

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

Wkładki do przełączników Aruba – 50 szt.	
1	<p>Dostawa do posiadanych przełączników (HP Switch 5406Rz12 (J9850A)) wkładek światłowodowych „Aruba 10G SFP+ LC SR 300 mm MMF XCVR (J9150D)” lub równoważnych charakteryzujących się łącznie:</p> <ul style="list-style-type: none"> - wszystkimi cechami wkładek „Aruba 10G SFP+ LC SR 300 mm MMF XCVR (J9150D), - „dożywotnią gwarancją” jakiej udziela producent na oryginalne wkładki „Aruba 10G SFP+ LC SR 300 mm MMF XCVR (J9150D)” stosowane do przełączników (HP Switch 5406Rz12 (J9850A), - moduły SFP+ zaoferowane przez Wykonawcę które będą częścią składową urządzenia sieciowego (HP Switch 5406Rz12 (J9850A)) muszą być objęte wsparciem serwisowym producenta dla tego urządzenia i przejmować jego wsparcie (https://support.hpe.com/hpesc/public/docDisplay?cc=uk&docId=emr_na-c02707631&lang=en-uk). - dla wkładki równoważnej zaoferowanej przez Wykonawcę wykorzystywanej w przełączniku Aruba (HP Switch 5406Rz12 (J9850A)) wsparcie techniczne świadczone przez producenta dla tych przełączników nie może zostać zakwestionowane przez producenta przełącznika z uwagi na wykorzystanie wkładki równoważnej.
Kable światłowodowe – 30 szt.	
2	<p>1 Dostawa kabli światłowodowych LC-LC 50/125 OM3 MM duplex 7 m</p>
Licencje do serwerów HPE iLO – 3 szt.	
3	<p>1 Dostawa licencji ILO Advanced 3 lata do posiadanych 3 serwerów HPE DL 380 Gen 10 (BD505A)</p>
Maskownica do serwera – 3 szt.	
4	<p>1 Dostawa maskownicy do 3 serwerów HPE DL 380 Gen 10 (HPE Gen10 2U Bezel Kit) P/N:(858790-001)</p>
Klaster urządzeń antyspamowych – 2 szt. (urządzenia)	
5	<p>Wymagania ogólne:</p> <p>System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.</p> <p>Dopuszcza się aby poszczególne elementy wchodzące w skład systemu 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.</p> <p>Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.</p>
	<p>Parametry Fizyczne:</p> <p>System musi być wyposażony w min 4 interfejsy Gigabit Ethernet RJ-45</p>
	<p>2 System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB - w przypadku awarii dysk twardy pozostaje u Zamawiającego.</p> <p>System musi posiadać wbudowany port konsoli szeregowej.</p> <p>Zasilanie z sieci 230V/50Hz.</p>
	<p>3 Ochrona poczty:</p>

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	Wsparcie dla co najmniej 20 domen pocztowych
	System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę.
	Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
	Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
	Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
	Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
	Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
	Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
	Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
	Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3,
	Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
	Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
	Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
	Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
	Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
4	Kontrola antywirusowa i ochrona przed malware:
	Skanowanie antywirusowe wiadomości SMTP.
	Kwarantanna dla zainfekowanych plików.
	Skanowanie załączników skompresowanych.
	Definiowanie komunikatów powiadomień w języku polskim.
	Blokowanie załączników w oparciu o typ pliku.
	Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
	Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanymi dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie	

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	<p>nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.</p> <p>Ochronę typu wirus outbreake.</p> <p>Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.</p>	
5	<p>Kontrola antyspam:</p> <p>Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.</p> <p>Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.</p> <p>Szczegółowa kontrola nagłówka wiadomości.</p> <p>Analiza heurystyczna.</p> <p>Współpraca z zewnętrznymi serwerami RBL, SURBL.</p> <p>Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.</p> <p>Możliwość dostrajania filtrów Bayes'a przez poszczególnych użytkowników.</p> <p>Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.</p>	
	<p>Kontrola w oparciu o Greylisting oraz SPF.</p> <p>Filtrowanie treści wiadomości i załączników.</p> <p>Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.</p> <p>Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.</p> <p>Ochrona typu outbreake.</p> <p>Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).</p> <p>Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.</p> <p>Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)</p> <p>Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.</p>	
	<p>Ochrona przed atakami na usługę poczty:</p> <p>Ochrona przed atakami na adres odbiorcy.</p> <p>Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.</p> <p>Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.</p> <p>Kontrola Reverse DNS (ochrona przed Anty-Spoofing).</p> <p>Weryfikacja poprawności adresu e-mail nadawcy.</p>	
	6	

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

7	Funkcje dodatkowe:
	<p>Funkcje logowania i raportowania:</p> <ol style="list-style-type: none"> 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
	<p>Funkcje pracy w trybie wysokiej dostępności (HA):</p> <ol style="list-style-type: none"> 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.
	<p>Aktualizacje sygnatur, dostęp do bazy spamu:</p> <ol style="list-style-type: none"> 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
8	Zarządzanie:
	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
	Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
	Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
9	Certyfikaty:
	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
10	Serwisy i Licencje:
	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować co najmniej:
	Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 36 miesięcy.
	Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.
11	Gwarancja oraz wsparcie:

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	<p>System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p>
	<p>Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.</p>
	<p>Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.</p>
	<p>Oferent winien przedłożyć dokumenty przy dostawie:</p>
	<p>Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</p>
	<p>Wdrożenie:</p>
	<p>Czynności w ramach usługi wdrożenia Systemu:</p> <ol style="list-style-type: none"> 1. Instalacja i Konfiguracja przez Wykonawcę urządzeń służących do budowy całości Klastra urządzeń antyspamowych, przygotowanie i przeprowadzenie testów poprzedzających Odbiór jakościowy poszczególnych urządzeń, wdrożenie Systemu; 2. uruchomienie Systemu w Lokalizacji przez Wykonawcę; 3. wykonanie i przekazanie przez Wykonawcę Dokumentacji Powdrożeniowej i przeniesienie na rzecz Zamawiającego majątkowych praw autorskich do tej Dokumentacji w zakresie określonym Umową; 4. Instalacja i Konfiguracja Systemu w Lokalizacji przez Wykonawcę; 5. sprawdzenie funkcjonalności przez Wykonawcę; 6. zatwierdzenie powyższych czynności Protokołem Odbioru;
12	<ol style="list-style-type: none"> 1. Dokumentacja musi zawierać szczegółowy opis techniczny zaimplementowanego rozwiązania z opisem uruchomionych funkcjonalności. 2. Dokumentacja techniczna będzie stanowiła dokument na podstawie którego będzie możliwe odbudowanie architektury zaimplementowanego rozwiązania. 3. Dokumentacja techniczna będzie zawierała: <ol style="list-style-type: none"> 1) przedstawienie ogólnej architektury systemu. 2) ogólną architekturę wdrożenia, 3) wykorzystywane mechanizmy redundancji 4) przedstawienie szczegółowej architektury z konfiguracją redundancji (sposób pracy, komunikacja pomiędzy elementami klastra, zarządzania i monitorowanie klastra urządzeń)
13	<p>Szkolenia:</p>

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

	Wykonawca jest zobowiązany do dostarczenia w formie voucherów szkoleniowych szkolenia podstawowego autoryzowanego przez producenta dostarczonych urządzeń szkolenia dla trzech administratorów Zamawiającego. Szkolenia zostaną zrealizowane przez autoryzowany przez producenta dostarczanych Urządzeń podmiot szkoleniowy. Szkolenia zostaną przeprowadzone w języku polskim. Czas ważności voucherów nie może być krótszy niż 6 miesięcy od dnia wdrożenia Systemu. Przekazanie voucherów musi nastąpić nie później niż wdrożenie Systemu.																																														
3	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td data-bbox="183 443 183 943"></td> <td data-bbox="183 443 2150 485" style="text-align: center;">Moduł dystrybucji zasilania (PDU) do montażu w szafie 19" wraz z czujnikiem monitorującym temperaturę – 2 szt.</td> </tr> <tr> <td data-bbox="183 485 183 525"></td> <td data-bbox="183 485 2150 525">Przeznaczony do montażu w szafie 19":</td> </tr> <tr> <td data-bbox="183 525 183 566"></td> <td data-bbox="183 525 2150 566">Możliwość montażu pionowo (ZeroU) i beznarzędziowo;</td> </tr> <tr> <td data-bbox="183 566 183 608"></td> <td data-bbox="183 566 2150 608">Nominalne napięcie wejściowe: 200V, 208V, 230V;</td> </tr> <tr> <td data-bbox="183 608 183 649"></td> <td data-bbox="183 608 2150 649">Częstotliwość na wejściu: 50/60 Hz;</td> </tr> <tr> <td data-bbox="183 649 183 691"></td> <td data-bbox="183 649 2150 691">Typ elektrycznego wtyku wejściowego: IEC-320 C20;</td> </tr> <tr> <td data-bbox="183 691 183 732"></td> <td data-bbox="183 691 2150 732">Maksymalny całkowity prąd wejściowy: 16A;</td> </tr> <tr> <td data-bbox="183 732 183 774"></td> <td data-bbox="183 732 2150 774">Napięcie wyjściowe: 200V, 208V, 230V AC;</td> </tr> <tr> <td data-bbox="183 774 183 815"></td> <td data-bbox="183 774 2150 815">Gniazda elektryczne wyjściowe: 21 x IEC-320 C13, 3 x IEC-320 C19 z blokadami wyposażone w niskoprofilowe wyłączniki automatyczne;</td> </tr> <tr> <td data-bbox="183 815 183 857"></td> <td data-bbox="183 815 2150 857">Sygnalizacja za pomocą diody LED wykorzystania każdego z gniazd wyjściowych;</td> </tr> <tr> <td data-bbox="183 857 183 898"></td> <td data-bbox="183 857 2150 898">Wskaźnik obciążenia LED wskazujący status całkowitego obciążenia listwy PDU na podstawie zdefiniowanych przez użytkownika progów alarmowych;</td> </tr> <tr> <td data-bbox="183 898 183 940"></td> <td data-bbox="183 898 2150 940">Lokalny wyświetlacz umożliwiający monitorowanie poboru mocy;</td> </tr> <tr> <td data-bbox="183 940 183 981"></td> <td data-bbox="183 940 2150 981">1 Port 10/100 Base-T do zdalnego zarządzania listwą poprzez sieć TCP/IP;</td> </tr> <tr> <td data-bbox="183 981 183 1023"></td> <td data-bbox="183 981 2150 1023">Obsługa protokołów IPv4 oraz IPv6;</td> </tr> <tr> <td data-bbox="183 1023 183 1064"></td> <td data-bbox="183 1023 2150 1064">Obsługa protokołów DHCP i BOOTP;</td> </tr> <tr> <td data-bbox="183 1064 183 1106"></td> <td data-bbox="183 1064 2150 1106">Obsługa Network Time Protocol (NTP);</td> </tr> <tr> <td data-bbox="183 1106 183 1147"></td> <td data-bbox="183 1106 2150 1147">Możliwość definiowania reguł dla firewall'a;</td> </tr> <tr> <td data-bbox="183 1147 183 1189"></td> <td data-bbox="183 1147 2150 1189">Port RJ-12 (wraz z potrzebnym przewodem) zapewniający dostęp lokalny za pomocą tekstowego terminalu szeregowego;</td> </tr> <tr> <td data-bbox="183 1189 183 1230"></td> <td data-bbox="183 1189 2150 1230">Sonda do monitorowania wilgotności i temperatury w szafie podłączana do listwy PDU poprzez port monitorowania parametrów środowiskowych;</td> </tr> <tr> <td data-bbox="183 1230 183 1272"></td> <td data-bbox="183 1230 2150 1272">Możliwość aktualizacji oprogramowania sprzętowego znajdującego się w pamięci flash listwy PDU poprzez sieć TCP/IP oraz wbudowany port USB (flash driver);</td> </tr> <tr> <td data-bbox="183 1272 183 1313"></td> <td data-bbox="183 1272 2150 1313">Wbudowany port In/Out zapewniający sterowanie urządzeń poprzez oprogramowanie zarządzające;</td> </tr> <tr> <td data-bbox="183 1313 183 1355"></td> <td data-bbox="183 1313 2150 1355">Obsługa Network Port Sharing (NPS);</td> </tr> <tr> <td data-bbox="183 1355 183 1430"></td> <td data-bbox="183 1355 2150 1430">Możliwość zarządzania przez sieć za pomocą w pełni funkcjonalnych sieciowych interfejsów zarządzania, które umożliwiają zarządzanie w oparciu o standardy WWW, SNMP i Telnet. Umożliwiające użytkownikom uzyskiwanie zdalnego dostępu do urządzenia, konfigurowanie go i zarządzanie nim;</td> </tr> </table>		Moduł dystrybucji zasilania (PDU) do montażu w szafie 19" wraz z czujnikiem monitorującym temperaturę – 2 szt.		Przeznaczony do montażu w szafie 19":		Możliwość montażu pionowo (ZeroU) i beznarzędziowo;		Nominalne napięcie wejściowe: 200V, 208V, 230V;		Częstotliwość na wejściu: 50/60 Hz;		Typ elektrycznego wtyku wejściowego: IEC-320 C20;		Maksymalny całkowity prąd wejściowy: 16A;		Napięcie wyjściowe: 200V, 208V, 230V AC;		Gniazda elektryczne wyjściowe: 21 x IEC-320 C13, 3 x IEC-320 C19 z blokadami wyposażone w niskoprofilowe wyłączniki automatyczne;		Sygnalizacja za pomocą diody LED wykorzystania każdego z gniazd wyjściowych;		Wskaźnik obciążenia LED wskazujący status całkowitego obciążenia listwy PDU na podstawie zdefiniowanych przez użytkownika progów alarmowych;		Lokalny wyświetlacz umożliwiający monitorowanie poboru mocy;		1 Port 10/100 Base-T do zdalnego zarządzania listwą poprzez sieć TCP/IP;		Obsługa protokołów IPv4 oraz IPv6;		Obsługa protokołów DHCP i BOOTP;		Obsługa Network Time Protocol (NTP);		Możliwość definiowania reguł dla firewall'a;		Port RJ-12 (wraz z potrzebnym przewodem) zapewniający dostęp lokalny za pomocą tekstowego terminalu szeregowego;		Sonda do monitorowania wilgotności i temperatury w szafie podłączana do listwy PDU poprzez port monitorowania parametrów środowiskowych;		Możliwość aktualizacji oprogramowania sprzętowego znajdującego się w pamięci flash listwy PDU poprzez sieć TCP/IP oraz wbudowany port USB (flash driver);		Wbudowany port In/Out zapewniający sterowanie urządzeń poprzez oprogramowanie zarządzające;		Obsługa Network Port Sharing (NPS);		Możliwość zarządzania przez sieć za pomocą w pełni funkcjonalnych sieciowych interfejsów zarządzania, które umożliwiają zarządzanie w oparciu o standardy WWW, SNMP i Telnet. Umożliwiające użytkownikom uzyskiwanie zdalnego dostępu do urządzenia, konfigurowanie go i zarządzanie nim;
	Moduł dystrybucji zasilania (PDU) do montażu w szafie 19" wraz z czujnikiem monitorującym temperaturę – 2 szt.																																														
	Przeznaczony do montażu w szafie 19":																																														
	Możliwość montażu pionowo (ZeroU) i beznarzędziowo;																																														
	Nominalne napięcie wejściowe: 200V, 208V, 230V;																																														
	Częstotliwość na wejściu: 50/60 Hz;																																														
	Typ elektrycznego wtyku wejściowego: IEC-320 C20;																																														
	Maksymalny całkowity prąd wejściowy: 16A;																																														
	Napięcie wyjściowe: 200V, 208V, 230V AC;																																														
	Gniazda elektryczne wyjściowe: 21 x IEC-320 C13, 3 x IEC-320 C19 z blokadami wyposażone w niskoprofilowe wyłączniki automatyczne;																																														
	Sygnalizacja za pomocą diody LED wykorzystania każdego z gniazd wyjściowych;																																														
	Wskaźnik obciążenia LED wskazujący status całkowitego obciążenia listwy PDU na podstawie zdefiniowanych przez użytkownika progów alarmowych;																																														
	Lokalny wyświetlacz umożliwiający monitorowanie poboru mocy;																																														
	1 Port 10/100 Base-T do zdalnego zarządzania listwą poprzez sieć TCP/IP;																																														
	Obsługa protokołów IPv4 oraz IPv6;																																														
	Obsługa protokołów DHCP i BOOTP;																																														
	Obsługa Network Time Protocol (NTP);																																														
	Możliwość definiowania reguł dla firewall'a;																																														
	Port RJ-12 (wraz z potrzebnym przewodem) zapewniający dostęp lokalny za pomocą tekstowego terminalu szeregowego;																																														
	Sonda do monitorowania wilgotności i temperatury w szafie podłączana do listwy PDU poprzez port monitorowania parametrów środowiskowych;																																														
	Możliwość aktualizacji oprogramowania sprzętowego znajdującego się w pamięci flash listwy PDU poprzez sieć TCP/IP oraz wbudowany port USB (flash driver);																																														
	Wbudowany port In/Out zapewniający sterowanie urządzeń poprzez oprogramowanie zarządzające;																																														
	Obsługa Network Port Sharing (NPS);																																														
	Możliwość zarządzania przez sieć za pomocą w pełni funkcjonalnych sieciowych interfejsów zarządzania, które umożliwiają zarządzanie w oparciu o standardy WWW, SNMP i Telnet. Umożliwiające użytkownikom uzyskiwanie zdalnego dostępu do urządzenia, konfigurowanie go i zarządzanie nim;																																														

OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa sprzętu komputerowego
CZĘŚĆ I Sprzęt sieciowy (Wymagania minimalne)

Zdalna kontrola pojedynczych wyjść umożliwiająca odłączenie wybranych, nieużywanych wyjść (zapobieganie przeciążeniu) lub załączenia zasilania dla Zamkniętego sprzętu (minimalizacja przestoju i eliminacja konieczności podejścia do sprzętu);
Pomiar prądu zapewniający zdalne, realizowane w czasie rzeczywistym monitorowanie podłączonych obciążeń;
Pomiar: mocy czynnej, mocy chwilowej, mocy biernej, energii, współczynnika mocy;
Możliwość ustawienia wartości, przy których uruchamiany jest alarm (w celu uniknięcia przeciążenia obwodów) poprzez zdefiniowanie progów.
Alarmy sieciowe i wizualne powinny informować użytkownika o potencjalnych problemach;
Programowalne opóźnienie zasilania zapewniające użytkownikom możliwość skonfigurowania kolejności włączania i wyłączenia zasilania na poszczególnych wyjściach w celu uniknięcia kumulacji momentu rozruchowego przy starcie urządzeń, który może być przyczyną przeciążenia obwodu i odłączenie obciążeń oraz zapewniające możliwości ustalania kolejności włączania sprzętu, tak by inne zależne od niego urządzenia mogły działać prawidłowo.
Możliwość grupowania i wspólnego zarządzania wyjściami (również przy zastosowaniu kilku modułów PDU);
Możliwość konfiguracji harmonogramu zdarzeń (jednorazowych, dziennych, tygodniowych);
Możliwość tworzenia użytkowników oraz przypisania im różnych praw do sterowania poszczególnymi wyjściami,
Logowanie zdarzeń, danych oraz firewall'a;
Kopiowanie logów na zdalny komputer przy pomocy protokołów ftp lub scp;
Informowanie o zdarzeniach poprzez e-mail;
Szyfrowane połączenie przy logowaniu zdalnym;
Możliwość zapisania i odtworzenia konfiguracji do / z pliku zewnętrznego;
Przycisk reset listwy PDU;
Maksymalna wysokość: 1830.00 mm;
Czujnik uniwersalny, który monitoruje temperaturę w centrum danych lub pomieszczeniu sieciowym.
Gwarancja producenta na bezawaryjne funkcjonowanie urządzenia na okres co najmniej 12 miesięcy na miejscu u Zamawiającego. Serwis urządzeń musi być realizowany przez Producenta lub przez Autoryzowanego Partnera Serwisowego Producenta