Załącznik nr 1 do SWZ– opis przedmiotu zamówienia

Specyfikacja techniczna urządzeń

Nr	CZĘŚĆ I	
1	**Serwery**	
	Ilość sztuk: 2	
	Parametry	**Wartości min/ wartości max.**
	Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) Wyposażony w zamykany na klucz, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. Serwer posiadający możliwość fabrycznego zamontowania czujnika, otwarcia obudowy, który współpracuje z modułem zarządzania serwera.
	Procesor serwer 1	Jeden procesor min. dwunastordzeniowy, x86 - 64 bity, Intel Xeon 4214R (min. 2,40GHz/12-core/100W) lub równoważny procesor min. 12 rdzeniowy, osiągający w testach SPECrate2017_int_base powyżej 140 punktów w konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org lub innej, równoważnej organizacji weryfikującej parametry urządzenia bądź stosownej jednostki certyfikującej W braku takiego potwierdzenia, Zamawiający dopuszcza przedstawienie raportu z badań. Płyta główna wspierająca zastosowanie procesorów od 4 do min. 28 rdzeniowych, mocy do min. 200W i taktowaniu CPU do min. 3.6GHz.
	Procesor serwer 2	Jeden procesor min. ośmiordzeniowy, x86 - 64 bity, Intel Xeon 6234 (min. 3,30GHz/8-core/130W) lub równoważny procesor min. 8 rdzeniowy, osiągający w testach SPECrate2017_int_base powyżej 120 punktów w konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org lub innej, równoważnej organizacji weryfikującej parametry urządzenia bądź stosownej jednostki certyfikującej W braku takiego potwierdzenia, Zamawiający dopuszcza przedstawienie raportu z badań. Płyta główna wspierająca zastosowanie procesorów od 4 do min. 28 rdzeniowych, mocy do min. 200W i taktowaniu CPU do min. 3.6GHz.
	Liczba procesorów w serwerze	Min. 1 procesor z możliwością rozbudowy do min. 2 procesorów
	Pamięć operacyjna	Minimum 128 GB RDIMM DDR4 2933 MT/s w modułach o pojemności minimum 32GB każdy, kompatybilna z oferowaną płytą główną. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC, Online Spare oraz Memory Mirror.
	Sloty rozszerzeń	Minimum 2 aktywne gniazda PCI-Express generacji 3, w tym min. gniazdo szybkości x16 (szybkość slotu – bus width).
	Dysk twardy	Zatoki dyskowe gotowe do zainstalowania minimum 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5" i opcja rozbudowy/rekonfiguracji o dodatkowe minimum 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5" montowane z przodu obudowy oraz możliwość zainstalowania minimum 1 dysku SFF SAS/SATA/SSD, 2,5" z tyłu serwera. Serwer musi posiadać możliwość instalacji pamięci typu flash – kart microSD/SD o pojemności min. 32 GB z obsługą ochrony danych min. RAID-1.Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Zainstalowane min. 2 dyski o pojemności min. 480 GB SSD SATA w trybie Mixed Use lub równoważnym.
	Kontroler	Zainstalowany kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę minimum 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Serwer posiada możliwość rozbudowy o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z minimum 4GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
	Interfejsy sieciowe	Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń". Minimum 2 karty, minimum 1 portowe FC 16Gb lub równoważne obsadzone wkładkami SFP+ SW minimum 16 Gb/s. Dołączone kompatybilne kable FC o długości minimum 2m w liczbie odpowiadającej liczbie portów FC do połączenia kart FC serwer-macierz.
	Karta graficzna	Zintegrowana karta graficzna
	Porty	Minimum 4x USB 3.0 (w tym minimum 1 port wewnętrzny) Minimum 1x VGA Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy o: - dodatkowy port DisplayPort dostępny z przodu serwera bez stosowania jakichkolwiek przejściówek; - port szeregowy typu DB9/DE-9 (9 pinowy) lub równoważny, wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się też stosowania przejściówek na kartach PCI.
	Zasilacz	Minimum 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

	Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
	Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, nie powodująca zmniejszenia minimalnej wymaganej liczby gniazd PCIe w serwerze, o minimalnej funkcjonalność: • monitorowanie podzespołów serwera: temperatura zasilacza, wentylatorów, procesorów, pamięci RAM, kontrolerów macierzowych i dyskowych (fizyczne i logiczne), karty sieciowe • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera; • dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI); - z poziomu linii komend; • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów; • monitorowanie zasilania oraz zużycia energii przez serwer z możliwością graficznej prezentacji; • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping); • zdalna aktualizacja oprogramowania (firmware); wsparcie dla Microsoft Active Directory lub równoważne.
	System monitorowania i analizowania konfiguracji serwerów	Każdy serwer winien być wyposażony w dostęp do systemu.. Jeżeli wymaga to dodatkowych licencji, Wykonawca winien dostarczyć wszystkie wymagane licencje. System w postaci platformy uruchamianej w chmurze, niezależny od infrastruktury IT zamawiającego oraz dostępny poprzez interfejs www. System musi zapewniać: - scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); - informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; - prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; - rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom; - analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania; - prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		- zalecenia dotyczące eliminacji źródeł/przyczyn problemów wydajnościowych serwerów.
	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019 lub nowszy Red Hat Enterprise Linux (RHEL) 7.x lub nowszy lub SUSE Linux Enterprise Server (SLES) 12 lub nowszy lub VMware ESXi 6.7 lub inny, równoważny
	Gwarancja	Minimum 24 miesięczny okres gwarancji producenta z naprawą w miejscu instalacji sprzętu najpóźniej następnego dnia roboczego od zgłoszenia usterki. Producent urządzenia musi umożliwić skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu. Pakiet gwarancyjny winien być składnikiem serwera oraz ma być przypisany do sprzętu na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań ze strony użytkownika Serwer nie będzie posiadał plomb lub innych elementów ograniczających dostęp do wnętrza. Udzielona gwarancja nie będzie ograniczała w rozbudowie lub rekonfiguracji serwera o ile będą one wykonywane zgodnie z wymogami technicznymi serwera. Możliwość realizacji gwarancji bezpośrednio przez serwis producenta z pominięciem dostawcy. Możliwość pobierania dokumentacji i sterowników z jednej lokalizacji w sieci Internet
	Inne	Sprzęt powinien być produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważne oraz posiadać deklaracje zgodności CE. Dokumenty te Wykonawca przedstawi po podpisaniu Umowy. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne.
	Szczegółowa specyfikacja techniczna	Wykonawca zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu wraz z podaniem numerów katalogowych poszczególnych modułów/podzespołów. Zamawiający wyklucza możliwość używania jakichkolwiek podzespołów i części, które nie zostały przebadane przez producenta serwera na okoliczność zgodności z oferowanym serwerem i które mogą wpłynąć na warunki gwarancji.

2	**Macierz Dyskowa**	
	Ilość sztuk: 1	
	Parametry	**Wartości min/ wartości max.**
	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

	Przestrzeń dyskowa	Macierz musi być wyposażona w minimum - 5 dysków SSD SFF o pojemności minimum 960 GB każdy. - 9 dysków SAS 10K SFF o pojemności minimum 1.8 TB każdy Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 90 dysków twardych.
	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. Komunikacja z dyskami 12Gb SAS.
	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej z minimum 128 dysków. Konfiguracja takiej grupy RAID musi umożliwiać zmianę rozmiaru takie grupy poprzez dodawanie i odejmowanie pojedynczych dysków w trybie online bez konieczności przerywania dostępu do danych.
	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC 16Gb lub równoważne. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
	Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 2 lat. Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 4 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
	Interfejsy do hostów	Macierz musi posiadać, co najmniej 4 porty FC 16Gb obsadzone wkładkami SFP SW 16 Gb/s
	Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. Wymagana możliwość autentykacji poprzez LDAP lub równoważne oraz funkcjonalność kontroli dostępu opartej na rolach. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy:

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		• administrator – pełen dostęp, • monitor – możliwość odczytu konfiguracji. System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów.
	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 400 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 60TB. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning lub równoważnym. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP lub równoważny). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
	Wewnętrzne kopie migawkowe	Macierz 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 alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 50 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
	Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		urządzenia.
	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux lub równoważne. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
	Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.
	Gwarancja	Minimum 24 miesięczny okres gwarancji producenta z naprawą w miejscu instalacji sprzętu najpóźniej następnego dnia roboczego od zgłoszenia usterki. Producent urządzenia musi umożliwić skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu. Pakiet gwarancyjny winien być składnikiem serwera oraz ma być przypisany do sprzętu na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań ze strony użytkownika Serwer nie będzie posiadał plomb lub innych elementów ograniczających dostęp do wnętrza. Udzielona gwarancja nie będzie ograniczała w rozbudowie lub rekonfiguracji serwera o ile będą one wykonywane zgodnie z wymogami technicznymi serwera. Możliwość realizacji gwarancji bezpośrednio przez serwis producenta z pominięciem dostawcy.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		Możliwość pobierania dokumentacji i sterowników z jednej lokalizacji w sieci Internet
	Inne	Sprzęt powinien być produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważne oraz posiadać deklaracje zgodności CE. Dokumenty te Wykonawca przedstawi po podpisaniu Umowy. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne.
	Szczegółowa specyfikacja techniczna	Wykonawca zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu wraz z podaniem numerów katalogowych poszczególnych modułów/podzespołów. Zamawiający wyklucza możliwość używania jakichkolwiek podzespołów i części, które nie zostały przebadane przez producenta serwera na okoliczność zgodności z oferowanym serwerem i które mogą wpłynąć na warunki gwarancji.

3	**Oprogramowanie**	
	Parametry	**Wartości min/ wartości max.**
	System operacyjny	2 licencje Windows Serwer Standard 2019 lub równoważny. Wymagania dla równoważnego systemu operacyjnego dla Windows Server 2019 Standard: • System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. • Licencja na system operacyjny musi być bez ograniczeń czasowych. • Licencje na system operacyjny muszą pozwalać na zainstalowanie przez Zamawiającego systemu na dwóch fizycznych serwerach z minimum 1 fizycznym procesorem. • Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. • Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. • System operacyjny musi posiadać graficzny interfejs użytkownika. • System operacyjny musi być w pełni kompatybilny z usługą

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		Active Directory w zakresie: a. zarządzania użytkownikami, b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c. możliwości przydzielania praw dostępu do zasobów sieciowych, d. instalacji zdalnej oprogramowania z pakietów msi, e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10. • System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. • System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. • System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. • Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. • System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. • System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6. • System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny. • System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, • administrowania oraz aktualizowania systemu. • System operacyjny musi posiadać obsługę PowerShell 5.1 • System operacyjny musi posiadać obsługa certyfikatów w Active Directory System operacyjny musi być kompatybilny z serwerami z punktu 1 (producent serwera musi udostępniać sterowniki oraz oprogramowanie do oferowanej wersji systemu operacyjnego). Dostarczona ilość licencji winna być zgodna z warunkami licencyjnymi (instalacja na serwerach z punktu 1) firmy Microsoft lub producenta systemu równoważnego.
	Licencje dostępowe	60 licencji dostępowych (User CAL) do oprogramowania Windows Server 2019 lub równoważnego 40 licencji dostępowych (Device CAL) do oprogramowania Windows Server 2019 lub równoważnego 5 licencji dostępowych (RDS User CAL) do oprogramowania Windows Server 2019 lub równoważnego Zamawiane licencje dostępowe muszą być zgodnie z oferowanym systemem operacyjnym oraz winny być zgodne z

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		warunkami licencyjnymi firmy Microsoft lub producenta systemu równoważnego.
UWAGA:		
Zaoferowane przez Wykonawcę serwery oraz macierz dyskowa powinny być ze sobą wzajemnie kompatybilne. Przez kompatybilność Zamawiający rozumie możliwość korzystania z zasobów oferowanej macierzy na oferowanych serwerach.		

Specyfikacja techniczna urządzeń

Nr	**CZĘŚĆ II**	
1	**Router klasy UTM**	
	Ilość sztuk: 1	
	Parametry	**Wartości min/ wartości max.**
	Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w minimum dwóch trybach: Routera z funkcją NAT lub transparentnym . System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
	Interfejsy, Dysk, Zasilanie	System realizujący funkcję Firewall musi dysponować: Porty: Min. 16 portów Ethernet 10/100/1000 Base-TX. Min. 6 gniazd SFP 1 Gbps. Min. 2 gniazda SFP+ 10 Gbps Min. 1 port konsoli szeregowej oraz min. 1 port USB umożliwiające podłączenie modemu 3G/4G Możliwość tworzenia min. 200 interfejsów wirtualnych - definiowanych jako VLAN'y (standard 802.1Q) Dysk: Zainstalowany dysk twardy o pojemności min 450GB System musi być wyposażony w zasilanie AC.
	Parametry wydajnościowe	• Firewall: obsługa nie mniej niż 1,4 mln. jednoczesnych połączeń oraz nie mniej niż 50 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 17 Gbps dla pakietów 512 B.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		• Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.0 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS): nie mniej niż 2 Gbps. • Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Kontrola Aplikacji, Antywirus: nie mniej niż 1 Gbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – nie mniej niż 1 Gbps.
	Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu – fiewall klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP lub równoważne). • Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Analiza ruchu szyfrowanego protokołem SSL. • Analiza ruchu szyfrowanego protokołem SSH.
	Redundancja, monitoring	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP lub równoważny. Powinna istnieć

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		możliwość tworzenia interfejsów redundantnych.
	Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać 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 lub równoważne. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Element systemu realizujący funkcję Firewall musi integrować 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). • VMware vCenter (ESXi). - lub równoważne.
	VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać (poniższe lub równoważne): • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • 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. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o min. HTML 5.0.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. • Minimum 300 jednoczesnych połączeń SSL VPN
	WAN	W zakresie routingu rozwiązanie zapewnia obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
	Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez: • określenie maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • określenie pasma dla poszczególnych aplikacji • możliwość zarządzania pasmem dla wybranych kategorii URL.
	Ochrona przed malware	• Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 3021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. • System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
	Ochrona przed atakami	• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków powinna zawierać minimum 4000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
	Kontrola aplikacji	• Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox, Onedrive) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
	Kontrola WWW	• Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 30 milionów adresów URL pogrupowanych w kategorie tematyczne. • W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. • Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. • W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		dokonywał inspekcji szyfrowanej komunikacji. • W ramach systemu możliwość blokowania nowo zarejestrowanych domen
	Uwierzytelnianie użytkowników w ramach sesji	System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
	Zarządzanie	• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i muszą mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. • Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. • System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
	Logowanie	W ramach logowania system pełniący funkcję Firewall musi

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. • Musi istnieć możliwość logowania do serwera SYSLOG. • Musi istnieć możliwość logowania do wbudowanego dysku twardego.
	Certyfikaty	Minimum ICSA lub EAL4 dla funkcji Firewall.
	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min 24 miesięcy.
	Gwarancja oraz wsparcie techniczne	System musi być objęty serwisem gwarancyjnym producenta przez okres min 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

2	**Zasilacz UPS z kartą zarządzającą**
	Ilość sztuk: 1
	Parametry / **Wartości min/ wartości max.**
Ogólne	Topologia UPS: line-interactive Minimalna moc pozorna: co najmniej 3000 VA Minimalna *moc* rzeczywista: nie mniej niż 2700 W Przebieg falowy: Sinus Czas przełączenia : co najwyżej 10 ms Liczba faz na wejściu: 1 (230V) Ochrona przed nagłym wzrostem napięcia Zarządzanie przez stronę www Auto-restart Alarm dźwiękowy
Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi Obudowa wyposażona w ekran kontrolny
Bateria	Minimalna pojemność baterii: 540 Ah Maksymalny czas ładowania: 3 h Pozostałe wymagania: - Akumulatory wymienialne podczas pracy

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

		- Automatyczny test baterii - Zimny start
	Porty	• Minimum 1 port zasilania wejściowego: IEC-C20 (kabel w zestawie) • Minimum 8 portów wyjściowych IEC-C13 (dołączone kable) • Minimum 1 port wyjściowy IEC-C19 (dołączony kabel) • Minimum 1 port USB (Type B) (dołączony kabel) • Minimum 1x RJ-45 Szeregowy lub równoważne spełniające wymogi dla określonego przez Zamawiającego złącza.
	Kartą zarządzającą	Kompatybilna z oferowanym zasilaczem UPS Zamontowana w dedykowanym porcie zasilacza Zdalne zarządzanie za pośrednictwem protokołu Telnet lub SSH Szyfrowanie kluczem publicznym/prywatnym o długości do 2048 bitów Obsługa czujnika temperatury i wilgotności Możliwość działania w sieci z protokołem IPv6. Interfejs dla przeglądarki WWW Możliwośc odczytywania informacji o stanie akumulatora, w tym parametrów kasety akumulatorowej. Informowanie o wystąpieniu zdarzeń w pracy akumulatora w czasie rzeczywistym. Wyposażona w porty: - Minimum 2x USB - Minimum 1x RJ-45 LAN 10/100 - Minimum 2x uniwersalne porty wejścia/wyjścia
	Certyfikaty	CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, GS Mark, IRAM, RCM, VDE, WEEE lub równoważne.
	Gwarancja	Minimum 2 lata na zasilacz oraz kartę zarządzającą.

3	**Kabel MCC Multi USB – USB C**
	Ilość sztuk: 1
	Parametry: długość: min. 25 cm, jeden koniec kabla MCC Multi USB drugi koniec kabla USB C zgodny z posiadanym przez Zamawiającego urządzeniem typu gimbal DJI Ronin-S
	Gwarancja: Minimum 2 lata.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł