Załącznik nr 3b do SIWZ

Przedmiot zamówienia obejmuje dostawę zgodnie z poniższym wykazem:

Przełącznik	
Lp.	**Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu**
1.	Minimum 48 portów 100BaseTX/1000BaseT
2.	Minimum 4 porty 10Gb SFP+
3.	Przepustowość: minimum 176 Gb/s
4.	Wydajność: minimum 131 Mp/s
5.	Bufor pakietów: minimum 3 MB.
6.	Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45).
7.	Wielkość tablicy routingu: minimum 1000 wpisów
8.	Tablica adresów MAC o wielkości minimum 16000 pozycji
9.	Obsługa Jumbo Frames
10.	Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9)
11.	Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN
12.	Dostęp do urządzenia przez konsolę szeregową (RS-232), http, SSHv2 i SNMPv3
13.	Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
14.	Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
15.	Obsługa Simple Network Time Protocol (SNTP) v4
16.	Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping)
17.	Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM, BGP
18.	Obsługa 802.1ad (Q-in-Q)
19.	Mechanizmy związane z zapewnieniem jakości usług w sieci: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych
20.	Obsługa uwierzytelniania użytkowników zgodna z 802.1x
21.	Obsługa uwierzytelniania użytkowników w oparciu o lokalną bazę adresów MAC
22.	Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
23.	Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
24.	Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
25.	Wbudowany serwer DHCP
26.	Ochrona przed rekonfiguracją struktury topologii, Root guard, BPDU guard, BPDU forwarding, BPDU tunnel
27.	Obsługa list kontroli dostępu IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Czasowe ACL, ACL na interfejsie VLAN
30.	Zakres pracy od 0 do 50°C
31.	Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 45 cm.
32.	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.

2. Firewall z analizatorem ruchu sieciowego – 1 sztuka		
Nazwa składnika/parametru technicznego sprzętu		**Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu**
Architektura systemu ochrony	**Typ systemu ochrony**	• System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym. • Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
	Wymagania systemowe	• System ochrony powinien spełniać wymagania w niżej wymienionym zakresie. • Obsługa nielimitowanej ilości hostów w sieci chronionej. • Typ procesora: Intel multi-core technology • Pamięć RAM: nie mniej niż 8 GB • Metalowa obudowa o wysokości maksymalnie 1U przeznaczona do montażu w szafie RACK. • Minimalna liczba i typ interfejsów fizycznych: 6x GE (IEEE 1000Base-T), 2x GE (IEEE 1000Base-X), 2x USB 3.0 (Type-A), 1x Console (RJ-45 lub DB9) z możliwością rozbudowy o co najmniej 8 x GE (IEEE 1000Base-T lub IEEE1000Base-X). • Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q) • Minimalna liczba nowych połączeń na sekundę: 135 000 • Minimalna liczba jednoczesnych połączeń: 8 000 000 • Minimalna przepustowość Firewall (IMIX): 5 500 Mbps • Minimalna przepustowość IPS: 7 000 Mbps • Minimalna przepustowość Web Proxy AV: 2 000 Mbps • Minimalna przepustowość IPSec: 1 250 Mbps • Minimalna liczba równoczesnych tuneli IPSec VPN: 1 300 • Minimalna liczba równoczesnych tuneli SSL VPN: 300 • Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB • Zintegrowany wielofunkcyjny wyświetlacz LCD
Podstawowe funkcje systemu ochrony	**Zarządzanie i utrzymanie**	• Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). • Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. • Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP • Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości min. 4096 bitów.

		• Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. • System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności. • System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. • System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. • Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). • System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. • Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. • System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. • Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej. • System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP. • Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik). • System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. • System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on- premise lub on-cloud. • Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji

		z zapisem do pliku lokalnego, do serwera FTP lub via email.
		• Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. • Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. • Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. • Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. • Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). • System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive. • W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie).
	Zapora sieciowa, konfiguracja sieciowa oraz routing	• Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. • Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas. • System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. • Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług. • Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. • System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN. • Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. • Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading. • System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). • System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking). • System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). • Rozwiązanie powinno zapewniać obsługę routingu statycznego.

		• Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). • Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). • System powinien oferować wsparcie dla IGMP snooping. • Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy). • Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. • Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). • System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. • System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. • Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. • Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów. • Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules. • Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta. • Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). • System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP. • System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania. • Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
	Podstawowe kształtowanie pasma oraz limity ilości danych	• System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników. • Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. • System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
	Bezpieczna sieć bezprzewodowa	• System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. • Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater. • Wdrożenie punktów dostępowych sieci bezprzewodowej

		powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. • Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. • Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej. • Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej. • Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. • Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication). • Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). • System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. • Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. • System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden. • System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe. • Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
	Autoryzacja użytkowników	• Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication. • Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. • System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+. • Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. • Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password).

		• Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server. • System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. • Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. • Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
	Samoobsługowy portal dla użytkowników	• Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci. • Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). • Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows. • Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android. • Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła. • Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika. • Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.
	Podstawowe opcje VPN	• System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: • Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) • Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
	Klient IPSec VPN (dostępny osobno)	• Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH. • Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512. • Wsparcie dla split-tunneling. • Wsparcie dla NAT-traversal. • Monitorowanie stanu połączenia.
Ochrona sieci	**IPS**	• Moduł ochrony klasy IPS z bazą minimum 7000 sygnatur. • Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS. • Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. • Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. • System powinien generować alerty w przypadku wykrycia

		ataku.
	ATP	• System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.
	Clientless VPN	• Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.
Ochrona i kontrola Web oraz aplikacji	**Ochrona i kontrola Web**	• Rozwiązanie powinno działać jakoTransparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. • Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP). • System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. • System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego. • Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups). • Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch). • Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów. • System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma. • System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. • Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies. • System powinien zapewniać możliwość emulacji skryptów JavaScript. • Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. • Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. • Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS. • Rozwiązanie powinno umożliwiać blokadę stron HTTPS. • Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS. • Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników. • System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.

	Ochrona i kontrola aplikacji	• Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2500 aplikacji. • Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. • Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. • Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania. • Rozwiązanie powinno umożliwiać blokowanie: - aplikacji, które pozwalają na transfer plików (np. P2P). - komunikatorów internetowych, przynajmniej Skype, Gadu-gadu. - proxy uruchamianych poprzez przeglądarki internetowe. - streaming media (radio internetowe, Youtube, Vimeo). • Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.
	Kształtowanie pasma dla Web i Aplikacji	• Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/ download/ łącznie. • Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. • Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared).
Logowanie oraz raportowanie		• System musi umożliwiać składowanie oraz archiwizację logów za pomocą wbudowanego i bezpłatnego mechanizmu o cechach analizatora ruchu, posiadającego również funkcję integracji z zewnętrznym oprogramowaniem Producenta. • System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. • System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali. • System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. • System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). • Rozwiązanie powinno umożliwiać wysyłanie raportów via email. • Rozwiązanie powinno generować raporty w PDF, HTML i

		XLS. • Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. • System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza • System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację • Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach • System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora. • System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji
Pozostałe	**Certyfikaty**	• CE, FCC Class A, CB, VCCI, C-Tick, UL, CCC
	Subskrypcje	• Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 3 lat.
	Gwarancja i wsparcie	• Wsparcie techniczne w trybie 24x7 na okres nie krótszy niż 3 lat.

3. Serwer – 2 sztuki	
Nazwa składnika/parametru technicznego sprzętu	**Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu**
Procesor	Zainstalowane dwa procesory 10-rdzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 896 punktów w teście SPECint_rate_base2006 lub min. 104 punkty w teście SPECrate2017_int_base dostępnych na stronie www.spec.org dla dwóch procesorów. Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu wyniki w/w testów. Wyniki powinny zostać przedstawione w postaci wydruku z pliku PDF oryginalnie pobranego ze strony spec.org.
Pamięć operacyjna	min. 128 GB pamięci RAM DDR4 RDIMM 2667MT/s z korekcją błędów ECC, SDDC, memory mirror, memory sparing, lockstep. Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać min. do 1.5TB pamięci RAM.
Pamięć masowa	Zainstalowane 1x120GB SSD SATA oraz 3x1.2TB SAS 12Gb/s 10k. Możliwość instalacji do 8 dysków 2.5” dysków SATA, SAS, SSD hot-plug. Wbudowany napęd DVD-RW
Interfejs sieciowy	Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+. - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. Zainstalowana dodatkowo jedna karta czteroportowa 1GbE w standardzie Base-T, dwie dwuportowe karty 10GbE w standardzie Base-T oraz karta dwuportowa FC 16Gb/s.
Obudowa	Obudowa Rack o wysokości max. 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Sloty PCI Express	Minimum 6 slotów PCI-Express generacji 3 o prędkości x8, Min. 2 sloty PCI-Express generacji 3 o prędkości x16 pełnej długości i wysokości
Zasilanie i chłodzenie	Minimum 2szt., redundantne, typu hot-plug o mocy maksymalnie 800W Redundantne wentylatory
Kontroler dyskowy	Zainstalowany sprzętowy kontroler RAID zapewniający obsługę zabezpieczeń RAID na poziomie 0/1/10,5,50,6,60. Moduł nieulotnej pamięci cache minimum 2GB. Wsparcie dla dysków samoszyfujących. lub możliwość zastosowania innych mechanizmów pozwalających na szyfrowanie danych na dyskach, np. poprzez kontroler
Grafika	Zintegrowana z płytą główną umożliwiająca wyświetlanie obrazu w rozdzielczości min. 1920x1200
Dodatkowe interfejsy	min. 3 porty USB 2.0, 2 porty USB 3.0, 4 porty RJ45, 1 port VGA lub DP na przednim panelu obudowy, 1 port VGAna tylnympanelu obudowy, min. 1 port RS232. Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego.
Zarządzanie i obsługa techniczna	Panel diagnostyczny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o, pamięciach, wentylatorach, zasilaczach, temperaturze. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3) oraz autentykacje 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, Telnet, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wsparcie dla dynamic DNS • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232 • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności min. 8GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z • poziomu BIOS serwera.

Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO- 14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów, Microsoft Windows 2012R2 x64, 2016 x64 i 2019 x64.
System operacyjny	1. Licencja na serwerowy system operacyjny jest przypisana do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym. Licencja musi obsługiwać 30 użytkowników (CAL) 2. Możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym. 3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 4. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 5. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonychw mechanizmy Hyper-Threading. 7. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 8. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów 9. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji 10. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 11. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 12. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 13. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wrazz dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 14. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

4. Macierz dyskowa – 1 sztuka	
Nazwa składnika/parametru technicznego	**Minimalne wymagania w zakresie parametrów technicznych**
Obudowa	Do instalacji w standardowej szafie RACK 19”. Wysokość maksymalnie 2U wraz z kompletem szyn do montażu w szafie Rack z możliwością instalacji minimum 12 dysków 3.5” Hot Plug.
Kontrolery	Dwa kontrolery posiadające łącznie minimum osiem portów FC minimum 16 Gb/s wraz z 4 wkładkami SFP do podłączenia serwerów, pracujące w trybie active-active. Wymagane poziomy zabezpieczenia RAID: 1,5,6,10. Minimum 4GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inną pamięć nieulotną lub podtrzymywana bateryjnie przez min. 72h w razie awarii.
Dyski twarde	Zainstalowane dyski: 4 dyski o pojemności minimum 4TB NearLine SAS 7.2k Hot-Plug 3.5” każdy. Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 190 dysków, wydajnych dysków SAS, SSD, ekonomicznych dysków typu SATA (lub NearLine SAS), samoszyfrujących dysków SED dostępnych w ofercie producenta macierzy lub równoważne mechanizy pozwalające na szyfrowanie danych na dyskach, możliwość mieszania typów dysków w obrębie macierzy oraz półki.
Oprogramowanie	Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Możliwość rozbudowy o licencję umożliwiającą utworzenie minimum 500 LUN’ów oraz 30 kopii migawkowych na LUN. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 30 hostów bez konieczności zakupu dodatkowych licencji. Zarządzanie macierzą poprzez minimum oprogramowanie zarządzające lub przeglądarkę internetową. - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH - Możliwość oskryptowywania procesu wykrywania urządzeń - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - Szczegółowy opis wykrytych systemów oraz ich komponentów - Możliwość eksportu raportu do CSV, HTML, XLS - Grupowanie urządzeń w oparciu o kryteria użytkownika - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń - 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 - Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu - 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 sterowników i oprogramowania wewnętrznego

	- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta - 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 gwarancji, adresy IP kart sieciowych.
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. Możliwość przydzielenia większej przestrzeni dyskowej dla serwerów niż fizycznie dostępna (Thin Provisioning) Fizyczne zabezpieczenie dedykowane przez producenta uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Warunki gwarancji	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz wyprodukowana zgodnie z normą ISO 9001:2008 oraz 14001 Zgodność z systemami operacyjnymi: Microsoft® Windows®, VMware®, Microsoft Hyper-V®, Red Hat® oraz SUSE

5. Przełącznik Fibre Channel –1 sztuka	
Lp.	**Minimalne wymagania w zakresie parametrów technicznych**
1.	Przełącznik FC musi być wykonany w technologii FC 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2 Gb/s z funkcją autonegocjacji prędkości.
2.	Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 8 portów FC przełącznika.
3.	Przełącznik musi być dostarczony wraz z minimum 8 modułami SFP FC 8 Gb/s.
4.	Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.
5.	Przełącznik FC musi posiadać nadmiarowe wentylatory N+1.
6.	Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
7.	Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.
8.	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.
9.	Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.

10.	Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: ▪ Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric ▪ Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP ▪ Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP ▪ Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów ▪ Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, ▪ Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. ▪ Konta użytkowników definiowane w środowisku RADIUS lub LDAP ▪ Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS ▪ Obsługa SNMP v3
11.	Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
12.	Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.
13.	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC
14.	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
15.	Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
16.	Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
17.	Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns.
18.	Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN
19.	Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID.
20.	Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP).
21.	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
22.	Być objęty gwarancją na sprzęt przynajmniej na trzy lata. Gwarancja powinna być świadczona w trybie co najmniej 365x7x24, z czterogodzinnym czasem reakcji .
23.	Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.
24.	Szyny do montażu w szafie rack.

6. Stacjonarny zestaw komputerowy – 4 sztuk	
Nazwa podzespołu	**Minimalne wymagania parametry**
Typ	Komputer stacjonarny. Typu All in One, komputer wbudowany w monitor. W ofercie wymagane jest podanie modelu producenta komputera.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 11500 punktów. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php
Pamięć operacyjna RAM	min. 8GB (1x8GB) DDR4 2666MHz non-ECC możliwość rozbudowy do min. 32GB
Parametry pamięci masowej	min. 512GB SSD M.2 PCIe NVMe
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej
Matryca	antyodblaskowa matryca o przekątnej min. 21,5” o rozdzielczości FHD (1920x1080) przy częstotliwości odświeżania 60Hz, Jasność matrycy co najmniej 250 cd/m², Kąty widzenia pion/poziom min. 89/89 stopni.
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera z mikrofonem cyfrowym obsługującym poprawę mowy i redukcję szumów. Kamera wsparta o diodę LED informującą użytkownika o włączonej kamerze. Wbudowana w obudowę matrycy mechaniczna maskownica kamery.
Obudowa	Typu All-in-One zintegrowana z monitorem min. 21,5”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) lub kłódki (oczko w obudowie do założenia kłódki). Podstawa musi oferować użytkownikowi możliwość regulacji w zakresie: - przód/ tył – regulacja min. 35 stopni (-5 / +30) - wysokości – min 100mm - lewo/prawo – w zakresie min. 90 stopni (45 lewo / 45 prawo) Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi, nie dopuszcza się stosowania śrub motylkowych, radełkowych czy zwykłych wkrętów. Suma wymiarów samej obudowy (bez podstawy) nie może przekraczać 99cm, Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100x100. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, wpisanym na stałe w BIOS. Możliwość instalacji dodatkowego dysku twardego HDD lub SSD. Zasilacz wewnętrzny o mocy max. 155W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%. Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx. Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu. W przypadku, kiedy u producenta występuje kilka zasilaczy, które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy. Wydruki 80PLUS muszą być potwierdzone przez producenta oświadczeniem producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają normę 80PLUS na zaoferowanym poziomie.Obudowa musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.

Bezpieczeństwo	Wlutowany w płytę główną (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiekolwiek złącza wyprowadzone na płycie) dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot'owania, działający w przypadku: uszkodzenia dysku twardego z systemem operacyjnym komputera oraz odłączenia dysku twardego, umożliwiający na wykonanie diagnostyki następujących podzespołów: -test pamięci RAM -test dysku twardego - test procesora -test monitora -test magistrali PCI-e -test portów USB -test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: -PC: Producent, model -BIOS: Wersja -Procesor : Nazwa, taktowanie -Pamięć RAM : Ilość zainstalowanej pamięci RAM, numer -seryjny poszczególnych kości pamięci -Dysk twardy: model, numer seryjny, -Monitor: producent, model. Zasilacz wyposażony w swój własny system diagnostyczny niezależny od pozostałych komponentów oferowanego komputera umożliwiający sprawdzenie poprawnego funkcjonowania zasilacza bez narażania pozostałych składowych na ewentualne uszkodzenia (przepięcia itp.) Czujnik otwarcia obudowy musi zbierać logi i zapisywać je w BIOS
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera, Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym - MAC Adres karty sieciowej, - wersja Biosu - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - aktywnej karcie graficznej - napędach lub dyskach podłączonych do portów SATA/M.2 Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na

	poziomie systemu, administratora oraz dysku twardego (nie dotyczy dysków M.2 PCIe NVMe. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego. Możliwość włączenia/wyłączenia: - selektywnie (pojedynczego) portów SATA - karty sieciowej - karty audio - wbudowanej kamery - czytnika kart - Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość włączenia/wyłączenia funkcji umożliwiającej dokonywanie downgrade'u BIOS, Możliwość wyłączania portów USB w tym: ▪ wszystkich portów USB, ▪ tylko portów USB znajdujących się na bocznym panelu obudowy, ▪ tylko portów USB znajdujących się na tylnym panelu obudowy. ▪ pojedynczo portów USB Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego bootowania które umożliwia m.in.: ▪ uruchamianie systemu zainstalowanego na HDD ▪ uruchamianie systemu z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, CDRW-USB ▪ uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej ▪ uruchomienie graficznego systemu diagnostycznego wejścia do BIOS
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) Wykonawca wraz z dostawą dostarczy Zamawiającemu wszystkie certyfikaty, deklaracje itp. do zaoferowanego sprzętu np.deklaracje zgodności CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Certyfikat TCO, wymagany wpis na stronie: https://tcocertified.com/product-finder/ – Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu wydruk / informacje wyżej wymienioną. Komputer musi spełniać wymogi normy Energy Star 6.0. Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu certyfikat potwierdzony przez producenta lub wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov (wydruk ze strony internetowej)
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB (załączyć oświadczenie producenta)

Warunki gwarancji	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.
Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.
System Operacyjny	Zainstalowany system operacyjny Windows 10 Professional , klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub rozwiązanie równoważne.
Oprogramowanie biurowe	Licencja pakietu biurowego zgodnego ze specyfikacją, poz. 8 – Pakiet oprogramowania biurowego;
Złącza i porty	Wbudowane porty: • min. 1 x DP 1.2 • min. 5 portów USB wyprowadzonych na zewnątrz komputera w tym min. 3 porty USB 3.0; min. 2 porty USB 3.0 usytuowane na boku obudowy i 3 porty USB na tylnym panelu w tym min 1 port USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.) • min. 2 porty audio w kombinacji 1x in i 1x out lub port combo • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), • Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 1 złącze M.2 2280 PCI-Express x4 min. 1 złącze M.2 dedykowane dla karty WiFi • Klawiatura USB w układzie polski programisty • Czytnik kart multimedialnych czytający min. karty SD • Mysz optyczna USB z sześcioma klawiszami oraz rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x

7. Laptop – 3 sztuk	
Nazwa podzespołu	**Minimalne wymagania parametry**
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Przekątna ekranu	FHD (1920 x 1080) z podświetleniem LED i powłoką przeciwodblaskową,
Procesor	Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 5000 punktów Passmark CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php
Płyta główna	Zaprojektowana na zlecenie producenta i oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera.
Pamięć RAM	min. 8GB (1x8GB) DDR4 2400MHz możliwość rozbudowy do min 32GB, wymagane min. 2 sloty na pamięci w tym min. jeden wolny
Pamięć masowa	min. 480GB SSD
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej
Klawiatura	Klawiatura wyspowa z wydzielą z prawej strony klawiaturą numeryczną, z wbudowanym w klawiaturze podświetleniem z możliwością manualnej regulacji, (układ US -QWERTY),
Multimedia	dwukanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy 2x 2W. cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, o rozdzielczości min. 1280x720 trwale zainstalowana w obudowie matrycy.
Bateria i zasilanie	Co najmniej 45Wh. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.Zasilacz o mocy min. 65W.
Waga	Waga max 2,3kg z baterią
Obudowa	Zawiasy notebooka wykonane z metalu. Kąt otwarcia notebooka min. 140 stopni.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie oraz w BIOS systemu
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: ▪ wersji BIOS, ▪ nr seryjnego komputera, ▪ całkowitej wielkości zainstalowanej pamięci RAM, ▪ sposobu obsadzenia slotów DIMM z rozbiciem na bank A i B (w przypadku obsadzenia tylko jednej kości pamięci drugi bank wolne pole) ▪ typie zainstalowanego procesora ▪ zainstalowanym i podpiętym HDD (mini SSD) ▪ kontrolerze video ▪ MAC adresie wbudowanej w płytę główną karty sieciowej
Certyfikaty	Certyfikat ISO9001:2000 dla producenta sprzętu - Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu ww. certyfikat. Certyfikat ISO 14001 dla producenta sprzętu Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu. Deklaracja zgodności CE - Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki EnergyStar 6.0 – Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu przekaże certyfikat potwierdzony przez producenta lub wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-

	energystar.org lub http://www.energystar.gov (wydruk ze strony internetowej) podparty oświadczeniem producenta. Certyfikat TCO, wymagany wpis na stronie: https://tcocertified.com/product-finder/ – Wykonawca, którego oferta została najwyżej oceniona przedstawi Zamawiającemu
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 19dB.
Diagnostyka	Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot, działający w przypadku odłączenia dysku twardego, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności: ▪ - test CPU ▪ - test pamięci RAM ▪ - test dysku twardego ▪ - test matrycy LCD Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera. Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o natywnej rozdzielczości matrycy, numerze seryjnym, typie i pojemności dysku twardego, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czytnik linii papilarnych Złącze typu Security Lock
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub rozwiązanie równoważne.
Oprogramowanie biurowe	Licencja pakietu biurowego zgodnego ze specyfikacją, poz. 10 – Pakiet oprogramowania biurowego; pakiet preinstalowany przez producenta komputera
Porty i złącza	Wbudowane porty i złącza: ▪ 1x VGA lub załączany adaptere z USB-C na VGA ▪ min. 1x HDMI 1.4 ▪ min. 1x RJ-45 (10/100/1000) ▪ min. 2x USB 3.1, jeden port dosilony ▪ min. 1x USB 2.0 ▪ min. 1x USB Type-C ▪ czytnik kart multimedialnych wspierający karty SD lub microSD ▪ czytnik linii papilarnych ▪ współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo ▪ touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN AC z modułem Bluetooth min. 5.0
Warunki gwarancyjne	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu

	tego warunku.

8. Pakiet oprogramowania biurowego stanowiące zestaw wraz z zestawami komputerowymi oraz laptopami – 7 sztuk	
Nazwa składnika/parametru technicznego	**Minimalne wymagania w zakresie parametrów technicznych**
Licencja	Oprogramowanie winno być dostarczone z bezterminową licencją na użytkowanie
Interfejs użytkownika	a) pełna polska wersjajęzykowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim; b) pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim; c) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; d) możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0); e) pakiet aplikacji biurowych powinien prawidłowo współpracować z aplikacjami w modelu chmury obliczeniowej, w szczególności do pracy grupowej i synchronizacji danych
Zawartość pakietu	Pakiet zintegrowanych aplikacji biurowych musi zawierać: a) edytor tekstów, b) arkusz kalkulacyjny, c) narzędzie do przygotowywania i prowadzenia prezentacji, d) narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), e) zainstalowanie na jednym komputerze produktów pochodzących od różnych producentów nie jest uznane za ofertę zintegrowanego pakietu
Edytor tekstów	Edytor tekstów musi umożliwiać: a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b) wstawianie oraz formatowanie tabel, c) wstawianie oraz formatowanie obiektów graficznych, d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, f) automatyczne tworzenie spisów treści, g) formatowanie nagłówków i stopek stron, h) sprawdzanie pisowni w języku polskim, i) śledzenie zmian wprowadzonych przez użytkowników, j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k) określenie układu strony (pionowa/pozioma), l) wydruk dokumentów, m) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, n) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, o) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,

	p) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem, q) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa
Arkusz kalkulacyjny	Arkusz kalkulacyjny musi umożliwiać: a) tworzenie raportów tabelarycznych, b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, f) wyszukiwanie i zamianę danych, g) wykonywanie analiz danych przy użyciu formatowania warunkowego, h) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, j) formatowanie czasu, daty i wartości finansowych z polskim formatem, k) zapis wielu arkuszy kalkulacyjnych w jednym pliku, l) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
Narzędzie do przygotowywania i prowadzenia prezentacji	Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a) przygotowywanie prezentacji multimedialnych, które będą prezentowanie przy użyciu projektora multimedialnego, b) drukowanie w formacie umożliwiającym robienie notatek, c) zapisanie jako prezentacja tylko do odczytu, d) nagrywanie narracji i dołączanie jej do prezentacji, e) opatrywanie slajdów notatkami dla prezentera, f) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, g) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, h) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, i) możliwość tworzenia animacji obiektów i całych slajdów, j) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, pełna zgodność z formatami plików utworzonych za pomoc oprogramowania MS PowerPoint 2003, MS PowerPoint 2007i 2010,

Narzędzie do zarządzania informacją prywatną	Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, c) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, d) automatyczne grupowanie poczty o tym samym tytule, e) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, f) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, g) zarządzanie kalendarzem h) udostępnianie kalendarza innym użytkownikom, i) przeglądanie kalendarza innych użytkowników, j) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, k) zarządzanie listą zadań, l) zlecanie zadań innym użytkownikom, m) zarządzanie listą kontaktów, n) udostępnianie listy kontaktów innym użytkownikom, o) przeglądanie listy kontaktów innych użytkowników, k) możliwość przesyłania kontaktów innym użytkowników,

9. Skaner dokumentów ilość - 1 sztuki	
Nazwa składnika/parametru technicznego sprzętu	**Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu**
Typ skanera	Skaner płaski z ADF zintegrowane w jednej obudowie
Rodzaj czujnika skanowania obrazu	Kolorowe matryce CCD
Źródło światła	Biała matryca LED
Rozdzielczość optyczna	Min. 600 dpi
Prędkość skanowania (A4, tryb portretu)	Jednostronny: min. 60 str./min, dwustronny: min. 120 obr./min (min. 200 dpi / min. 300 dpi)
Maksymalny format skanowania	Skaner płaski min. 216 mm x297mm Podajnik ADF min. 216mm x 5580 mm
Dzienna przepustowość	Min 4 000 stron
Pojemność ADF	80 arkuszy (A4: 80 g/m²)
Połączenie	USB 3.0

10. Oprogramowanie antywirusowe stanowiące komplet do Zestawów komputerowych i laptopów – 7 sztuk	
Nazwa składnika/parametru technicznego	**Minimalne wymagania w zakresie parametrów technicznych**
Wsparcie dla systemów operacyjnych	• Microsoft Windows 10 Pro x86 / x64 • Microsoft Windows 8.1 Pro x86 / x64 • Microsoft Windows 8 Pro x86 / x64 • Microsoft Windows 7 Professional x86 / x64

Opis	• Polskojęzyczny interfejs konsoli zarządzającej i programu na stacjach roboczych.
	• Program powinien posiadać certyfikaty niezależnych laboratoriów.
	• Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
	• Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
	• Program ma możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury.
	• Kontrola sieci – kontrola dostępu do zasobów sieciowych w zależności od ich zawartości i lokalizacji:
	  ◦ Możliwość definiowania reguł filtrujących zawartość na wybranej stronie lub wszystkich stronach w zależności od kategorii zawartości: pornogafia, narkotyki, broń, gry, sieci społecznościowe, banery, itd.
	  ◦ Możliwość definiowania reguł blokujących bądź zezwalających na wyświetlanie określonej treści na wybranej stronie lub wszystkich stronach w zależności od kategorii danych: pliki wideo, audio, archiwa itd.
	• Monitor wykrywania luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.
	• Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX).
	• Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.

	• Wbudowany moduł skanujący protokoły POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego. • Skaner poczty powinien mieć możliwość zmiany nazwy lub usuwania określonych typów załączników. • Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki. • Wbudowany moduł skanujący ruch komunikatorów ICQ, MSN, AIM, Mail.Ru Agent oraz IRC. • Moduł zapory ogniowej: • Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów. • Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy. • Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. • Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie bądą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy. • Skanowanie w czasie rzeczywistym: • Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera. • Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np.modyfikacj rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania. • System antywirusowy posiada możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
Aktualizacja baz danych sygnatur zagrożeń	• Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
Konsola zdalnego zarządzania	• System zdalnego zarządzania powinien posiadać polskojęzyczny interfejs konsoli programu. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych.

1. **Zamawiający wymaga:**

   1) Na dostarczone serwery, macierz oraz zestawy komputerowe Wykonawca zapewni co najmniej 3 letni okres gwarancyjny z czasem reakcji 8 godziny, naprawa w miejscu instalacji sprzętu. Wykonawca przedstawi przed podpisaniem umowy do akceptacji Zamawiającemu, dokument wystawiony przez producenta oferowanych komputerów (lub jego autoryzowanego przedstawiciela), potwierdzający, że oferowane serwery, będą objęte gwarancją na zasadach określonych w § 12 ust. 1 wzoru umowy,

   2) Wykonawca w formularzu ofertowym winien zaznaczyć, które elementy zamówienia będzie powierzał podwykonawcy,

   3) na każdym urządzeniu wchodzącym w przedmiot zamówienia należy zamieścić w widocznym miejscu trwałą nie ścieralną informację wg wzoru:

Wymiary informacji: 12 cm / 6 cm lub dostosowane do wielkości rządzenia.Zamawiający wymaga, aby element promocyjny nie odlepiał się po jakimś czasie lub na skutek wykonywania czynności sprzątających typu wytarcie kurzu.

4) dostarczony sprzęt będzie wolny od wad fizycznych i nie noszący oznak użytkowania. Sprzęt nie może stanowić roszczeń osób trzecich,

5) zamieszczona powyżej specyfikacja sprzętowa ma wyłącznie charakter przykładowy i dotyczy wymagań minimalnych. Dopuszcza się możliwość zastosowania dowolnych typów i modeli sprzętu pod warunkiem spełniania wyżej określonych parametrów,

6) w przypadku określenia danego elementu nazwą producenta należy automatycznie stosować pojęcie „lub równoważne". Równoważność dla poszczególnych elementów (części) jest opisana
w poszczególnych tabelach. Równoważność stanowią:

7) w przypadku systemu operacyjnego dla zestawów Komputerowych oraz Laptopów równoważność jest opisana w pkt. 3,

8) w przypadku pakietu biurowego dla zestawów Komputerowych oraz Laptopów równoważność jest opisana w pkt. 4,

9) w przypadku zaoferowania elementu (części) równoważnego Wykonawca musi podać parametry oferowanego elementu, aby Zamawiający mógł stwierdzić jego równoważność z wymogami SIWZ. Jeżeli równoważny element dotyczy np. rodzaju procesora, który winien posiadać określoną ilość punktów wskazanych w SIWZ testach, a dla którego to procesora oferowanego przez Wykonawcę nie były prowadzone określone w SIWZ testy rankingowe, Wykonawca musi dołączyć do oferty scenariusz oraz wyniki przeprowadzonych na własny koszt testów oferowanego procesora,

10) ilekroć w opisie przedmiotu zamówienia występują nazwy konkretnych elementów, wyrobów lub określenia (parametry techniczne) sugerujące wyroby, elementy konkretnych firm, producentów Wykonawca winien uznać, iż podano produkty tylko i wyłącznie przykładowe, a Zamawiający dopuszcza możliwość zastosowania elementów, wyrobów, materiałów równoważnych o właściwościach, parametrach technicznych nie gorszych niż przyjęto w szczegółowym opisie przedmiotu zamówienia.

2. <u>Informacje szczegółowe:</u>

1) Prace należy realizować w dni robocze w godzinach od 8.00-15.00.

2) Wszystkie prace należy wykonywać w obecności pracownika Zamawiającego.

3) Zakres prac w Urzędzie:

a) Serwer, macierz, przełączniki:

- montaż serwerów oraz pozostałego sprzętu i oprogramowania w serwerowni w budynku Urzędu.
- instalacja, aktualizacja i konfiguracja serwerów w szczegółowym ustaleniu z Zamawiającym i według potrzeb przez niego określonych. Przekazanie licencji;
- oklejenie sprzętu naklejkami promocyjnymi. Wykonanie zdjęć z realizacji zadania,
- przeprowadzenie testów integracyjnych zamontowanego sprzętu;

- przekazanie Zamawiającemu dokumentacji zdjęciowej, licencji, dokumentacji technicznej, nośników, okablowania zasilającego oraz sieciowego;
- włączenie, skonfigurowanie wskazanego serwera do urządzenia brzegowego;

b) zestawy komputerowe oraz laptopy:

– dostarczenie sprzętu, wniesienie;
– rozpakowanie sprzętu;
– ułożenie i podłączenie sprzętu we wskazanym miejscu;
– zamaskowanie (ułożenie) okablowania w sposób estetyczny np. w maskownicach jeśli są dostępne;
– instalacja, konfiguracja do potrzeb użytkownika sprzętu komputerowego;
– pobranie aktualizacji systemowych i ich instalacja i konfiguracja;
– wykonanie testów drukowania i połączenia internetowego;
– założenie konta użytkownika i hasła logowania do systemu w uzgodnieniu z użytkownikiem. Hasło i login należy do każdej stacji należy przekazać Zamawiającemu;
– przekazanie kompletu nośników okablowania zasilającego oraz sieciowego, licencji;
– oklejenie sprzętu nalepkami promocyjnymi;
– wykonanie zdjęć z zakończonych prac obrazujący sprzęt komputerowy. Na zdjęciach muszą również być widoczne naklejki promocyjne;
– podpisanie protokołu z realizacji instalacji.

c) skanery:

– dostarczenie sprzętu, wniesienie;
– rozpakowanie sprzętu;
– ułożenie i podłączenie sprzętu we wskazanym miejscu;
– zamaskowanie (ułożenie) okablowania w sposób estetyczny np. w maskownicach jeśli sa dostępne;
– wykonanie testów drukowania i połączenia internetowego;
– oklejenie sprzętu nalepkami promocyjnymi;
– wykonanie zdjęć z zakończonych prac obrazujący sprzęt komputerowy. Na zdjęciach muszą również być widoczne naklejki promocyjne;
– podpisanie protokołu z realizacji instalacji.
– instalacja, konfiguracja do potrzeb użytkownika

4) W ramach instalacji Wykonawca połączy urządzenia przy wykorzystaniu niezbędnego okablowania dostarczonego w ramach zamówienia. Minimalny zakres usług dla infrastruktury serwerowej:

– montaż w szafie RACK;
– podpięcie wszystkich niezbędnych kabli;
– weryfikacja i aktualizacja BIOS;
– instalacja systemu operacyjnego wraz z wymaganymi aktualizacjami;
– uruchomienie i konfiguracja domeny Active Directory
– Przeprowadzenie instruktażu administratora

5) Wykonawca ustali z Zamawiającym harmonogram prac rozlokowania nowych zestawów.

6) Zamawiający zastrzega sobie prawo do weryfikacji oferowanych równoważnych elementów (części) oraz oprogramowania czy spełniają opisy równoważności.

7) W przypadku, kiedy oferowane równoważne elementy lub oprogramowanie nie będą spełniać stawianych warunków oferta zostanie odrzucona jako nie spełniająca warunków SIWZ..

8) Komisja Przetargowa sporządzi stosowany protokół z przeprowadzonej procedury weryfikującej równoważność zaoferowanych elementów (części) i oprogramowania.

c) <u>Opis Równoważności oprogramowania system operacyjny</u>

1) możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek,

2) możliwość dokonywania uaktualnień sterowników urządzeń przez Internet -witrynę producenta systemu,

3) darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) wymagane podanie nazwy strony serwera WWW.

4) internetowa aktualizacja zapewniona w języku polskim,

5) wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6,

6) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

7) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),

8) funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,

9) interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta,

10) możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu,

11) zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,

12) zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,

13) zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych,

14) system operacyjny posiada podstawowe funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika,

15) system operacyjny posiada wbudowaną funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika,

16) zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,

17) wbudowany system pomocy w języku polskim,

18) system operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),

19) możliwość zarządzania stacją roboczą poprzez polityki -przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
20) wdrażanie IPSEC oparte na politykach -wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
21) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
22) wsparcie dla logowania przy pomocy smartcard,
23) rozbudowane polityki bezpieczeństwa -polityki dla systemu operacyjnego i dla wskazanych aplikacji,
24) system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,
25) wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 -możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
26) wsparcie dla JScript i VBScript -możliwość uruchamiania interpretera poleceń,
27) zdalna pomoc i współdzielenie aplikacji -możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; Graficzne środowisko instalacji konfiguracji,
28) rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz zaplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
29) rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
30) graficzne środowisko instalacji i konfiguracji,
31) transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
32) zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
33) oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
34) możliwość przywracania plików systemowych,
35) system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
36) możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (przy użyciu numerów identyfikacyjnych sprzętu),
37) możliwość podłączenia oraz pełnej integracji z domeną Windows Server 2012R2,
38) obsługa wszystkich zasad grupy Active Directory bez instalacji i konfiguracji dodatkowego oprogramowania.

d) Opis Równoważności oprogramowania pakiet biurowy

1) oprogramowanie winno być dostarczone z bezterminową licencją na użytkowanie,
2) wymagania odnośnie interfejsu użytkownika:
   i. pełna polska wersja językowa interfejsu użytkownika,
   ii. prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych,

3) pakiet zintegrowanych aplikacji biurowych musi zawierać:
   i. edytor tekstów,
   ii. arkusz kalkulacyjny,
   iii. narzędzie do przygotowywania i prowadzenia prezentacji,
   iv. narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
4) edytor tekstów musi umożliwiać:
   a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
   b) wstawianie oraz formatowanie tabel,
   c) wstawianie oraz formatowanie obiektów graficznych,
   d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
   e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
   f) automatyczne tworzenie spisów treści,
   g) formatowanie nagłówków i stopek stron,
   h) sprawdzanie pisowni w języku polskim,
   i) śledzenie zmian wprowadzonych przez użytkowników,
   j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
   k) określenie układu strony (pionowa/pozioma),
   l) wydruk dokumentów,
   m) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego,
   n) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,
   o) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
   p) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem,
   q) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego
   w Polsce prawa.
5) arkusz kalkulacyjny musi umożliwiać:
   i. tworzenie raportów tabelarycznych,
   ii. tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
   iii. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje

na danych finansowych i na miarach czasu,

iv. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),

v. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,

vi. wyszukiwanie i zamianę danych,

vii. wykonywanie analiz danych przy użyciu formatowania warunkowego,

viii. nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,

ix. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,

x. formatowanie czasu, daty i wartości finansowych z polskim formatem,

xi. zapis wielu arkuszy kalkulacyjnych w jednym pliku,

xii. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,

xiii. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

6) narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

i. przygotowywanie prezentacji multimedialnych, które będą prezentowanie przy użyciu projektora multimedialnego,

ii. drukowanie w formacie umożliwiającym robienie notatek,

iii. zapisanie jako prezentacja tylko do odczytu,

iv. nagrywanie narracji i dołączanie jej do prezentacji,

v. opatrywanie slajdów notatkami dla prezentera,

vi. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,

vii. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,

viii. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,

ix. możliwość tworzenia animacji obiektów i całych slajdów,

x. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,

xi. pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

7) narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

i. pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,

ii. filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,

iii. tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,

iv. automatyczne grupowanie poczty o tym samym tytule,

v. tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,

vi. oflagowanie poczty elektronicznej z określeniem terminu przypomnienia,

vii. zarządzanie kalendarzem

viii. udostępnianie kalendarza innym użytkownikom,

ix. przeglądanie kalendarza innych użytkowników,

x. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,

xi. zarządzanie listą zadań,

xii. zlecanie zadań innym użytkownikom,

xiii. zarządzanie listą kontaktów,

xiv. udostępnianie listy kontaktów innym użytkownikom,

xv. przeglądanie listy kontaktów innych użytkowników,

xvi. możliwość przesyłania kontaktów innym użytkowników.