Załącznik nr 7 do SWZ- OPZ

I. Laptopy – 69 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Ekran	15.6 FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nits Kąt otwarcia matrycy min.180 stopni
Wydajność	Oferowany komputer przenośny musi osiągać w teście wydajności : PC Mark10– wynik 2800 punktów. **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	8GB z możliwością rozbudowy do min. 16GB RAM.
Pamięć masowa	256GB NVMe SSD M.2 Komputer musi oferować montaż dwóch dysków w konfiguracji M.2 + 2,5”
Grafika	Osiągająca w teście Sysmark25 Creativity 600 punktów. **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
Klawiatura	Z wydzieloną strefą numeryczną (układ US),. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną; Wbudowane głośniki stereo 2x2W.

	Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywnościmtrwale zainstalowana w obudowie matrycy. Port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 5 AC 201 2x2 + Bluetooth 4.2
Bateria i zasilanie	Bateria umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii- 8 godzin, potwierdzony przeprowadzonym testem BAPCO MobileMark25 Battery Life. **Wydruk z oprogramowania testującego załączyć do oferty** Zasilacz o mocy min. 45W
Waga i wymiary	Waga max 1.7 kg z baterią
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane; Uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią.
Certyfikaty	Laptop musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001 – **certyfikaty załączyć do oferty;** Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym – **załączyć do oferty wydruk ze strony producenta oprogramowania**;
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, pendrive;
Bezpieczeństwo	TPM zintegrowany z płyta główną; Musi umożliwiać szyfrowanie 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.
Porty i złącza	Wbudowane (nie dopuszcza się przejściówek): 1 x HDMI 1.4 1 x RJ-45, 3 x USB w tym min. 2x USB 3.2, port zasilania, złącze linki zabezpieczającej
Warunki gwarancyjne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. 2-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Oferent musi posiadać ISO 27001 na świadczenie usług – **certyfikat załączyć do oferty**
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 3. Obsługa komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 4. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i

	angielskim 5. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 6. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 7. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; 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 dostępne w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
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; 83. Deduplikacja danych na źródle, 84. Backup przyrostowy i różnicowy, 85. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 86. Backup danych lokalnych – plikowy oraz poczty; 87. Backup otwartych plików; 88. Filtr plików oraz folderów, 89. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), 90. Przywracanie danych do wskazanej lokalizacji,

	91. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 92. Wyszukiwanie plików w repozytorium użytkownika, 93. Automatyczne logowanie, 94. Zapamiętywanie danych logowania, 95. Automatyczne uruchamianie programu przy starcie systemu, 96. Ustawianie priorytetu dla procesu backupu, 97. Zmiana klucza szyfrującego, 98. Konfiguracja wydajności procesu backupu, 99. Zastępowanie nazwy pliku GUID-em, 100. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 101. Kompresja danych, 102. Transmisja po bezpiecznym protokole TLS, 103. Deklaracja klucza szyfrującego dane użytkownika, 104. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 105. Obliczanie sumy kontrolnej, 106. Kopie zapasowe musza być przechowywane w data center, na terenie Polski. 107. Licencje musza być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB; 108. Wsparcie techniczne, świadczone w języku polskim;

II. Zestaw komputerowy – 9 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 PC Mark10 wynik 2800 punktów. **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	8GB DDR4 z możliwością rozbudowy do 64 GB;
Pamięć masowa	256 SSD
Grafika	Zintegrowana ze wsparciem dla DirectX 12.
Wyposażenie	Karta dźwiękowa zintegrowana z płytą główną, 2 kanałowa;

multimedialne	
Obudowa	Obudowa zaprojektowana i wykonana na zlecenie producenta komputera. Możliwość montażu niskoprofilowych kart graficznych, montaż beznarzędziowy dysku 3,5" oraz 2,5", napędu optycznego i kart rozszerzeń. Obudowa wykonana z wytrzymałego tworzywa, blachy o grubości co najmniej 0,5 mm. Możliwość montażu dysku 2,5" oraz 3,5" wewnątrz obudowy Zatoki na dyski i napędy: 2× 2,5/3,5, 1× 3,5, 1x 5,25; Wyposażona w co najmniej 2 porty 3.1 oraz złącza mikrofonu i słuchawek z przodu obudowy Wbudowana karta sieciowa 10/100/1000 Zasilacz o mocy minimum 300W 80+ Bronze. W obudowie zamontowane trzy fabrycznie filtry przeciwkurzowe; Trzystopniowy kontroler obrotów na 6 wentylatorów
Certyfikaty i standardy	Komputer musi być wyprodukowany zgodnie z ISO 9001, ISO 27001, ISO 28000 – **certyfikaty załączyć do oferty;** Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym – **załączyć do oferty wydruk ze strony producenta oprogramowania**;
Wbudowane porty	Wbudowane porty: • 1 x DVI lub VGA, • 1 x HDMI ver. 1.4 • 6 portów USB wyprowadzonych na zewnątrz komputera w tym min.: 2 porty USB 3.2 z przodu obudowy; Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp. Porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL, PXE 2.1. Płyta główna zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości., przeznaczona dla danego urządzenia; wyposażona w : • SATA III (6 Gb/s) - 4 szt. • M.2 - 2szt. • PCIe 3.0 x16 - 1 szt. • PCIe 3.0 x1 - 2szt. • 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, z obsługą DDR4-3200 MHz Klawiatura USB w układzie polski programisty Mysz USB z klawiszami oraz rolką (scroll) Wbudowana w obudowę nagrywarka DVD +/-RW szybkość min. x24 Wsparcie dla konfiguracji RAID Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera. Ochrona przed nadmiernym napięciem zasilania: System zasilania chroniący obwód zaprojektowany przez producenta płyty głównej z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd

	połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo złych zasilaczy.
Warunki gwarancji	2-letnia gwarancja producenta, Czas reakcji serwisu do końca następnego dnia roboczego. Oferent musi posiadać certyfikat ISO 27001 na świadczenie usług serwisowych – **dokument potwierdzający załączyć do oferty.**
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 3. Obsługa komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 4. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 5. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 6. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 7. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; 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 dostępne w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
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 13. wrażliwości 14. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 15. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 16. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 17. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 18. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 19. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 20. Blokada możliwości uruchamiania oprogramowania z takich dysków. 21. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 22. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 23. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 24. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 25. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 26. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 27. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; 28. 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; 29. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych zainstalowanych w różnych lokalizacjach; 30. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 31. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 32. Musi posiadać dostęp do konsoli z dowolnego miejsca; 33. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 34. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 35. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych; 36. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 37. 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; 38. Wirtualna klawiatury 39. Możliwość blokowania każdej aplikacji 40. Możliwość zablokowania aplikacji w oparciu o kategorie 41. Możliwość dodania własnych aplikacji do listy zablokowanych 42. Dodawanie aplikacji w formie portable 43. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 44. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 45. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 46. Możliwość zablokowania funkcji Printscreen 47. Monitorowania przesyłu danych między aplikacjami; 48. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 49. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj

	50. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 51. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 52. Ochrona zawartości schowka systemu 53. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 54. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 55. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 56. Możliwość tworzenia profilu DLP dla każdej polityki 57. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 58. Ochrona przez wyciekiem plików poprzez programy typu p2p 59. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 60. Monitorowanie określonych rodzajów plików. 61. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 62. Możliwość śledzenia zmian we wszystkich plikach 63. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 64. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 65. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 66. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 67. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 68. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 69. Musi posiadać możliwość eksportu danych użytkownika 70. Musi umożliwiać import listy urządzeń z pliku CSV 71. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 72. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 73. 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; 74. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 75. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 76. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 77. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 78. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: 79. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 80. Portal musi być dostępny w postaci usługi hostowanej;

	81. Skanowanie podatności za pomocą nodów skanujących 82. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 83. 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. Deduplikacja danych na źródle, 85. Backup przyrostowy i różnicowy, 86. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 87. Backup danych lokalnych – plikowy oraz poczty; 88. Backup otwartych plików; 89. Filtr plików oraz folderów, 90. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), 91. Przywracanie danych do wskazanej lokalizacji, 92. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 93. Wyszukiwanie plików w repozytorium użytkownika, 94. Automatyczne logowanie, 95. Zapamiętywanie danych logowania, 96. Automatyczne uruchamianie programu przy starcie systemu, 97. Ustawianie priorytetu dla procesu backupu, 98. Zmiana klucza szyfrującego, 99. Konfiguracja wydajności procesu backupu, 100. Zastępowanie nazwy pliku GUID-em, 101. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 102. Kompresja danych, 103. Transmisja po bezpiecznym protokole TLS, 104. Deklaracja klucza szyfrującego dane użytkownika, 105. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 106. Obliczanie sumy kontrolnej, 107. Kopie zapasowe musza być przechowywane w data center, na terenie Polski. 108. Licencje musza być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB; 109. Wsparcie techniczne, świadczone w języku polskim;

Monitor – 9 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rozmiar (klasa)	21,5 cala;

Typ panelu	IPS, VA lub MVA;
Format obrazu	16:9
Wielkość piksela	Maksymalnie 0,25
Rozdzielczość	1920 x 1080
Twardość ekranu	3H
Czas reakcji matrycy	Maksymalnie 5 ms.
Jasność	250 nitów;
Kontrast statyczny	3000:1
Głośniki	2 x 2W;
Pochylenie	od -5 do 20 stopni;
Katy widzenia	178 stopni;
Złącza	1 x VGA, 1 x HDMI, 1 x DVI, wejście i wyjście audio;
Warunki gwarancji	3 lata;
Wymagania dodatkowe	Kensington Lock. zgodność ze standardem VESA, kabel HDMI, Energy Star 8;

III. Tablet - 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	2 GHz, 8 rdzeni;
Pamięć RAM	4 GB;
Pamięć wbudowana	64 GB Możliwość rozbudowy o dodatkową pamięć do 1 TB;
Ekran	10,5” , 1920x1200, TFT;
Łączność	Wi-Fi 802.11 b/g/n/ac 2,4 oraz 5 GHz WI-fi Direct Bluetooth 5.0 GPS, Glonass
Złącza	USB- 1 szt. Wyjście słuchawkowe 3,5 mm. stereo – 1 szt.. Czytnik kart pamięci SD/microSD 1 szt.
Czujniki	Akcelerometr; Czujnik żyroskopowy; Czujnik geomagnetyczny; Czujnik Halla; Czujnik światła
Bateria	7000 mAh;
Zainstalowany system operacyjny	Musi umożliwiać: • Komunikację głosową z aplikacjami obsługującymi usługę interakcji głosowej. • Bezpośrednie udostępnianie materiałów wybranym osobom w wybranych aplikacjach. • Uśpienie urządzenia. • Przełączenie aplikacji rzadziej używanych w tryb czuwania co zmniejsza zużycie baterii. • Obsługę USB oraz ładowanie urządzenia i przesyłanie danych z użyciem tego samego kabla. • Sterowanie uprawnieniami zainstalowanych aplikacji.

	• Weryfikację przy uruchomieniu czy oprogramowanie układowe lub system operacyjny różni się od wersji fabrycznej. • Obsługę rysika Bluetooth w tym klawiszy modyfikujących oraz czułości na nacisk. • Zaznaczanie tekstu. • Cofanie/przywracanie oraz inne działania na tekście. • Tłumaczenie tekstu. • Drukowanie dwustronne. • Automatyczną obsługę internetowych adresów URL zainstalowanych aplikacji, co musi pozwalać na ich uruchamianie zamiast ich stron internetowych. • Zarządzanie głośnością powiadomień, muzyki i alarmów. • Działanie jako przenośny hotspot Wi-Fi z obsługą pasma 5 GHz. • Używanie kart microSD i pamięci zewnętrznych jako zaszyfrowanej, rozszerzonej pamięci. • Przenoszenie konta, aplikacji i danych na nowe urządzenie. • Tworzenie automatycznej kopii zapasowej aplikacji. • Tworzenie i przywracanie kopii zapasowej dodatkowych ustawień systemu, takich jak ustawienia synchronizacji, preferowane aplikacje, ustawienia ułatwień dostępu

Oprogramowanie zabezpieczające	• Oprogramowanie musi pozwalać na pełne skanowanie;
	• Skanowanie w tle
	• Skanowanie w celu wykrycia zagrożeń typu malware
	• Skanowanie karty pamięci
	• Wyznaczanie wyjątków od skanowania na poziomie plików i folderów.
	• Aanalizowanie zainstalowanych aplikacji na urządzenia pod kątem luk w bezpieczeństwie oraz raportować o wystąpieniu o takiej aplikacji.
	• Harmonogram skanowania
	• Harmonogram skanowania musi wywoływać skanowanie w chwili wykrycia że urządzenie jest ładowane
	• Oprogramowanie musi analizować ustawienia urządzenia w celu minimalizowania zagrożeń oraz przekierowywać do ustawień które powinny być zamienione.
	• Oprogramowanie musi analizować ustawienia co najmniej następujących funkcji
	  ○ Konta i synchronizacja
	  ○ Bluetooth
	  ○ Szyfrowanie pamięci urządzenia
	  ○ Hotspot i Tethering
	  ○ Blokada ekranu
	  ○ Nieznane źródła aplikacji
	  ○ Debugowanie USB
	  ○ Wi-Fi
	• Oprogramowanie musi analizować i monitorować uprawnienia aplikacji co najmniej do:
	  ○ Dostęp do kontaktów
	  ○ Dostęp do danych identyfikacyjnych
	  ○ Śledzenie lokalizacji

	○ Dostęp do wiadomości ○ Dostęp do sieci • Oprogramowanie musi chronić przeglądanie Internetu • Oprogramowanie musi chronić przez atakami typu Phishing. • Oprogramowanie musi posiadać funkcję optymalizacji urządzenia • Oprogramowanie musi analizować uruchomione aplikacje i potrafić zamykać aplikacje nieużywane; • Oprogramowanie musi wspomagać zarządzanie energią poprzez zamykanie nieużywanych aplikacji, kontrolę jasności ekranu, kontrolę WiFi, bluetooth. • Oprogramowanie musi pozwalać na tworzenie co najmniej następujących raportów: wykorzystanie CPU, żywotność baterii oraz wykorzystanie pamięci. • Oprogramowanie powinno mieć białą listę aplikacji które nie powinny być zatrzymywane. • Oprogramowanie musi posiadać funkcję monitorowania wykorzystania sieci, informowania o zbliżającym się limicie danych oraz blokowania transmisji w przypadku osiągnięcia limitu transmisji danych. • Oprogramowanie musi wykonaywać kopię zapasową w chmurz i ja odzyskać; • Urządzenie musi posiadać funkcję bezpiecznego usunięcia danych z urządzenia i wszystkich jego nośników. • Oprogramowanie musi mieć ochronę rodzicielską o następujących funkcjach: ○Blokowanie stron po kategoriach (co najmniej: oprogramowanie, media społecznościowe, tylko dla dorosłych) ○Blokowanie stron ze wskazanego adresu URL. Funkcja musi działać w co najmniej następujących przeglądarkach internetowych: Chrome, Firefox, Maxthon, Opera i Dolphin. ○Musi posiadać funkcje wyjątków adresów URL • Uwierzytelnianie przez odczyt linii papilarnych; • Oprogramowanie musi informować o nowych aktualizacjach i ważnych alarmach bezpieczeństwa; • Oprogramowanie powinno wykonywać raporty: ○ Znalezione wirusy ○ Zablokowanie połączenia ○ Aktywności związane z ochroną przed kradzieżą ○ Strony internetowe które zostały zablokowane ○ Informacje o kopi zapasowej ○ Informacje o ostatniej aktualizacji bazy wirusów • Zdalne pobieranie lokalizacji urządzenia • Zdalne usuniecie danych z urządzenia np.: w przypadku kradzieży. • Oprogramowanie musi udostępniać kamerę i mikrofon w celu rejestracji w przypadku kradzieży urządzenia. • Oprogramowanie powinno w przypadku dwóch nieudanych prób wprowadzenia hasła blokady ekranu, wykonać automatycznie zdjęcie przy wykorzystaniu aparatu na froncie i tyle urządzenia; • Oprogramowanie musi posiadać certyfikaty AVTest oraz AV Comparatives Approved mobile produkt. • Jeżeli urządzenie jest zablokowanie żadne wiadomości i informacje

	nie mogą być wyświetlane na ekranie urządzenia. • Dział wsparcia dostępny po chat oraz www. • Oprogramowanie musi pozwalać na wybranie do jakich danych prywatnych może mogą mieć dostęp aplikacje; • Okno pokazujące: zużycie RAM. • Możliwość wyłączenia działających w tle aplikacji, • Śledzenie zużycia baterii
Aparat	8.0 Mpix - tył, 5 Mpix. – przód, autofocus;
Rozdzielczośc nagrywania	FHD (1920 x 1080), 30 klatek/sekundę
Rozdzielczość odtwarzania wideo	FHD (1920 x 1080), 60 klatek/sekundę
Format odtwarzania wideo	MP4, M4V, AVI, FLV;
Format odtwarzania audio	MP3, M4A, OGG, OGA, WAV, FLAC, MID, MIDI;
Dodatkowe wymagania	Możliwość synchronizacji z PC; Funkcja rejestracji ekranu;
Gwarancja	24 miesiące;

Zamawiający zastrzega sobie możliwość wezwania Wykonawców, 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 SWZ.

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 Wykonawcy 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.