

.....
Pieczęć Wykonawcy/Wykonawców

„Dostawa serwera dla GDDKiA Oddział w Krakowie”

Oświadczamy, że oferowany przez nas sprzęt posiada następujące parametry:

1. Serwer - 1 szt.

Oferowany model

Producent

Lp.	Opis	Minimalne wymagania	Potwierdzenie spełnienia
1	Obudowa	a) Obudowa Rack o wysokości 2U b) 16 wnęk na dyski 2.5" c) Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej d) Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.	TAK/NIE*

2	Płyta główna	a) Płyta główna z możliwością zainstalowania do dwóch procesorów. b) Obsługa procesorów 32 rdzeniowych. c) Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. d) Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. e) Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
3	Chipset	a) Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	TAK/NIE*
4	Procesor	a) Zainstalowany jeden procesor min. 20-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiającym osiągnięcie wyniku min. 356 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	TAK/NIE*
5	RAM	a) 2x 32GB DDR5 RDIMM 6400MT/s,	TAK/NIE*
6	Kontroler RAID	a) Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących 	TAK/NIE*
7	Dyski twarde	a) Zainstalowane: <ul style="list-style-type: none"> 6x dysk SAS o pojemności min. 20TB, Hot-Plug 2x dysk SSD STA o pojemności min. 1.92TB Read Intensive 	TAK/NIE*
8	Gniazda PCI	a) Dwa sloty PCIe	TAK/NIE*

		
9	Interfejsy sieciowe /FC/SAS	a) 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy b) 2 port VGA z czego jeden z przodu obudowy c) Możliwość rozbudowy o port RS232	TAK/NIE*
10	Video	a) Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	TAK/NIE*
11	Wentylatory	a) Redundantne, Hot-Plug	TAK/NIE*
12	Zasilacze	a) Redundantne, Hot-Plug min. 1100W klasy Titanium	TAK/NIE*
13	Elementy montażowe	a) Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych b) Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych	TAK/NIE*
14	Bezpieczeństwo	a) Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. b) 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.	TAK/NIE*

		c) Możliwość wyłączenia w BIOS funkcji przycisku zasilania. d) BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła e) Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. f) Moduł TPM 2.0 g) Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera h) Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem i) Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.	
15	Karta Zarządzania	a) Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane 	TAK/NIE*

		<p>historyczne powinny być dostępne przez min. 7 dni wstecz.</p> <ul style="list-style-type: none"> • 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 opraciu o harmonogram • Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera 	
--	--	---	--

		<ul style="list-style-type: none"> • Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI <p>b) Możliwość rozszerzenia funkcjonalności karty o:</p> <ul style="list-style-type: none"> • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch • 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 (w CFM) 	
16	Oprogramowanie do zarządzania	a) Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:	<p>TAK/NIE*</p> <p>.....</p>

		<ul style="list-style-type: none"> • 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 	<p>.....</p> <p>.....</p>
--	--	--	---------------------------

		<ul style="list-style-type: none"> • 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 modułarnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. 	
--	--	--	--

		<ul style="list-style-type: none"> • 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 zarządzającymi • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V 	
17	Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware.</p> <p>Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <p>a) Monitoring:</p> <ul style="list-style-type: none"> • ilość podłączonych oraz rozłączonych systemów • stan podłączonych urządzeń • informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów • Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia • informacje o statusie gwarancji dla poszczególnych urządzeń • informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń • informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. • Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych • Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie 	<p>TAK/NIE*</p> <p>.....</p> <p>.....</p> <p>.....</p>

		<p>parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych</p> <ul style="list-style-type: none"> • Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych • Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC • Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej • Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ➤ Obciążeniu procesora ➤ Zużyciu pamięci RAM ➤ Temperaturze procesorów ➤ Temperaturze powietrza wlotowego ➤ Zużyciu prądu ➤ Zmianach w fizycznej konfiguracji serwera ➤ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach • Monitoring parametrów pamięci masowych z informacją o minimum <ul style="list-style-type: none"> ➤ Opóźnienia ➤ IOPS ➤ Przepustowości ➤ Utylizacji kontrolerów ➤ Pojemność całkowita i dostępna ➤ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów 	
--	--	--	--

		<ul style="list-style-type: none"> ➤ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach ➤ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ➤ Informacje o poziomie redukcji ➤ Informacje o statusie replikacji oraz snapshotów • Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> ➤ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ➤ Stanie komponentów: zasilacze, wentylatory ➤ Podłączonych hostach ➤ Ilości i statusu portów ➤ Utylizacji procesora ➤ Utylizacji poszczególnych portów ➤ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach • Aktualizacja firmware <ul style="list-style-type: none"> ➤ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ➤ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ➤ możliwość aktualizacji firmware, oprogramowania zarządzającego dla 	
--	--	---	--

		<p>rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania</p> <ul style="list-style-type: none"> ➤ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ➤ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania <ul style="list-style-type: none"> • Raporty <ul style="list-style-type: none"> ➤ Możliwość generowania raportów dla serwerów zawierających informację <ul style="list-style-type: none"> - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej - Średnim obciążeniu: procesorów, pamięci RAM, IO, ➤ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ➤ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> ➤ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik 	
--	--	---	--

		<p>bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia</p> <ul style="list-style-type: none"> ➤ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń ➤ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych ➤ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów <ul style="list-style-type: none"> • Wspierane urządzenia <ul style="list-style-type: none"> ➤ Urządzenie Producenta dostarczane w ramach postępowania ➤ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent <ul style="list-style-type: none"> ➤ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury • Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> ➤ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz 	
--	--	--	--

		zarządzania incydentami w ramach infrastruktury <ul style="list-style-type: none"> Inne <ul style="list-style-type: none"> Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android 	
18	Certyfikaty	<p>a) Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</p> <p>b) Serwer musi posiadać deklarację CE</p> <p>c) Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami</p> <p>d) 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 wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu</p> <p>e) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025</p>	TAK/NIE*

19	Dokumentacja użytkownika	a) Zamawiający wymaga dokumentacji w języku polskim lub angielskim b) Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela	TAK/NIE*
20	Warunki gwarancji	a) Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat b) Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet c) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania d) Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy e) Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki f) Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę g) Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego h) Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym	TAK/NIE*

		<p>wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</p> <p>i) Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii.</p> <p>Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> • Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego 	
--	--	--	--

		<p>zgodnie z umową serwisową zakupionego produktu</p> <p>h) Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty</p>	
--	--	--	--