwierdzenia poprawności działania i braku uszkodzeń mechanicznych;
i) W przypadku wystąpienia rozbieżności pomiędzy zapisami §6 umowy a treścią dokumentu gwarancyjnego dołączonego do towaru, stosuje się zapisy umowy.

§7

1. Zamawiający zastrzega sobie prawo odstąpienia od całości lub części niezrealizowanej umowy, w przypadku nienależytego wykonania umowy ze skutkiem natychmiastowym w terminie 30 dni od powzięcia wiadomości o tych okolicznościach, m.in. w następujących przypadkach:
   a) niedostarczenia sprzętu w terminie wskazanym w § 2 ust. 1,
   b) ujawnienia sprzętu niebędącego fabrycznie nowym,
   c) ujawnienia w dostarczonym sprzęcie wad fizycznych lub prawnych,
   d) innego rodzaju nienależytego wykonania lub nie wykonania umowy, czyniącego dalsze jej realizowanie bezprzedmiotowym.
2. Zamawiający może odstąpić od umowy w przypadku zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
3. W przypadku, o którym mowa w ust. 1, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

§8

Osoby odpowiedzialne za realizację zamówienia:

a) z ramienia Zamawiającego: …… tel.: …….
b) z ramienia Wykonawcy: …… tel.: …….

§9

Wykonawca zobowiązuje się nie dokonywać cesji wierzytelności.

§10

1. W sprawach nieuregulowanych umową mają zastosowanie przepisy Kodeksu cywilnego.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej zastrzeżonej pod rygorem nieważności.
3. Ewentualne spory mogące wyniknąć z realizacji niniejszej umowy strony załatwiają polubownie, a w przypadku nie rozwiązania problemu poddają pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Integralną część niniejszej umowy stanowią:
   a) Załącznik nr 1 - Formularz ofertowy,
   b) Załącznik nr 2 - Klauzula informacyjna,
   c) Załącznik nr 3 - Zapytanie ofertowe str. 1 do 8.

WYKONAWCA **ZAMAWIAJĄCY**

* niepotrzebne usunąć/skreślić

Załącznik nr 3 do zapytania ofertowego – klauzula RODO

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1) Administratorem danych jest SP ZOZ WSPR w Białymstoku, ul. Poleska 89, 15-874 Białystok; email: sekretariat@wspr.bialystok.pl, tel. 85 663 73 01;

2) Kontakt do Inspektora Danych Osobowych - e-mail – iod@wspr.bialystok.pl;

3) Dane są zbierane w celach wynikających z prawnie uzasadnionych interesów realizowanych przez SP ZOZ WSPR w Białymstoku, co oznacza w szczególności:

a) zawarcie i wykonanie niniejszej Umowy,

b) obsługę, dochodzenie i obronę w razie zaistnienia wzajemnych roszczeń.

4) Dane mogą być przekazywane podmiotom współpracującym z SP ZOZ WSPR w Białymstoku na podstawie zawartych umów, zgodnie z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych tj. w szczególności podmiotom świadczącym usługi informatyczne.;

5) Dane będą przechowywane przez okres obowiązywania Umowy, a także do czasu wygaśnięcia wzajemnych roszczeń wynikających z tej Umowy;

6) Przysługuje Panu/Pani prawo do dostępu do własnych danych, ich sprostowania, usunięcia, lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu do przetwarzania danych;

7) Wspomniane prawa można zrealizować za pomocą pisemnych wniosków znajdujących się na stronie www.pogotowie.bialystok.pl lub w sekretariacie SP ZOZ WSPR, ul. Poleska 89, 15-874 Białystok;

8) Przysługuje Panu/Pani prawo do wniesienia skargi do organu nadzorczego;

9) Podanie danych zawartych w umowie jest niezbędne w związku z jej realizacją;

10) Dane wprowadzone do systemu informatycznego nie będą przetwarzane w sposób zautomatyzowany oraz nie będą poddawane profilowaniu;

11) Administrator danych dokłada wszelkich starań, aby zapewnić wszelkie środki fizycznej, technicznej i organizacyjnej ochrony danych osobowych przed ich przypadkowym czy umyślnym zniszczeniem, przypadkową utratą, zmianą, nieuprawnionym ujawnieniem, wykorzystaniem czy dostępem, zgodnie ze wszystkimi obowiązującymi przepisami;

12) Oświadczam, iż zapoznałem się z w/w informacją, podpisując niniejszą umowę akceptuję jej treść.