

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

**Przedmiotem zamówienia jest dostawa i instalacja infrastruktury informatycznej w ramach projektu Wzmocnienie cyberbezpieczeństwa Gminy Kielce.**

**Projekt Wzmocnienie cyberbezpieczeństwa Gminy Kielce jest realizowany w ramach FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC)**

**Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2.**

**– Wzmocnienie krajowego systemu cyberbezpieczeństwa.**

W ramach projektu Zamawiający planuje modernizację i rozbudowę posiadanej aktualnie platformy sprzętowej Centrum Przetwarzania Danych, która obejmuje sieć szkieletową, dystrybucyjną, dostępową oraz punkty styku z siecią Internet.

Intencją Zamawiającego jest zakupienie rozwiązania kompatybilnego z już posiadanymi urządzeniami firewall do zabezpieczenia sieci oraz przełącznikami i routerami tworzącymi sieć MAN produkcji firmy Juniper Networks. Jednym z kluczowych argumentów jest chęć zachowania homogeniczności sieci. Aktualna infrastruktura, w której wszystkie urządzenia pochodzą od jednego producenta, umożliwi spójne zarządzanie, łatwiejsze diagnozowanie problemów oraz uproszczone utrzymanie sieci. Korzystanie z systemu zarządzania Junos Space oraz rozwiązania Juniper STRM dodatkowo centralizuje i upraszcza zarządzanie całą infrastrukturą.

W celu zapewnienia najnowszych technologii i optymalnego działania sieci, Zamawiający zamierza odświeżyć swoją infrastrukturę sieciową, zachowując jednocześnie homogeniczność sieci.

Zamawiający planuje wymianę obecnie używanych routerów oraz firewalli klastrem zbudowanym z dwóch urządzeń przenosząc ich funkcje na nowe urządzenia typu firewall. Nowe urządzenia muszą posiadać wszystkie funkcje zastępowanych urządzeń oraz nowe funkcjonalności i niezbędną wydajność. Nowe urządzenia muszą w szczególności być kompatybilne (współpracować) z posiadanymi urządzeniami do zarządzania i monitoringu całej sieci MAN to jest Junos Space oraz rozwiązania Juniper STRM, pozwalającymi na centralne zarządzanie wszystkimi urządzeniami sieci.

Dodatkowo zamawiający posiada środowisko Data Center zbudowane z dwóch systemów Blade HP BLC7000 oraz kilkanaście serwerów kasetowych HP BL460c połączonych z macierzą dyskową Hitachi HUS 150 o pojemności dysków brutto 175 TB.

Macierz dyskowa jest połączona ze środowiskiem serwerowym za pomocą przełączników HP B-series 8/12c SAN Switch BladeSystem c-Class.

Celem Zamawiającego jest zakup nowych urządzeń – serwerów i macierzy dyskowej, które pozwolą na rozbudowę posiadanego środowiska oraz umożliwią współpracę z posiadaną infrastrukturą serwerową i zapewnią dostęp do danych gromadzonych zarówno w nowej jak i w posiadanej obecnie macierzy dyskowej.

### **W skład przedmiotu zamówienia wchodzi następujące pozycje:**

3 sztuki urządzeń typu Firewall,

2 sztuki serwerów,

1 sztuka macierz dyskowa,

2 sztuki przełączników do sieci SAN.

Minimalne wymagania techniczne dla poszczególnych urządzeń opisano poniżej.

## I. Parametry techniczno-funkcjonalne dla urządzenia typu firewall.

Lp.	Wymagania minimalne
1	Firewall musi być dostarczony jako dedykowane urządzenie sieciowe w postaci chassis o wysokości 1 U, przystosowanego do montażu w szafie rack, wyposażonego w wymienne 2 redundantne źródła zasilania AC.
2	Zarządzanie firewallem musi odbywać przy pomocy tekstowego interfejsu użytkownika (dostępnego przez port konsoli, telnet, ssh) oraz przy pomocy graficznego interfejsu użytkownika. Musi istnieć możliwość zarządzania przez centralny system zarządzający tego samego producenta.
3	System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenie musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwany przez urządzenie.
4	System operacyjny firewalla musi śledzić stan sesji użytkowników ( <i>stateful processing</i> ), tworzyć i zarządzać tablicą stanu sesji
5	Urządzenie musi być wyposażone w nie mniej niż 32 GB pamięci RAM oraz w co najmniej jeden dysk SSD o pojemności co najmniej 110 GB.
6	Firewall musi być dostarczony z nie mniej niż 16 wbudowanymi interfejsami Ethernet 10/100/1000 zakończonymi wtykiem RJ-45, co najmniej 4 interfejsami 10 Gigabit Ethernet umożliwiającymi obsadzenie wkładkami SFP+ oraz co najmniej 2 interfejsami 25 Gigabit Ethernet na moduły SFP28. Porty 25G oraz 10G muszą obsługiwać MACSec AES256. Wszystkie porty muszą być wyposażone we wkładki światłowodowe o nominalnej prędkości.
7	Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Porty służące do synchronizacji muszą być odrębne od wymienionych w poprzednim punkcie jeżeli urządzenie wymaga ich dedykowania do celów synchronizacyjnych.
8	Musi istnieć możliwość synchronizacji urządzeń klastra HA z wykorzystaniem łączy L3 tj. po adresach IP różnych podsieci. Urządzenie musi też zapewniać mechanizmy kierowania ruchu tranzytowego do jednostki aktywnej z wykorzystaniem protokołów routingu.
9	Z punktu widzenia systemu operacyjnego firewalla wszystkie usługi bezpieczeństwa muszą być zdefiniowane w tym samym pliku konfiguracyjnym zdefiniowanym na module kontrolnym.
10	Firewall musi realizować zadania Stateful Firewall z wydajnością nie mniejszą niż 12 Gb/s liczoną dla ruchu IMIX. Firewall musi obsługiwać nie mniej niż 2 miliony równoległych sesji oraz zestawiać nie mniej niż 150 tysięcy nowych połączeń/sekundę.
11	Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać ruch szyfrowany o przepustowości nie mniej niż 8 Gb/s dla ruchu IMIX.
12	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 15000 reguł polityki bezpieczeństwa.



13	Urządzenie musi umożliwiać integrację z systemami QKD (quantum key distribution) w zakresie synchronizacji kluczy szyfrowania IPsec, z wykorzystaniem ETSI GS QKD API.
14	Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi obsługiwać co najmniej 2 miliony prefiksów w RIB oraz co najmniej 1 milion w FIB.
15	Urządzenie musi obsługiwać protokoły sygnalizacji RSVP oraz LDP, w tym funkcję Fast Reroute.
16	Urządzenie musi obsługiwać aplikacje MPLS, co najmniej L2 VPN/L2 Circuit, L3 VPN oraz Multicast VPN (MVPN).
17	Urządzenie musi posiadać funkcję tworzenia wirtualnych ruterów w liczbie co najmniej 490, oraz sieci VLAN z tagowaniem 802.1Q.
18	Urządzenie musi umożliwiać stworzenie co najmniej 500 odrębnych stref bezpieczeństwa (security zones)
19	Urządzenie musi obsługiwać routing pomiędzy tunelami VXLAN sygnalizowanymi przez M-BGP EVPN.
20	Urządzenie musi posiadać możliwość definicji polityk dostępu do stron www na podstawie definiowalnych samodzielnie list domen whitelist/blacklist. W przypadku dostępu https, wpisy mają być porównywane z polem SNI.
21	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz przycinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków IP, TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach
22	Urządzenie musi umożliwiać translację adresów NAT, statyczną i dynamiczną, IPv4 i IPv6, w zakresie adresów źródłowych i docelowych (w tym tzw. Twice-NAT) z mechanizmami Port Block Allocation i Port Address Translation. Wymagana możliwość zdefiniowania 7900 reguł translacji.
23	Urządzenie musi umożliwiać inspekcję sesji SSL przez ich rozszyfrowanie (Forward Proxy), dla wskazanych adresów docelowych, obsługując co najmniej 59 tysięcy sesji TLS1.3 z prędkością ich zestawiania nie mniejszą niż 2400 sesji na sekundę.
24	Urządzenie musi umożliwiać definicję polityk bezpieczeństwa z wykorzystaniem danych uwierzytelnienia użytkownika, w tym integracji z usługami LDAP i RADIUS.
25	Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, <i>intrusion prevention</i> ) realizowaną z wydajnością co najmniej 4 Gbps. Ustalenie listy blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall.
26	Urządzenie musi posiadać możliwość dynamicznego rozpoznawania aplikacji i definiowania polityk bezpieczeństwa, z uwzględnieniem kierowania ruchu przez odpowiednie łącza oraz wskazywania polityk QoS.
27	Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 4 poprzednich, kompletnych konfiguracji.
28	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.
29	Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej.
30	Funkcjonalności subskrypcyjne tj co najmniej IPS, rozpoznawanie aplikacji mają być zapewnione do dnia 31.03.2026 r. włącznie w ramach niniejszej specyfikacji.

31	<p>Co najmniej 2-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii w trybie 24x7. Producent wysyła sprzęt następnego dnia roboczego.</p> <p>Wszystkie naprawy gwarancyjne muszą być wykonane w miejscu instalacji.</p> <p>W przypadku braku możliwości usunięcia awarii sprzętu w miejscu użytkowania Wykonawca zobowiązany jest do dostarczenia i uruchomienia bez dodatkowych opłat sprzętu zastępczego o nie gorszych parametrach technicznych lub cechach funkcjonalnych.</p> <p>Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.</p> <p>Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej na zasadach opisanych w rozdziale V SOPZ do dnia 31.03.2026 r. włącznie.</p>
----	---

## II. Parametry techniczno-funkcjonalne dla serwera.

Element konfiguracji	Wymagania minimalne
Obudowa	<p>Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi).</p> <p>Możliwość wyposażenia serwera w zamykany, zdejmowany panel przedni chroniący przed nieuprawnionym dostępem do dysków.</p> <p>Możliwość wyposażenia serwera w czujniki otwarcia obudowy współpracujące z BIOS/UEFI.</p> <p>Zainstalowany moduł TPM 2.0.</p>
Procesor	<p>Dwa procesory minimum 24-rdzeniowe, x86 - 64 bity o taktowaniu CPU min. 2.0 GHz., osiągające w testach SPECrate2017_int_base powyżej 421 punktów w konfiguracji dwuprocesorowej, wynik testu musi być opublikowany na stronie <a href="http://www.spec.org">www.spec.org</a>.</p> <p>Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeniowych, mocy do min. 350W i taktowaniu CPU do min. 3.6GHz.</p>
Liczba procesorów	Zainstalowane min. 2 procesory
Pamięć operacyjna	<p>Minimum 512 GB RDIMM DDR5 4800 MT/s w modułach o pojemności 32GB każdy.</p> <p>Płyta główna z minimum 32 slotami na pamięć i umożliwiającą instalację do minimum 8TB.</p>
Gniazda rozszerzeń	<p>Minimum 3 aktywne gniazda PCI-Express generacji 5, w tym min. 1 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height).</p> <p>Możliwość rozbudowy do 6 slotów PCI-Express generacji 5.</p>
Dysk twardy	<p>Zatoki dyskowe gotowe do zainstalowania minimum 8 dysków SFF typu Hot Swap, SATA, 2,5" i opcja rozbudowy/rekonfiguracji o dodatkowe minimum 8 dysków typu Hot Swap, SATA, 2,5".</p> <p>Zainstalowane minimum dwa dyski M.2 NVMe 480GB SSD każdy, zestawione w sprzętowy RAID1, umieszczone na dedykowanej karcie PCI-e.</p>
Kontroler	<p>Możliwość wyposażenia serwera w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych NVMe/SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.</p> <p>Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.</p>
Interfejsy sieciowe	<p>Minimum 2 wbudowane porty Ethernet 10 Gb/s SFP+ z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.</p> <p>Zainstalowana jedna karta dwuportowa FC32GB.</p> <p>Karty muszą być wyposażone we wkładki o nominalnej prędkości portów.</p>
Karta graficzna	Zintegrowana karta graficzna
Porty	<p>Min. 4 x USB 3.2 Gen1 (w tym 1 port wewnętrzny)</p> <p>Min. 1x VGA</p> <p>Możliwość rozbudowy o:</p> <ul style="list-style-type: none"> <li>- dodatkowy port typu DisplayPort dostępny z przodu serwera</li> </ul>

	- port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45.
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW.
Zasilacz	Minimum 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1800W.
Karta/moduł zarządzający	<p>Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:</p> <ul style="list-style-type: none"> <li>• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe</li> <li>• wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP</li> <li>• dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera</li> <li>• dostęp do karty możliwy <ul style="list-style-type: none"> <li>- z poziomu przeglądarki webowej (GUI)</li> <li>- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)</li> <li>- z poziomu skryptu (XML/Perl)</li> <li>- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)</li> </ul> </li> <li>• wbudowane narzędzia diagnostyczne</li> <li>• zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego</li> <li>• obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie</li> <li>• wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników</li> <li>• przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)</li> <li>• obsługa zdalnego serwera logowania (remote syslog)</li> <li>• wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i i wirtualnych folderów</li> <li>• mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie</li> <li>• funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności</li> <li>• monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji</li> <li>• konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)</li> <li>• zdalna aktualizacja oprogramowania (firmware)</li> <li>• zarządzanie grupami serwerów, w tym: <ul style="list-style-type: none"> <li>- tworzenie i konfiguracja grup serwerów</li> <li>- sterowanie zasilaniem (wł/wył)</li> <li>- ograniczenie poboru mocy dla grupy (power capping)</li> <li>- aktualizacja oprogramowania (firmware)</li> <li>- wspólne wirtualne media dla grupy</li> </ul> </li> <li>• możliwość równoczesnej obsługi przez 6 administratorów</li> </ul>



	<ul style="list-style-type: none"> <li>• autentykacja dwuskładnikowa (Kerberos)</li> <li>• wsparcie dla Microsoft Active Directory</li> <li>• obsługa SSL i SSH</li> <li>• enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli</li> <li>• wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API</li> <li>• wsparcie dla Integrated Remote Console for Windows clients</li> <li>• możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)</li> </ul>
Gwarancja, wsparcie techniczne	<p>Co najmniej 2-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w miejscu instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Możliwość zgłaszania awarii w trybie 24x7. Serwis realizowany przez serwis producenta lub autoryzowanego partnera producenta serwera.</p> <p>Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej na zasadach opisanych w rozdziale V SOPZ do dnia 31.03.2026 r. włącznie.</p>
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. 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 Dyrektywy WEEE 2002/96/EC. 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 umieszczenie oferowanego urządzenia w rejestrze internetowym <b>www.epeat.net</b> na poziomie min. Epeat bronze według normy wprowadzonej w 2019 roku.</p>

### III. Parametry techniczno-funkcjonalne dla macierzy dyskowej.

Element konfiguracji	Wymagania minimalne
Obudowa	Obudowa o wysokości maksymalnie 2U dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie. Co najmniej 24 zatoki przystosowane do instalacji dysków NVMe.
Kontroler dyskowy	<p>Zainstalowane minimum dwa redundantne kontrolery pamięci dyskowej, pracujące w trybie symetrycznym Active-Active, obsługujące protokół komunikacji NVMe z dyskami.</p> <p>Pod określeniem tryb Active-Active Symetryczny Zamawiający rozumie, że zasób pamięci dyskowej jest równolegle dostępny na co najmniej 4 portach należących do co najmniej 2 różnych kontrolerów pamięci dyskowej. Każdy z kontrolerów musi mieć możliwość prezentacji wszystkich wolumenów utworzonych w ramach całej pamięci dyskowej. Dodatkowo kontrolery muszą posiadać wbudowaną funkcjonalność szyfrowania dysków w standardzie AES 256.</p> <p>Nie jest dopuszczalne rozwiązanie, w którym usługi protokołu Fibre Channel realizowane są w oparciu o emulację protokołu FC na wewnętrznym systemie plików pamięci dyskowej.</p> <p>Nie dopuszcza się rozwiązania zbudowanego z kilku macierzy połączonych wirtualizatorem.</p>
Procesor	Architektura przetwarzania danych w ramach procesów wewnętrznych na kontrolerach musi być realizowana za pomocą procesorów x86 firmy Intel serii co najmniej Sapphire Rapids.

	Każdy z kontrolerów musi być wyposażony w procesor o co najmniej 12 rdzeniach o taktowaniu minimum 2.5 GHz.
Pamięć cache	Macierz dyskowa musi posiadać zainstalowaną pamięć cache DDR5 o sumarycznej pojemności fizycznej co najmniej 760GB. Nie dopuszcza się użycia pamięci cache zbudowanej w formie dodatkowych, dedykowanych dysków SSD lub Flash. W przypadku awarii zasilania dane z pamięci cache muszą być zabezpieczone metodą trwałego zapisu do pamięci nieulotnej.
Wydajność	Wymagana wydajność co najmniej 180K IOPS przy włączonej deduplikacji i kompresji danych. Dla wydajności macierzy należy przyjąć warunki: odczyt/zapis na poziomie 70/30, 100% losowo przy bloku 8kB, zerowych trafieniach w pamięć CACHE.
Zasilacz	Dwa w pełni redundantne zasilane prądem 230V
Porty sieciowe	Każdy z dostarczanych kontrolerów pamięci dyskowej musi być wyposażony w co najmniej 4 interfejsy FC, każdy o przepustowości co najmniej 32 Gbps. Każdy z Portów FC musi być obsadzony właściwą do komunikacji wkładką. Macierz dyskowa musi umożliwiać instalację następujących interfejsów sieciowych: <ul style="list-style-type: none"> <li>• Co najmniej 32 interfejsy FC, każdy o przepustowości co najmniej 64 Gbps.</li> <li>• Co najmniej 16 interfejsów iSCSI, każdy o przepustowości co najmniej 25 Gbps.</li> <li>• Co najmniej 8 interfejsów Ethernet (TCP), każdy o przepustowości co najmniej 100 Gbps.</li> </ul>
Dyski	Co najmniej 9 wewnętrznych dysków, każdy w technologii co najmniej NVMe 1.4, każdy o pojemności co najmniej 7.6 TB i posiadający podwójne interfejsy do komunikacji z kontrolerami pamięci dyskowej.
Efektywna pojemność	Co najmniej 110 TiB pojemności efektywnej na dane, po uwzględnieniu mechanizmu redukcji danych ADR max. 4:1 przy 90% pool depletion oraz uwzględnieniu mechanizmu zapewniającego odporność na awarie dowolnych 2 dysków macierzy.
Kompresja i deduplikacja	Macierz dyskowa musi posiadać mechanizmy kompresji i deduplikacji danych w trybie in-line. Funkcjonalność kompresji musi zostać realizowana przez dedykowane, wbudowane moduły sprzętowe.
Rozbudowa	Macierz dyskowa musi umożliwiać rozbudowę do co najmniej 70 dysków NVMe, bez użycia wirtualizacji innych macierzy i/lub łączenia kilku macierzy w jeden stos. Macierz dyskowa musi umożliwiać rozbudowę do co najmniej 1.8 PB surowej przestrzeni raw, otrzymanej z wewnętrznych dysków macierzy, bez użycia wirtualizacji innych macierzy oraz dokładania dodatkowych kontrolerów. Cena musi zawierać koszt licencji na obsługę maksymalnej obsługiwanej pojemności jednak nie mniejszej niż 1.8 PB pojemności raw.
Parametry szczegółowe	Pełna wewnętrzna redundancja kontrolerów, portów wewnętrznych, zasilania, chłodzenia i ścieżek danych na poziomie minimum N+1. Możliwość uaktualniania oprogramowania systemowego bez przerywania działania pamięci dyskowej, z utrzymaniem wszystkich funkcjonalności oraz z równoczesnym utrzymaniem dostępu do danych poprzez wszystkie ścieżki komunikacyjne Front-End z obydwu kontrolerów. <ul style="list-style-type: none"> <li>• Macierz dyskowa musi być wyposażona w system zapewniający bezpieczne, bez utraty danych, automatyczne wyłączenie w przypadku całkowitego zaniku zasilania.</li> <li>• Macierz dyskowa musi posiadać funkcjonalność oszczędzania energii, w czasie niskiej aktywności procesory powinny pracować w trybie niskiego poboru mocy.</li> <li>• Macierz dyskowa musi umożliwiać wymianę kontrolerów, kart rozszerzeń, dysków, zasilaczy i wentylatorów w trybie Hot Swap - w trakcie pracy pamięci dyskowej.</li> </ul>



- Macierz dyskowa musi umożliwiać stosowanie dysków „Hot Spare” lub alternatywnie tzw. „przestrzeni spare” i wymianę dysków w trybie Hot Swap.
- Macierz dyskowa powinna posiadać możliwość szyfrowania wybranej grupy dysków lub wszystkich dysków w niej zainstalowanych.
- Dostarczone oprogramowanie i funkcjonalności muszą być udostępniane przez firmware bez modyfikacji przez Wykonawcę i jest to standardowe oprogramowanie producenta. Zamawiający nie dopuszcza takiej sytuacji, w której oprogramowanie pamięci dyskowej jest specjalnie przygotowane dla Zamawiającego.
- Macierz dyskowa powinna posiadać możliwość szyfrowania wybranej grupy dysków lub wszystkich dysków w niej zainstalowanych.
- Dostarczone oprogramowanie i funkcjonalności muszą być udostępniane przez firmware bez modyfikacji przez Wykonawcę i jest to standardowe oprogramowanie producenta. Zamawiający nie dopuszcza takiej sytuacji, w której oprogramowanie pamięci dyskowej jest specjalnie przygotowane dla Zamawiającego.
- Jeśli jest to konieczne, wraz z macierzą dyskową muszą zostać dostarczone licencje na funkcję kontrolerów umożliwiającą wykorzystywanie obu kontrolerów macierzy dyskowej w taki sposób, aby oprogramowanie zainstalowane w systemie operacyjnym klienta (serwera do wirtualizacji pamięci dyskowej) automatycznie przełączało ścieżki do zasobów, np. w przypadku uszkodzenia portu karty HBA, przełącznika SAN, kontrolera pamięci dyskowej czy przewodu światłowodowego.
- Macierz dyskowa musi posiadać funkcjonalność zdalnej replikacji danych w trybie synchronicznym i asynchronicznym za pomocą protokołu FC i iSCSI oraz replikację active-active typu Metro Cluster (równoległy dostęp do wolumenów z obydwu macierzy, w każdej parze replikacyjnej w trybie zapisu i odczytu). Oprogramowanie musi zapewniać funkcjonalność zawieszania replikacji i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zmiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora.
- Macierz dyskowa musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point in time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym. Oferowane urządzenie musi obsługiwać minimum 400 000 kopii migawkowych (1024 per udział/dysk logiczny). Realizacja kopii migawkowych w trybie Copy-on-Write nie jest dopuszczona.
- Dostarczane oprogramowanie zarządzające macierzą dyskową oraz licencje muszą umożliwiać:
  - stałe monitorowanie stanu macierzy przez jej producenta z wykorzystaniem połączenia internetowego i protokołu HTTPS.
  - informowanie o wykorzystaniu zasobów dyskowych macierzy m.in. całkowitej pojemności przestrzeni dyskowej macierzy, wykorzystanej przestrzeni dyskowej, skonfigurowanej przestrzeni przydzielonej do serwerów i nie przydzielonej do serwerów oraz przestrzeni nie skonfigurowanej (wolnej);
  - monitorowanie zasobów wykorzystujących funkcjonalność thin-provisioning i ostrzeganie z wyprzedzeniem o możliwości wyczerpania zasobów;
  - monitorowanie stanu pracy par replikacyjnych, kopii migawkowych i klonów oraz funkcjonalności klastra active-active;
  - bieżące monitorowanie wydajności macierzy mierzonej w operacjach IOPS (zapis i odczyt), strumieniu MB/s (zapis i odczyt) oraz czasów



	<p>odpowiedzi RT (zapis i odczyt) m.in. dla poszczególnych wolumenów logicznych, puli dyskowych oraz portów;</p> <ul style="list-style-type: none"> <li>- przygotowywanie raportów historycznych z okresu co najmniej 12 miesięcy zawierających informacje o wydajności mierzonej w IOPS i MB/s dla poszczególnych wolumenów logicznych i puli dyskowych.</li> <li>- wykrywanie błędów i izolowanie uszkodzeń, monitorowanie w czasie rzeczywistym.</li> <li>- zarządzanie macierzą z graficznego interfejsu użytkownika (GUI), linii komend (CLI) oraz programowego REST API.</li> <li>- monitoring i analizę wydajności systemu pamięci masowej (również macierzy firm trzecich), przełączników SAN oraz serwerów.</li> <li>- monitorowanie parametrów wydajnościowych w zakresie co najmniej IOPS, MB/s oraz czasów odpowiedzi RT i raportowanie przekroczenia zdefiniowanych progów.</li> <li>- korelację zmian parametrów wydajnościowych ze zmianami konfiguracji w środowisku.</li> <li>- generowanie alertów dla administratora przez e-mail, SNMP</li> <li>- wykorzystanie zewnętrznych serwerów uwierzytelniania użytkowników: MS AD/LDAP</li> <li>- automatyzację zadań administracyjnych utworzoną w formie framework – graficznie przedstawienie zadań wykonywanych automatycznie zdefiniowany do uruchomienia poprzez wykrycie monitu (trigera).</li> <li>- automatyzowanie zmiany parametrów QOS dla wewnętrznej wirtualizacji zasobów udostępnianych do hostów/serwerów</li> <li>- zarządzanie oraz konfiguracja systemu kopii migawkowych wraz z repliką na inne ośrodki za pomocą GUI</li> </ul>
Wsparcie dla systemów operacyjnych	<p>Macierz musi wspierać co najmniej poniższe systemy:</p> <ul style="list-style-type: none"> <li>• VMware ESXi 7.0 i nowszy</li> <li>• Windows Server 2022</li> <li>• Oracle Linux 8</li> <li>• Red Hat EL 8 i nowszy</li> <li>• Citrix Hypervisor 8.2 LTSR</li> </ul> <p>Informacja o wspieranych systemach operacyjnych musi być dostępna na oficjalnej stronie producenta macierzy.</p>
Gwarancja, wsparcie techniczne	<p>Co najmniej 2-letnia gwarancja producenta w miejscu instalacji.</p> <p>Możliwość zgłaszania awarii w trybie 24x7.</p> <p>Reakcja serwisu 4 h, usunięcie awarii NBD.</p> <p>Serwis realizowany przez serwis producenta lub autoryzowanego partnera producenta serwera.</p> <p>Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej na zasadach opisanych w rozdziale V SOPZ do dnia 31.03.2026 r. włącznie.</p>

#### IV. Parametry techniczno-funkcjonalne dla przełącznika SAN

	Element konfiguracji	Wymagania minimalne
1.	Typ obudowy	Obudowa do montażu w szafie rack 19" za pomocą dostarczonych dedykowanych elementów.
2.	Typ przełącznika	<ul style="list-style-type: none"> <li>• Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, Gb/s w zależności od rodzaju zastosowanych wkładek SFP.</li> <li>• Przełącznik FC musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzone wkładkami SFP 16Gb/s Short Wave.</li> </ul>
3.	Mechanizmy zwiększające poziom bezpieczeństwa	<ul style="list-style-type: none"> <li>• Mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric.</li> </ul>

		<ul style="list-style-type: none"> <li>• Uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP.</li> <li>• Uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP.</li> <li>• Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.</li> <li>• Definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control).</li> <li>• Definiowane kont administratorów w środowiskach RADIUS, TACACS+, LDAP w MS Active Directory.</li> <li>• Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS obsługa SNMP v1 oraz v3</li> <li>• IP Filter dla portu administracyjnego przełącznika</li> </ul>
4.	Możliwość konfiguracji	<ul style="list-style-type: none"> <li>• Polecenia tekstowe w interfejsie znakowym konsoli terminala.</li> <li>• Przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.</li> </ul>
5.	Narzędzia diagnostyczne	<ul style="list-style-type: none"> <li>• Logowanie zdarzeń poprzez mechanizm „syslog”.</li> <li>• Ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administratora musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu.</li> <li>• Port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością, co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric.</li> <li>• FC ping</li> <li>• FC traceroute</li> </ul>
6.	Dodatkowe wymagania	<ul style="list-style-type: none"> <li>• Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubskrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 16Gb/s lub 32Gb/s w zależności do zastosowanych wkładek FC.</li> <li>• Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 32Gb/s musi wynosić minimum 768 Gb/s end-to-end.</li> <li>• Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.</li> <li>• Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.</li> <li>• Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.</li> <li>• Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 wkładki SFP 32Gb/s to 80W.</li> </ul>

		<ul style="list-style-type: none"> <li>• Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 wkładki SFP 32Gb/s to 220 BTU na godzinę.</li> <li>• Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.</li> <li>• Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.</li> <li>• Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.</li> <li>• Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika</li> </ul>
7.	Gwarancja, wsparcie techniczne	<p>Co najmniej 2-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii w trybie 24x7. Czas reakcji – 4 godziny od zgłoszenia. Wszystkie naprawy gwarancyjne muszą być możliwe na miejscu. W przypadku braku możliwości usunięcia awarii sprzętu w miejscu użytkowania Wykonawca zobowiązany jest do dostarczenia i uruchomienia bez dodatkowych opłat sprzętu zastępczego o nie gorszych parametrach technicznych lub cechach funkcjonalnych.</p> <p>Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.</p> <p>Serwis realizowany przez producenta lub jego autoryzowanego partnera. Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej na zasadach opisanych w rozdziale V SOPZ do dnia 31.03.2026 r. włącznie.</p>

## V. Zakres wsparcia i opieki technicznej zapewnianych przez Wykonawcę w ramach zamówienia :

Wsparcie musi obejmować co najmniej:

1. Wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta lub autoryzowanego partnera serwisowego producenta.
2. Usługę wymiany uszkodzonego sprzętu.
3. Dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
4. Udzielanie porad dotyczących optymalizacji konfiguracji oraz aktualizacji urządzeń zgodnie z najnowszymi zaleceniami producenta.
5. Diagnozowanie zaistniałych problemów w trakcie eksploatacji dostarczonych urządzeń i oprogramowania.
6. Rozwiązywanie problemów sieciowych.
7. Pomoc w procesie migracji danych z posiadanej macierzy Hitachi HUS 150 na nowe rozwiązanie, uruchomieniu funkcji wirtualizacji na nowej macierzy wybranych wolumenów, tworzenia nowych partycji, rekonfiguracji sieci SAN i przydzielania zasobów.
8. Pomoc w procesie konfiguracji i rekonfiguracji parametrów nowej macierzy dyskowej w tym optymalizacja działania i wykorzystania zasobów.
9. Od poniedziałku do piątku w godzinach od 8:00 do 17:00 telefoniczny dostęp do pracownika Wykonawcy, który będzie posiadał odpowiednią wiedzę w zakresie oferowanych rozwiązań oraz udzieli pomocy administratorom Zamawiającego przy rozwiązywaniu problemów.
10. Raz do roku wykonywanie konserwacji infrastruktury.
11. Min raz do roku aktualizacji oprogramowania wbudowanego na macierzy dyskowej.
12. Prace serwisowe muszą odbywać się w siedzibie Zamawiającego.

## VI. Zakres usług instalacji i wdrożenia



## 1. Przygotowanie projektu technicznego i dokumentacji powykonawczej.

- 1.1. Analiza obecnych konfiguracji urządzeń w infrastrukturze Zamawiającego,
- 1.2. Migracja funkcjonalności z obecnych urządzeń -udzielenie konsultacji w trakcie i po migracji funkcji sieciowych oraz konfiguracji z obecnie wykorzystywanych routerów oraz firewalli na nowe urządzenia.
- 1.3. Pomoc w migracji starych urządzeń na nowe.
- 1.4. Zapewnienie wsparcia technicznego w procesie wymiany starych firewalli na nowe, z uwzględnieniem minimalizacji przestojów i utrzymania ciągłości działania sieci.
- 1.5. Pomoc w przeprojektowaniu istniejącej sieci.
- 1.6. Konsultacje w zakresie przeprojektowania istniejącej infrastruktury sieciowej, w celu zoptymalizowania jej pod kątem nowych urządzeń oraz przyszłych potrzeb.
- 1.7. Pomoc w uruchomieniu mechanizmów bezpieczeństwa.
- 1.8. Wsparcie w konfiguracji i wdrożeniu zaawansowanych mechanizmów bezpieczeństwa, w tym subskrypcji na IPS oraz rozpoznawanie aplikacji, aby zapewnić zgodność z najlepszymi praktykami w zakresie ochrony sieci.
- 1.9. Określenie warunków instalacji i podłączenia do sieci zasilającej oraz logicznej.
- 1.10. Określenie konfiguracji urządzeń oraz sposobu podłączenia do istniejącej infrastruktury,
- 1.11. Uzgodnienie z zamawiającym konfiguracji zasobu dyskowego dla macierzy dyskowej, sieci SAN i sposobu podłączenia do istniejącej infrastruktury SAN.
- 1.12. Wykonawca zapewnia wszelkie komponenty i akcesoria niezbędne do instalacji dostarczonej infrastruktury takie jak: kable, przewody, patchcordsy miedziane i światłowody, wkładki światłowody itp.

## 2. Instalacja i wdrożenie rozwiązania:

- 2.1. Minimalne czynności wdrożeniowe dla urządzeń typu firewall:
  - 2.1.1. Montaż we wskazanych przez Zamawiającego szafach nowych urządzeń, ich usieciowienie
  - 2.1.2. Aktualizacja oprogramowania wbudowanego i dodatkowego,
  - 2.1.3. Migracja usług i funkcjonalności z obecnie wykorzystywanych urządzeń (router, firewall) na nowo dostarczone urządzenia, w szczególności:
    - przenoszenie reguł zapory i polityk bezpieczeństwa
    - przeniesienie instancji routingu z routerów
    - optymalizacja konfiguracji
  - 2.1.4. Demontaż starych urządzeń
  - 2.1.5. Sprawdzenie poprawności podłączenia urządzeń do infrastruktury Zamawiającego,
  - 2.1.6. Rekonfiguracja routerów MX Juniper w szkielet sieci
  - 2.1.7. Testy niezawodnościowe
  - 2.1.8. Testy funkcjonalności
- 2.2. Minimalne czynności wdrożeniowe dla macierzy dyskowej i sieci SAN.
  - 2.2.1. Montaż we wskazanych przez Zamawiającego szafach nowych urządzeń, ich usieciowienie
  - 2.2.2. Aktualizacja oprogramowania wbudowanego i dodatkowego,
  - 2.2.3. Konfiguracja macierzy w uzgodnieniu z zamawiającym,
  - 2.2.4. Konfiguracja sieci SAN,
  - 2.2.5. Wystawienie zasobów z istniejącej macierzy dyskowej poprzez zwirtualizowanie ich zasobów.
  - 2.2.6. Wystawienie zasobu dyskowego do serwerów
- 2.3. Minimalne czynności wdrożeniowe dla urządzeń typu Serwery:
  - 2.3.1. Montaż we wskazanych przez Zamawiającego szafach nowych urządzeń, ich usieciowienie
  - 2.3.2. Aktualizacja oprogramowania wbudowanego i dodatkowego,
  - 2.3.3. Konfiguracja serwerów, adresów sieciowych,
  - 2.3.4. Podłączenie serwerów do wystawionych zasobach na macierzy dyskowej.

### 3. Wykonanie dokumentacji powykonawczej

#### 3.1. Opis zainstalowanych urządzeń.

3.1.1. Opis rozmieszczenia urządzeń w szafach serwerowych i dystrybucyjnych.

3.1.2. Opis połączeń elektrycznych i logicznych, adresacja interfejsów produkcyjnych i konfiguracyjnych.

3.2. Szczegółowa konfiguracja zainstalowanych urządzeń ze schematami połączeń sieci WAN, LAN i SAN.

3.3. Zabezpieczone na zewnętrznym nośniku pliki konfiguracyjne wszystkich dostarczonych urządzeń.

3.4. Adresy, konta i hasła dostępu do oprogramowania do zarządzania i monitorowania zainstalowanych urządzeń.

### 4. Szkolenia

4.1. Przeprowadzenie szkoleń dla 6 administratorów z zakresu administrowania, reagowania na awarie dostarczonym rozwiązaniem w wymiarze min 16h.

4.2. Prace wdrożeniowe nie mogą spowodować utraty gwarancji oraz zdestabilizować posiadanej sieci MAN zbudowanej na urządzeniach firmy Juniper oraz data Centra bazującego na środowisku serwerowym HPE oraz storage Hitachi.

### 5. Dodatkowe wymagania.

5.1. Serwis (Firewall, serwery, macierz dyskowa) musi być realizowany przez producenta lub autoryzowanego partnera, który posiada stosowane uprawnienia.

5.2. Instalacja i konfiguracja urządzeń musi być realizowana zgodnie z certyfikatem jakości ISO 9001 -2015 oraz ISO/IEC 27001:2013.

5.3. Wszystkie dostarczone w ramach zamówienia urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Oferowane urządzenia muszą być przeznaczone do sprzedaży na terenie Unii Europejskiej i być objęte gwarancją producenta zapewniającą realizację uprawnień wynikających z tejże gwarancji na terenie Polski, przez Zamawiającego i na jego rzecz, bez względu na kanał dystrybucji, będący źródłem nabycia przedmiotu zamówienia.