Załącznik nr 6 do SIWZ

I. Serwer plików NAS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	**Osiagający wynik 5000 pkt w teście PassMark CPU Mark – załączyć do oferty wydruk ze strony www.cpubenchmark.net lub www.passmark.com**
Pamięć	4 GB z mozliwościa rozbudowy do 32 GB;
Kieszenie na dyski	8 z możliwością rozszerzenia do 36, w tym 2 x NVMe;
Obsługiwane dyski	2,5 i 3,5 calaSATA HDD, 2,5 cala SATA SSD, M.2 NVMe SSD, hot swap;
Porty	4 z 1 GbE z obsługą funkcji Link Aggregation; 4 x USB 3.2; 2 x eSATA;
Wspierane systemy plików	Btrfs, EXT4;
Obudowa	Tower
Głośność	Maksymalnie 25 dB;
Zasilacz	250W;
Zużycie energii	Maksymalnie 60W;
System operacyjny	1. Rozmiar wolumenu – 100 TB; 2. Liczba wolumenów wewnętrznych - 64; 3. Pamięć podręczna odczytu/zapisu na dyskach SSD 4. SSD TRIM; 5. Obsługa macierzy RAID – 0,1,5,6,10; 6. Możliwość powiększenia wolumenu za pomocą większych dysków twardych; 7. Mozliwość powiększenia wolumenu przez dodanie dysków twardych; 8. Obsługa dysków hot spare; 9. Obsługa FTP, FTP przez SSL/TLS i SFTP; 10. Integracja listy kontroli dostępu ACL 11. Uwierzytelnienie NFS Kerberos; 12. Liczba lokalnych kont użytkowników -2048; 13. Liczba lokalnych grup – 256; 14. Liczba folderów udostenionych – 512; 15. Liczba zadań synchr. folderów udostępnionych – 16; 16. Liczba zdarzeń Syslog na sekundę – 1000; 17. Wparcie dla wirualizatorów – VMware, Hyoer V, Citrix; 18. Obsługiwane protokoły sieciowe - SMB1, SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV; 19. Obsługa protokołu SSH podczas przesyłania plików; 20. Synchronizacja folderów współdzielonych; 21. Kopia zapasowa jednostek LUN 22. Zarządzanie pamięcią masową i monitorowanie użycia pamięci masowej serwera; 23. Obsługa migawek i tworzenia zadań replikacji dla folderów współdzielonych i jednostek LUN 24. Przeglądanie migawek tylko do odczytu 25. Menedżer plików do przeglądania i zarządzania folderami i plikami przechowywanymi na serwerze;

<table>
<tr><td></td><td>26. Bezpieczne udostępnianie plików
27. Dostęp i zarządzanie z komputerów osobistych, tabletów i telefonów komórkowych;
28. Montowanie dysków wirtualnych, folderów zdalnych i pamięci masowej w chmurze publicznej;
29. Odzyskiwanie lub pobieranie usuniętych plików z kosza
30. Wyświetlanie i dostosowywanie uprawnień ACL do plików i folderów;
31. Obsługa edytora ACL
32. Dostosowywanie atrybutów folderów współdzielonych do wyświetlania;
33. Kompresowanie lub wyodrębnianie zarchiwizowanych plików i folderów;
34. Montowanie dysków wirtualnych w celu uzyskania dostępu do zawartości plików obrazów dysków (.iso
35. Montowanie folderów zdalnych ze zdalnych serwerów obsługujących protokoły SMB1/SMB2/SMB3/NFS
36. Łączenie ze zdalnymi usługami chmury publicznej i serwerami plików;
37. Obsługiwane protokoły: FTP, SFTP, WebDAV, WebDAV HTTPS
38. Centralne zarządzanie za pośrednictwem menedżera łączy udostępnionych;
39. Logi transferu plików i działań użytkownika z możliwościa eksportu;</td></tr>
<tr><td>Warunki gwarancji</td><td>3 lata;</td></tr>
<tr><td>Wymagania dodatkowe</td><td>Zestaw montażowy w szafie rack, wentylator obudowy, kontrolki LED z regulacja jasności, możliwość zaplanowania włączenia i wyłączenia, funkcja WoL, ;</td></tr>
<tr><td>Dysk twardy TYP 1- 4 szt.</td><td>
<table>
<tr><th>Nazwa komponentu</th><th>Wymagane minimalne parametry techniczne</th></tr>
<tr><td>Poiojemność</td><td>10 TB;</td></tr>
<tr><td>Prędkośc obrotowa</td><td>7200 ob./min.;</td></tr>
<tr><td>Interfejs</td><td>SATA 6 Gb/s;</td></tr>
<tr><td>Cache</td><td>256 MB;</td></tr>
<tr><td>MTBF</td><td>1 mln. godzin;</td></tr>
<tr><td>Zuzycie energii podczas pracy</td><td>Maksymalnie 12W;</td></tr>
<tr><td>Glosność podczas pracy</td><td>Maksymalnie 35 dBA;</td></tr>
<tr><td>Gwarancja</td><td>3 lata;</td></tr>
</table>
</td></tr>
<tr><td>Dysk twardy TYP 2- 1 szt.</td><td>
<table>
<tr><th>Nazwa komponentu</th><th>Wymagane minimalne parametry techniczne</th></tr>
<tr><td>Poiojemność</td><td>800 GB;</td></tr>
<tr><td>Obudowa</td><td>M.2;</td></tr>
<tr><td>Interfejs</td><td>NVMe PCIe 3,0 x 4</td></tr>
<tr><td>MTBF</td><td>1,8 mln. godzin;</td></tr>
<tr><td>Zuzycie energii podczas pracy</td><td>Maksymalnie 4W;</td></tr>
<tr><td>Gwarancja</td><td>5 lat</td></tr>
</table>
</td></tr>
</table>

II. Urządzenia Sieciowe + osprzęt

Przełącznik zarzadzalny szt.4	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Model	Przełącznik dostępowy warstwy 2 **SZT.4**
Ilość portów	48x 10/100/1000Base-T RJ45 + 4x 1/10GBase-X SFP+
Przepustowość	130 Mp/s
Bufor pakietów	1,5 MB
Ramki jumbo	10 000;
Tablica MAC	15 000, dopuszcza się tablicę współdzieloną dla funkcji dla unicast i multicast w proporcji 1:1;
Tablica Multicast MAC	1 000;
Tablica ACL	380;
Ilość Interfejsów VLAN (IP)	512
Taktowanie procesora	800 MHz
Pamięć FLASH	32 MB
Pamięć RAM	256 MB
Funkcje podwyższonej dostępności	IEEE 802.1D STP/802.1w RSTP/802.1s MSTP, IEEE 802.3ad LACP, Virtual Cable Testing, DDM, LLDP / LLDP-MED, Loop guard, ERPS (ITU-T G.8032)
Kontrola ruchu	802.1Q VLANs, oparty na portach I protokołach VLAN, podsieć IP oparta na VLAN, Voice VLAN, Mac VLAN, load balance, GVRP, elastyczny QinQ
Bezpieczeństwo	Filtrowanie adresów MAC na warstwie 2, tunel BPDU, autoryzacja I autentykacja logowania przez RADIUS, TACACS+, SSH v1/v2, DHCP/DHCPv6 snooping, IP/IPv6, zabezpieczenie portow, IEEE 802.1x opart na portach i MAC adresach;
QoS	Kolejkowanie I prioretyzowanie per port,, zaufany COS/TOS/IP, kontrola przepływu, ważone wczesne wykrywanie;
L2/L3 Multicast	Multicast VLAN, IGMP v1,v2, v3, zapytanie IGMP, IGMP Snooping (v1,v2,v3), IPv6 MLD v1/v2 Snooping
Warstwa 3 IPv6	Podwójny protokół stakowania IPv4/IPv6 Dual Protocol Stack, adresacja IPv6;
Zarządzanie	Port konsolowy RS-232 (RJ45), web GUI, Telnet, SNMP v1/v2c/v3, TFTP/FTP, kopia zapasowa konfiguracji oraz jej przywracanie, wielopoziomowy CLI,, DHCP Client/Relay/Server, DHCP per VLAN, DHCPv6 Relay/Server, SNTP / NTP, sFlow, Stack, port mirroring, RSPAN, IEEE 802.3ah EFM, IEEE 802.1ag CFM
MIB	Oparty o TCP/IP, SNMPv2c/v3, bridge, rozszerzenie bridge'a, ethernet, grupy RMON 1,2,3,9, zdalne zarządzanie, SMIv2
Pobór mocy	Maksymalnie 50W;
Warunki gwarancji	3 lata;

Wkładki Światłowodowe	
Wkładki SFP+- TYP 1 - 4 szt.	Dedykowany do linków optycznych o prędkości 10Gbps. Przystosowany sieci światłowodowej jednomodowej 9/125nm Rodzaj modułu – SFP+ Tryb transmisji WDM; Rodzaj złącza – LC/PC; Zasieg – 20 km; Długość RX/TX – 1330/1270 nm; Czułość – -14 dBm; Pobór mocy – maksymalnie 4W;
Wkładki SFP+- TYP 2 - 4 szt.	Dedykowany do linków optycznych o prędkości 10Gbps. Przystosowany sieci światłowodowej jednomodowej 9/125nm Rodzaj modułu – SFP+ Tryb transmisji WDM; Rodzaj złącza – LC/PC; Zasieg – 20 km; Długość RX/TX – 1270/1330 nm; Czułość – -14 dBm; Pobór mocy – maksymalnie 4W;

III. Zestaw komputerowy (komputer, monitor, mysz, klawiatura)-20 szt.

Komputer stacjonarny – 20 szt.	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Typ	Komputer stacjonarny.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Wydajność	**Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall rating, wynik 1400 pkt. Wydruk z oprogramowania testującego załączyć do oferty.** Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).

	Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć RAM	16GB DDR4 3200MHz. Możliwość rozbudowy do 128GB. Cztery sloty w tym jeden slot wolny.
Pamięć masowa	SSD 512GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5" lub 3.5".
Grafika	**Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Creativity wynik 1300 pkt. Wydruk z oprogramowania testującego załączyć do oferty.** Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Wyposażenie multimedialne	Karta dźwiękowa czterokanałowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo; Na tylnym panelu port audio line out.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5" lub 1 x dysku 2.5" wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25"; Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 80 cm; Na panelu przednim zamontowany filtr powietrza chroniący wnętrze przed kurzem, pyłem itp. Filtr demontowany bez użycia narzędzi. Zasilacz o mocy 300W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności 89% przy obciążeniu zasilacza na poziomie 100%, Musi pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Musi umożliwiać zastosowanie zabezpieczenia w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).

	Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. Sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System musi być usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. System diagnostyczny nie może wykorzystywać wolnych slotów na płycie głównej, wnęk zewnętrznych w specyfikacji oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	TPM zintegrowany z płyta główną.
BIOS	Zgodny ze specyfikacją UEFI; Musi zawierać nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego i bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: 1. Wersji BIOS; 2. Nr seryjnym komputera; 3. Ilości zainstalowanej pamięci RAM; 4. Prędkości zainstalowanych pamięci RAM; 5. Technologii pamięci; 6. Sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki; 7. Typie zainstalowanego procesora, ilości rdzeni, prędkości; 8. Pojemności dysku; 9. Wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA; 10. MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio; Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie; Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń; Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednocześnie zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA; Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.

	Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Funkcja włączająca przypomnienie o konieczności oczyszczenia lub zastąpienia filtra powietrza;i BIOS musi posiadać menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS i upgrade BIOS;
Wirtualizacja	Sprzętowe wsparcie wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu; Możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu;
Certyfikaty i standardy	Urządzenia muszą być wyprodukowane szgodnie z normą **PN-EN ISO 50 001 – certyfikat załączyć do oferty;**
Wbudowane porty	1x HDMI 1.4, 1x VGA, 2x DisplayPort, port audio combo na przednim panelu panelu, 1 x RJ-45, czytnik kart pamięci SD. 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: - Panel przedni: 5x USB 3.2, w tym 1x USB-C - Panel tylny: 3 x USB; Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych; Porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL; Płyta główna wyposażona w: 2x PCIe x16 Gen.3, 1x PCIe x1, 1x PCI 4x DIMM z obsługą do 128 GB DDR4 RAM, 2x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Wbudowana nagrywarka DVD +/-RW
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	3-letnia gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać **ISO 27001** na świadczenie usług serwisowych
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

	b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);

	28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umozliwiajacy pracę w domenie;
Oprogramowanie zabezpieczające	1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny; 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci 7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu

	komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; 27.Konsola zarządzająca musi umożliwiać co najmniej: a) przechowywanie danych w bazie typu SQL; b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; d) centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. e) raportowanie, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych

	zainstalowanych w różnych lokalizacjach; 29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 31. Musi posiadać dostęp do konsoli z dowolnego miejsca; 32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych; 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 36. Konsola systemu musi umożliwiać, co najmniej: a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD c) regulowanie połączeń WiFi i Bluetooth d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeniu g) tymczasowe dodania dostępu do urządzenia przez administratora h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używanie tylko zaufanych urządzeń sieciowych; 37. Wirtualna klawiatury 38. Możliwość blokowania każdej aplikacji 39. Możliwość zablokowania aplikacji w oparciu o kategorie 40. Możliwość dodania własnych aplikacji do listy zablokowanych 41. Dodawanie aplikacji w formie portable 42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 45. Możliwość zablokowania funkcji Printscreen 46. Monitorowania przesyłu danych między aplikacjami; 47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 51. Ochrona zawartości schowka systemu

	52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 55. Możliwość tworzenia profilu DLP dla każdej polityki 56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 57. Ochrona przez wyciekiem plików poprzez programy typu p2p 58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 59. Monitorowanie określonych rodzajów plików. 60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 61. Możliwość śledzenia zmian we wszystkich plikach 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 68. Musi posiadać możliwość eksportu danych użytkownika 69. Musi umożliwiać import listy urządzeń z pliku CSV 70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; 73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 76. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: 78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 79. Portal musi być dostępny w postaci usługi hostowanej; 80. Skanowanie podatności za pomocą nodów skanujących 81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 82. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów

	b) zablokowanie możliwości zmiany widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV; 84. **B**ackup i przywracanie danych; 85. Deduplikacja danych na źródle, 86. Backup przyrostowy i różnicowy, 87. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 88. Backup danych lokalnych – plikowy oraz poczty; 89. Backup otwartych plików; 90. Filtr plików oraz folderów; 91. Domyślne wykluczenia zbędnych plików; 92. Przywracanie danych do wskazanej lokalizacji, 93. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora; 94. Wyszukiwanie plików w repozytorium użytkownika; 95. Automatyczne logowanie; 96. Zapamiętywanie danych logowania; 97. Automatyczne uruchamianie programu przy starcie systemu; 98. Ustawianie priorytetu dla procesu backupu; 99. Zmiana klucza szyfrującego; 100. Ustawienia przepustowości/zajętości pasm;, 101. Konfiguracja wydajności procesu backup; 102. Zastępowanie nazwy pliku GUID-em; 103. Szyfrowanie danych algorytmem AES 256 CBC po stronie komputera użytkownika, 104. Kompresja danych; 105. Transmisja po bezpiecznym protokole TLS; 106. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji; 107. Obliczanie sumy kontrolnej; 108. Kopie zapasowe musza być przechowywane w data center; 109. Licencje przypisywane do urządzenia z przestrzenią w chmurze 50 GB. 110. Licencja obowiązuje minimum przez okres gwarancji laptopa. 111. Wsparcie techniczne musi być świadczone w języku polskim; 112. Oprogramowanie zarządzające producenta komputera, umożliwiające: - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade system - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość sprawdzenia przed instalacją każdego sterownika, aplikacji, BIOS'u bezpośrednio na stronie producenta oraz uzyskanie informacji o: • poprawkach i usprawnieniach dotyczących aktualizacji • dacie wydania ostatniej aktualizacji • priorytecie aktualizacji • zgodności z systemami operacyjnymi • jakiego komponentu sprzętu dotyczy aktualizacja • wszystkich poprzednich aktualizacjach

	• najnowszych aktualizacji z podziałem na krytyczne, rekomendowane i opcjonalne 113. Możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku przy instalacji sterownika, aplikacji która tego wymaga.

Monitor – 20 szt.	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Rozmiar (klasa)	21 cali;
Typ panelu	IPS lub VA, matowy;
Format obrazu	16:9
Rozdzielczość	1920 x 1080
Czas reakcji matrycy	Maksymalnie 5 ms.
Jasność	250 cd/m^2
Kontrast	3000:1
Plamka	Maksymalnie 0.25 mm.;
Głośniki wbudowane	2 x 1W;
Regulacja wysokości	0-12 cm;
Pivot	90 stopni;
Pochylenie	-od -5 do 20 stopni;
Katy widzenia	178 stopni;
Złącza	1 x VGA, 1 x HDMI, 1 x DisplayPort, 2 x USB, wyjscie sluchawkowe;
Typowe zużycie energii	Maksymalnie 20W;
Warunki gwarancji	3 lata;
Wymagania dodatkowe	Kompatybilmość z Kensington Lock, zgodność ze standardem VESA, kabel HDMI, USB, **certyfikat TCO 8 – załączyć do oferty;**

IV. Oprogramowanie biurowe – 25 szt.

Zainstalowane na komputerach oprogramowanie biurowe- kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika;
   b) Prostota i intuicyjność obsługi, pozwalająca na prace osobom nieposiadającym umiejętności technicznych;
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,

b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
c) umożliwia wykorzystanie schematów XML
d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)

3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
4. Zamawiający wymaga licencji przeznaczonych wyłącznie dla jednostek edukacyjnych;
5. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
6. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
   d) Narzędzie do zarzadzania informacja prywata (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
8. Edytor tekstu musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługa 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 edycje 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 i z narzędzia do zarzadzania informacją prywatną
   n) Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 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 udostepniającego 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 umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
   r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i

pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

9. Arkusz kalkulacyjny musi umożliwiać:
   a) Tworzenie raportów tabelarycznych
   b) Tworzenie wykresów liniowych (wraz linia 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) Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych
   f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g) Wyszukiwanie i zamianę danych
   h) Wykonywanie analiz danych przy użyciu formatowania warunkowego
   i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
   k) Formatowanie czasu, daty i wartości finansowych z polskim formatem
   l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   m) Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
   n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
   a) Prezentowanie przy użyciu projektora multimedialnego
   b) Drukowanie w formacie umożliwiającym robienie notatek
   c) Zapisanie w postaci tylko do odczytu.
   d) Nagrywanie narracji dołączanej 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) Tworzenie 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
   k) Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
11. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, 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 elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy

f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g) Zarzadzanie 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) Zarzadzanie lista zadań
l) Zlecanie zadań innym użytkownikom
m) Zarzadzanie listą kontaktów
n) Udostępnianie listy kontaktów innym użytkownikom
o) Przeglądanie listy kontaktów innych użytkowników
a) Możliwość przesyłania kontaktów innym użytkowników

12. Licencja wieczysta, niewygasając. Ni dopuszcza się licencji subskrypcyjnej.

V. Laptop – 5 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej
Ekran	15.6" LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową; Klapa komputera otwierana do 180 stopni.
Wydajność komputera	Oferowany komputer przenośny musi osiągać w teście wydajności : **SYSMARK 25 – wynik 1250 – test z przeprowadzonej konfiguracji załączyć do oferty.** Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć RAM	8GB DDR4 z możliwością rozszerzenia do 32GB;
Dysk twardy	256 GB SSD Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.: - systemu operacyjnego - oprogramowania antywirusowego Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania. Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5.

Karta graficzna	Grafika musi umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5;
Karta dźwiękowa	Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony
Wbudowane połączenia i karty sieciowe	Karta sieciowa LAN 10/100/1000 LAN WLAN 802.11 ax wraz z Bluetooth 5.1
Porty/złącza (wbudowane)	1x Złącze RJ-45 1x czytnik kart pamięci SD 1x USB Thunderbolt 4 3x USB 3.2 1x VGA 1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo) 1x HDMI ze wsparciem HDCP 1x zasilanie DC-in
Klawiatura	Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy).
Urządzenie wskazujące	Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka. Czytnik linii papilarnych
Kamera	Wbudowana, o parametrach: HD 1280x720, 720p HD audio/video nagrywanie. Wbudowane dwa kierunkowe mikrofony. Mechaniczna przesłona kamery.
Bateria	Litowo-jonowa 45Whr; Czas pracy - 6h według wyników testów BAPCO MobileMark 25 – test załączyć do oferty;
Zasilacz	Zewnętrzny, o mocy maksymalnie 90W.
Obudowa waga i wymiary	Waga - maksymalnie 1,8kg,; Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium. Obudowa musi spełniać standard MIL-STD 810G;
Bezpieczeństwo	- Zabezpieczenie BIOS i dysku twardego hasłem użytkownika. - Złącze typu Kensington Lock. - TPM 2.0
Certyfikaty	Serwer musi być wyprodukowany zgodnie z **normą ISO-9001:2015 oraz ISO-45001 - załaczyć do oferty certyfikaty;** Standard MIL-STD-810G - potwierdzony w oficjalnych dokumentach producenta lub załączony wynik z przeprowadzonych testów;
Warunki gwarancji	Gwarancja producenta komputera - 36 miesięcy Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera. Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO 27001 Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych.
Wsparcie techniczne producenta	1. Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu; 2. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera;

	3. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane;
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup);

	24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: d) Login i hasło, e) Karty inteligentne i certyfikaty (smartcard), f) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umozliwiajacy pracę w domenie;
Oprogramowanie użytkowe	1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny; 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu,

	6. Automatyczne odłączanie zainfekowanej końcówki od sieci 7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portó 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware 27. Konsola zarządzająca musi umożliwiać co najmniej: a) przechowywanie danych w bazie typu SQL; b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; d) centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet.

	e) raportowanie, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych zainstalowanych w różnych lokalizacjach; 29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 31. Musi posiadać dostęp do konsoli z dowolnego miejsca; 32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych; 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 36. Konsola systemu musi umożliwiać, co najmniej: a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD c) regulowanie połączeń WiFi i Bluetooth d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeniu g) tymczasowe dodania dostępu do urządzenia przez administratora h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używanie tylko zaufanych urządzeń sieciowych; 37. Wirtualna klawiatury 38. Możliwość blokowania każdej aplikacji 39. Możliwość zablokowania aplikacji w oparciu o kategorie 40. Możliwość dodania własnych aplikacji do listy zablokowanych 41. Dodawanie aplikacji w formie portable 42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 45. Możliwość zablokowania funkcji Printscreen 46. Monitorowania przesyłu danych między aplikacjami;

	47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 51. Ochrona zawartości schowka systemu 52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 55.Możliwość tworzenia profilu DLP dla każdej polityki 56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 57. Ochrona przez wyciekiem plików poprzez programy typu p2p 58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 59. Monitorowanie określonych rodzajów plików. 60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 61. Możliwość śledzenia zmian we wszystkich plikach 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 68. Musi posiadać możliwość eksportu danych użytkownika 69. Musi umożliwiać import listy urządzeń z pliku CSV 70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; 73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 76. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa:

	78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 79. Portal musi być dostępny w postaci usługi hostowanej; 80. Skanowanie podatności za pomocą nodów skanujących 81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 82. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowanie możliwości zmiany widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV; 114. **B**ackup i przywracanie danych; 115. Deduplikacja danych na źródle, 116. Backup przyrostowy i różnicowy, 117. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 118. Backup danych lokalnych – plikowy oraz poczty; 119. Backup otwartych plików; 120. Filtr plików oraz folderów; 121. Domyślne wykluczenia zbędnych plików; 122. Przywracanie danych do wskazanej lokalizacji, 123. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora; 124. Wyszukiwanie plików w repozytorium użytkownika; 125. Automatyczne logowanie; 126. Zapamiętywanie danych logowania; 127. Automatyczne uruchamianie programu przy starcie systemu; 128. Ustawianie priorytetu dla procesu backupu; 129. **Z**miana klucza szyfrującego; 130. Ustawienia przepustowości/zajętości pasm;, 131. Konfiguracja wydajności procesu backup; 132. Zastępowanie nazwy pliku GUID-em; 133. Szyfrowanie danych algorytmem AES 256 CBC po stronie komputera użytkownika, 134. Kompresja danych; 135. Transmisja po bezpiecznym protokole TLS; 136. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji; 137. Obliczanie sumy kontrolnej; 138. Kopie zapasowe musza być przechowywane w data center; 139. Licencje przypisywane do urządzenia z przestrzenią w chmurze 50 GB. 140. Licencja obowiązuje minimum przez okres gwarancji laptopa. 141. Wsparcie techniczne musi być świadczone w języku polskim;

V. Serwerowy system operacyjny – 2 szt.

System operacyjny w najnowszej wersji pozwalający na uruchomienie dwóch wirtualnych maszyn z odpowiednią ilością rdzeni procesora. Spełniający poniższe wymagania:

1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
2. 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.
3. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9. Możliwość uruchamianie aplikacji internetowych wykorzystujących techologię ASP.NET.
10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
11. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
12. Graficzny interfejs użytkownika.
13. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
15. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
16. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
17. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
18. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
    e) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: dystrybucję certyfikatów poprzez http, konsolidację CA dla wielu lasów domeny, automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
    f) Szyfrowanie plików i folderów.

g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6).
k) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerac;,
l) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
m) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath);
n) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
o) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
p) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WSManagement organizacji DMTF; x) Materiały edukacyjne w języku polskim.

19. Licencja na 16 rdzeni procesorowych;
20. Analizator najlepszych praktyk
21. Pamięć dynamiczna przy wirtualizacji;
22. Dodawanie i wymiana kości RAM bez wyłączania systemu operacyjnego;
23. Konsola zarządzająca;
24. Sieciowy load balancing;
25. Migracja pamięci masowej;
26. Aktywacja zbiorcza;
27. Manager zasobów systemu operacyjnego;
28. Logowanie licencji serwera;
29. Nieograniczona liczba połączeń RRAS;
30. Obsługa 64 gniazd 64 bitowych;
31. Obsługa 24 TB pamięci RAM;
32. Możliwość dołączenia do domeny;
33. Kodeki DLNA i strumieniowe przesyłanie multimediów internetowych;
34. Certyfikaty usług katalogowych;
35. Zarządzanie usługami katalogowymi;
36. Serwer: DHCP, DNS, iPAM, iSNS, SMTP, faksów, plików, dla NFS;
37. Deduplikacja danych
38. Replikacja systemu plików DFS;
39. Funkcja serwera docelowego iSCSI I kontrolera sieci;
40. Możliwość dostępu i pulpitu zdalnego;
41. Usługi IIS;
42. Usługa inteligentnego transferu w tle;
43. Szyfrowanie I odblokowywanie dysków bitlocker;
44. Możliwość pracy w klastrze;
45. Zarządzanie politykami grupowymi;
46. Monitorowanie portów LPR;
47. Kolejkowanie wiadomości;
48. Protokół rozpoznawania nazw równorzędnych;
49. Manager połączeń RAS;

50. Zdalna pomoc użytkownikom sieciowym;
51. Zdalna kompresja różnicowa;
52. RSAT;
53. RPC przez proxy HTTP;
54. Usługi TCP/IP;
55. Udostępnianie plików SMB 1.0/CIFS;
56. Klient Telnet i TFTP;
57. Wewnętrzna baza danych;
58. Kopia zapasowa serwera;
59. Narzędzia do migracji system operacyjnego;
60. Filtr TIFF IF;
61. Przeglądarka XPS;
62. Licencja bezterminowa;

Zamawiający zastrzega sobie możliwość wezwania oiferentów, którzy złożyli oferty niepodlegające odrzuceniu w niniejszym postępowaniu, do okazania zaoferowanego sprzętu i oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SIWZ.
Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe).
Niestawienie się oferenta w wyznaczonym czasie i miejscu na okazaniu (prezentacji) sprzętu i/lub oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez oferenta wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.

INFORMATYK
Robert Gobis

Z upoważnienia Wójta
ZASTĘPCA WÓJTA
mgr inż. Tomasz Kołodziejczyk