Zał. A do SWZ
Załącznik nr 1 do Umowy

Opis Przedmiotu Zamówienia

1. Laptop

MINIMALNE WYMAGANIA	
LAPTOP	
Liczba sztuk	1 sztuka
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Przekątna ekranu	16,0 WQXGA (2560x1600), powłoką przeciwodblaskową, jasność 300 nits, Częstotliwość odświeżania ekranu 165Hz,
Wydajność komputera	Oferowany komputer przenośny musi osiągać w teście wydajności : SYSMARK 25 – wynik min. 1600 – test w oferowanej 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.).
Pamięć RAM	32GB DDR5, dwa złącza na pamięć, możliwość rozbudowy do 64GB RAM.
Pamięć masowa	512GB PCIe; Możliwość instalacji drugiego dysku PCIe
Karta graficzna	Niezintegrowana karta graficzna posiadająca wsparcie do DirectX 12, osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 5000 pkt. – test z przeprowadzonej konfiguracji załączyć do oferty.
Klawiatura	Klawiatura odporna na zalanie (układ US), min 100 klawiszy, z wydzieloną klawiaturą numeryczną. Klawiatura podświetlana. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo 2x2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa 720p z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy. 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 6 AX 2x2 + Bluetooth 5
Bateria i zasilanie	Bateria Polymer min. 4-komory [min. 36Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii min. 9 godzin, potwierdzony przeprowadzonym testem MobileMark25 Battery Life - do oferty załączyć wydruk przeprowadzonego testu lub link publikacji na stronie BAPCO, w oferowanej konfiguracji. Zasilacz o mocy min. 90W
Waga i wymiary	Waga max 2.4 kg z baterią Wysokość laptopa nie większa niż 24mm.
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Aluminiowa pokrywa matrycy.
Certyfikaty	• Certyfikat ISO 9001, ISO 14001, ISO 50001 dla producenta sprzętu (należy załączyć do oferty) • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. Potwierdzenie należy załączyć do oferty.

Dodatkowe oprogramowanie - w formularzu oferty należy podać pełną nazwę	Oprogramowanie zabezpieczające chroniące przed zagrożeniami, posiadające poniższe funkcjonalności: Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej. Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej Opis technologii 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. 2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware. 3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) 4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach. 5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny. 6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania. 7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami. 8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe. 9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików. 10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów. 11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem. 12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http. 13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania. 14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego. 16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego. 17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta. 18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.

	19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca. 20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych. 23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie. 24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. 25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego. 26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym 28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów. 31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne. 33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta. 34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku. 35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta. 36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania. 39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

	41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej. 42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta. 44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych. 45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki. 46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn. 47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta. 48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW. 49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej. 50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS. 51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna". 52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna" rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów. 53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna" rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp. 54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn. 55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna" czyści zawartość schowka systemowego. 56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup. 57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji. 59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej). 60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora. 61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych. 62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV. 63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.

	64. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji. 65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie. 66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów. 67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć. 68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu. 69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. 71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego. 73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej. 74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth. 76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. 77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy. 78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu. 79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach. 80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego. 81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu. 82. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 83. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.

	85. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 86. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 87. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 91. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 92. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. 93. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 94. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach. 95. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. 96. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware. 97. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 98. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji. 99. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji 100. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji. 101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku. 102. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny. 103. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN 104. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD) 105. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej. 106. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).

	107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji. Centralna administracja 1. Portal zarządzający jest dostępny w języku polskim. 2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej. 3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta. 4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. 5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami. 10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana. 16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.

	22. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 24. Profile mogą być przypisane do pojedynczych hostów lub do grup. 25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji. 29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego. 34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu. 36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną. Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia usług serwisowych oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. (dokumenty załączyć do oferty).
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 użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional lub równoważny spełniający poniższe warunki:

	Oferowany system musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, który spełnia 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 wielu językach do wyboru – w tym 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 kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta. 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).

	29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Integracja z ActiveDirectory.
Porty i złącza	Wbudowane porty i złącza: • USB 3.2 - 2 szt. • USB Typu-C (z DisplayPort) - 2 szt. • HDMI 2.1 - 1 szt. • Czytnik kart pamięci SD - 1 szt. • RJ-45 (LAN) - 1 szt. • Wyjście słuchawkowe/wejście mikrofonowe - 1 szt.
Warunki gwarancyjne, wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Minimum 12 miesięczna gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres : - mieć opiekę kierownika technicznego ds. Eskalacji - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) Dla zapewnienia wysokiego poziomu usług serwisowych Wykonawca musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia serwisu sprzętu komputerowego. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim. Wykonawca na etapie składania ofert winien przedłożyć dokumenty: Certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia serwisu sprzętu komputerowego.

2. Monitor 34”

MINIMALNE WYMAGANIA	
MONITOR 34”	
Liczba sztuk	3 sztuki
Rodzaj wyświetlacza:	Monitor LCD z podświetleniem LED / matryca aktywna TFT
Wielkość przekątnej:	34.14"
Zaokrąglony ekran:	Tak (3800R)
Wbudowane urządzenia:	Koncentrator USB 3.2 Generacji 1.
Typ panela:	IPS
Współczynnik kształtu:	21:9
Rozdzielczość natywna:	UWQHD 3440 x 1440
Rozstaw pikseli:	0.2325 mm
Pikseli na cal:	109
Jasność:	300 cd/m²
Współczynnik kontrastu:	1000:1 / 3000000:1 (dynamic)
Obsługa kolorów:	1,07 miliarda kolorów
Czas reakcji:	6 ms (standard), 4 ms (maks.)

Częstotliwość odświeżania pionowego:	60 Hz
Poziomy kąt widzenia:	178
Pionowy kąt widzenia:	178
Powłoka ekranu:	Antyrefleksyjna
Technologia podświetlenia:	WLED
Charakterystyka:	Przestrzeń barw 99% sRGB, zintegrowane zarządzanie kablami, 8-bit + Głębia Kolorów FRC
Wymiary (szer./głęb./wys.):	81.73 cm x 24.5 cm x 46.93 cm - z podstawką (najniższa pozycja)
Waga:	Maksymalnie 10.8 kg
Interfejsy:	DisplayPort 1.2 2 x HDMI Wyjście DisplayPort USB-C 3.1 Gen 1 USB-C 3,2 Generacji 1 upstream USB 3.2 Generacji 1. upstream (typ B) 3 x USB 3.2 Generacji 1. downstream USB-C 3.2 Generacji 1. downstream Słuchawki
Regulacja pozycji ekranu:	Wysokość, pokrętło, odchylenie
Kąt pochylenia:	-5/+35
Kąt obrotu:	90
Regulacja wysokości:	135 mm
Interfejs Montażowy VESA:	100 x 100 mm
Cechy:	Slot blokady bezpieczeństwa (kabel blokady sprzedawany osobno)
Dołączone przewody:	1 x kabel USB-C - 1.8 m
Lokalizacja:	Angielski / Europa
Typ Gniazda Zabezpieczającego:	Gniazdo bezpieczeństwa Kensington
Napięcie wejściowe:	AC 100-240 V (50/60 Hz)
Pobór Mocy SDR (tryb Wł.):	31.6 kWh/1000 godz.
Pobór Mocy HDR (tryb Wł.):	34.2 kWh/1000 godz.
Pobór Mocy (Standardowy):	200 wat
Pobór Mocy (Maksymalny):	250 wat
Certyfikat TCO:	Certyfikat TCO – załączyć do oferty
EPEAT Compliant:	EPEAT Gold
Certyfikat ENERGY STAR:	Tak
Gwarancja producenta	Minimum 12 miesięcy w serwisie

3. Monitor 27”

MINIMALNE WYMAGANIA	
MONITOR 27”	
Liczba sztuk	1 sztuka
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą LED, IPS lub VA 27” Pokrycie barw: 100% (sRGB)
Jasność	350 cd/m2
Kontrast statyczny	2000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy	max 6 ms
Rozdzielczość maksymalna	2560x1440 przy 120Hz
Wyświetlane kolory	16.7 milionów
Zakres pochylenia monitora	+20°~-5°
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia LED
Zużycie energii	Typowo 25W, czuwanie mniej niż 0,5W
Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot
Waga	Maksymalnie 8 kg
Złącze	1 x HDMI 1.4 1 x DisplayPort 1.4 1 x DisplayPort (Out) 1 x USB-C 3.2 Gen 2 2 x USB-A 3.2 Gen 2 1 x Wyjście liniowe audio
Gwarancja	Minimum 12 miesięcy gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. TCO – załączyć do oferty .
Inne	Odłączana stopa, VESA 100mm Redukcja migotania (Flicker free) Filtr światła niebieskiego Obrotowa podstawa (Swivel): -45° do 45° Panel obrotowy (Pivot): -90° do 90° Regulacja wysokości (Height): 15 cm

4. Stacja dokująca

MINIMALNE WYMAGANIA	
STACJA DOKUJĄCA	
Typ	Stacja dokująca (ładowanie, obraz, dane, dźwięk)/ replikator portów
Liczba sztuk	20 sztuk
Interfejs	USB-C (Thunderbolt 4)
Obsługiwane systemy	• Windows 10, • Windows 11, • Ubuntu 20.04 lub nowsza wersja
Kolor	Czarny
Maksymalna rozdzielczość wyjściowa	• 5K – 60 Hz (Pojedynczy wyświetlacz) • 4K – 60 Hz (Wyświetlacz Quad Display)

Maksymalna rozdzielczość	5120x2880 px
Ilość wspieranych monitorów	4
Zasilacz sieciowy	180W
Ładowanie (USB-C)	do 130W
Złącza interfejsu	• USB-C 3.2 gen 2 – 1 szt. • USB-C 3.2 gen 2 (DisplayPort)– 1 szt. • USB 3.2 gen 1 (PowerShare) – 1 szt. • USB 3.2 gen 1 – 2 szt. • Thunderbolt – 2 szt. • HDMI 2.0 – 1 szt. • DisplayPort 1.4– 2 szt. • RJ45(1 GB/s) – 1 szt.
Inne cechy	• Kontrolka LED, • Projekt modułowy, • Przejściówka adresu MAC, • Uaktywnienie z siecio LAN, • Hight Bit Rate 3 (HBR3), • Hight Bit Rate 2 (HBR2).
Dodatkowa zawartość zestawu	• Kabel zasilający (Thunderbolt 4) – 1 szt. • Zasilacz sieciowy 180W – 1 szt.
Gwarancja	Minimum 12 miesięcy
Bezpieczeństwo	Slot na linkę zabezpieczającą

5. Komputer MFF typ 1

MINIMALNE WYMAGANIA	
KOMPUTER MFF	
Liczba sztuk	22 sztuki
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Wydajność obliczeniowa	Oferowany komputer przenośny musi osiągać w teście wydajności : SYSMARK 25 – wynik min. 1600 – test w oferowanej 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.).
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia. Wykonawca dostarczy oświadczenie poparte oświadczeniem producenta komputera iż przez cały okres trwania gwarancji płyta główna w przypadku uszkodzenia zostanie wymieniona na ten sam model, z możliwością przypisania numeru seryjnego komputera w BIOS. Wyposażona w sloty i złącza : • 2 złącza SODIMM z obsługą do 64GB pamięci RAM, • 1 złącze M.2 dedykowane dla dysku SSD • 1 złącze SATA z zasilaniem

	• 1 złącze M.2 WLAN Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez stosowania przejściówek/hub'ów itp. na front obudowy : przedni: • 1x Universal audio jack (słuchawki I mikrofon) • 2x USB 3.2 Gen 1 typ A tylny: • 1x DisplayPort 1.4a (HBR2) • 1x HDMI 1.4b • 2x USB 3.2 Gen 1 typ A • 2x USB 2.0 • 1x RJ45 10/100/1000 • Złącze zasilania • Dodatkowy port wyprowadzony z płyty głownej zamontowany na tylnym panelu I/O bez zajmowania slotów dla kart rozszerzeń: USB Type-C z DisplayPort
Pamięć RAM	16GB DDR4. Możliwość rozbudowy do min 64GB, min. dwa sloty pamięci
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe
Wydajność grafiki	karta graficzna posiadająca wsparcie do DirectX 12, osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 5000 pkt. – test z przeprowadzonej konfiguracji załączyć do oferty.
Sieć bezprzewodowa	Karta WIFI 6E 802.11ax z Bluetooth w wersji 5.2 [AX211]
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, Port słuchawek i mikrofonu (combo).
Obudowa	Małogabarytowa typu Terminal, umożliwiająca montaż wewnątrz obudowy min. 1 szt. M.2 SSD oraz 2,5". Suma wymiarów obudowy mierzona po krawędziach obudowy nie może przekraczać 398mm, waga komputera nie większa niż 1.32kg (bez zasilacza). Zasilacz o mocy min. 65W o efektywności min. 88%, informacja dostępna w oficjalnym dokumencie producenta, załączyć dokument lub wskazać link do dokumentu Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona). Obudowa powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, 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	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny

	nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządze, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym 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. Funkcja ustawienia hasła dla dysku M.2. Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą 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, upgrade BIOS.
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: ▪ monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; ▪ zdalną konfigurację ustawień BIOS, ▪ zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; ▪ zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani

	dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie; ▪ zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. ▪ technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/) ▪ nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS. ▪ wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional lub równoważny spełniający poniższe warunki: Oferowany system musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, który spełnia 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 wielu językach do wyboru – w tym 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 kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.

	13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta. 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Integracja z ActiveDirectory.
Certyfikaty i standardy	Certyfikat ISO 9001 (załączyć dokument potwierdzający spełnianie wymogu) Certyfikat ISO14001 (załączyć dokument potwierdzający spełnianie wymogu) Certyfikat ISO 50001 (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE (załączyć do oferty) Certyfikat EPEAT Gold dla Polski – do oferty należy załączyć wydruk ze strony https://epeat.net/ - załączyć do oferty wydruk z strony Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie **22** dB (załączyć oświadczenie producenta).
Wymagania dodatkowe	Klawiatura USB w układzie polski programisty Mysz laserowa USB z klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.

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 gwarancyjne, wsparcia techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Min. 12 miesięczna gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres : • mieć opiekę kierownika technicznego ds. Eskalacji • dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) Dla zapewnienia wysokiego poziomu usług serwisowych Wykonawca musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia serwisu sprzętu komputerowego. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim. Wykonawca na etapie składania ofert winien przedłożyć dokumenty: • Certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia serwisu sprzętu komputerowego.
Dodatkowe oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego. Oprogramowanie musi w pełni integrować się z Microsoft SCCM Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego. Zamawiający oczekuje oprogramowania zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej: - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające: • upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, • możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: o poprawkach i usprawnieniach dotyczących aktualizacji o dacie wydania ostatniej aktualizacji o priorytecie aktualizacji o zgodności z systemami operacyjnymi o jakiego komponentu sprzętu dotyczy aktualizacja o wszystkich poprzednich aktualizacjach z informacjami jak powyżej.

	• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne • możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. • rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) • sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) • dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

6. Komputer MFF typ 2

MINIMALNE WYMAGANIA	
KOMPUTER MFF	
Liczba sztuk	3 sztuki
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Wydajność obliczeniowa	Oferowany komputer przenośny musi osiągać w teście wydajności : SYSMARK 25 – wynik min. 1600 – test w oferowanej 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.).
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia. Wykonawca dostarczy oświadczenie poparte oświadczeniem producenta komputera iż przez cały okres trwania gwarancji płyta główna w przypadku uszkodzenia zostanie wymieniona na ten sam model, z możliwością przypisania numeru seryjnego komputera w BIOS. Wyposażona w sloty i złącza : • 2 złącza SODIMM z obsługą do 64GB pamięci RAM, • 1 złącze M.2 dedykowane dla dysku SSD • 1 złącze SATA z zasilaniem • 1 złącze M.2 WLAN Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez stosowania przejściówek/hub'ów itp. na front obudowy : przedni:

	• 1x Universal audio jack (słuchawki I mikrofon) • 2x USB 3.2 Gen 1 typ A tylny: • 1x DisplayPort 1.4a (HBR2) • 1x HDMI 1.4b • 2x USB 3.2 Gen 1 typ A • 2x USB 2.0 • 1x RJ45 10/100/1000 • Złącze zasilania • Dodatkowy port wyprowadzony z płyty głównej zamontowany na tylnym panelu I/O bez zajmowania slotów dla kart rozszerzeń: USB Type-C z DisplayPort
Pamięć RAM	16GB DDR4. Możliwość rozbudowy do min 64GB, min. dwa sloty pamięci
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe
Wydajność grafiki	karta graficzna posiadająca wsparcie do DirectX 12, osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 5000 pkt. – test z przeprowadzonej konfiguracji załączyć do oferty.
Sieć bezprzewodowa	Karta WIFI 6E 802.11ax z Bluetooth w wersji 5.2 [AX211]
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, Port słuchawek i mikrofonu (combo).
Obudowa	Małogabarytowa typu Terminal, umożliwiająca montaż wewnątrz obudowy min. 1 szt. M.2 SSD oraz 2,5". Suma wymiarów obudowy mierzona po krawędziach obudowy nie może przekraczać 398mm, waga komputera nie większa niż 1.32kg (bez zasilacza). Zasilacz o mocy min. 65W o efektywności min. 88%, informacja dostępna w oficjalnym dokumencie producenta, załączyć dokument lub wskazać link do dokumentu Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona). Obudowa powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, 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	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.

Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządze, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym 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. Funkcja ustawienia hasła dla dysku M.2. Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą 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, upgrade BIOS.
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: ▪ monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; ▪ zdalną konfigurację ustawień BIOS, ▪ zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; ▪ zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie;

	▪ zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. ▪ technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/) ▪ nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS. ▪ wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
System operacyjny	brak
Certyfikaty i standardy	Certyfikat ISO 9001 (załączyć dokument potwierdzający spełnianie wymogu) Certyfikat ISO14001 (załączyć dokument potwierdzający spełnianie wymogu) Certyfikat ISO 50001 (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE (załączyć do oferty) Certyfikat EPEAT Gold dla Polski – do oferty należy załączyć wydruk ze strony https://epeat.net/ - załączyć do oferty wydruk z strony Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie **22** dB (załączyć oświadczenie producenta).
Wymagania dodatkowe	Klawiatura USB w układzie polski programisty Mysz laserowa USB z klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
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 gwarancyjne, wsparcia techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Min. 12 miesięczna gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres :

	• mieć opiekę kierownika technicznego ds. Eskalacji • dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) Dla zapewnienia wysokiego poziomu usług serwisowych Wykonawca musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia serwisu sprzętu komputerowego. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim. Wykonawca na etapie składania ofert winien przedłożyć dokumenty: • Certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia serwisu sprzętu komputerowego.

7. Kontroler do drona

MINIMALNE WYMAGANIA	
KONTROLER	
Liczba sztuk	1 sztuka
Model	DJI RC RM330 lub równoważny kompatybilny z dronem DJI Mini 3 Pro
System transmisji wideo	Wykorzystanie technologii transmisji wideo, która po połączeniu z kompatybilnym modelem drona przełączy się na odpowiednią dla niego technologię transmisji wideo.
Maksymalny zasięg transmisji (bez przeszkód, bez zakłóceń)	12-15 km (FCC), 8 km (CE/ SRRC/ MIC)
Częstotliwość robocza	• 2,400-2,4835 GHz; • 5,727-5,850 GHz;
Anteny	2 anteny, 1T2R
Moc transmitera (EIRP)	• 2,400-2,4835 GHz: <26 dBm (FCC), <20 dBm (CE / SRRC / MIC); • 5,725-5,850 GHz: <26 dBm (FCC), <23 dBm (SRRC), <14 dBm (CE);
Protokół WiFi	802.11 a/b/g/n
Częstotliwość robocza (WiFi)	• 2,400-2,4835 GHz; • 5,150-5,250 GHz; • 5,725-5,850 GHz;
Moc transmitera (EIRP) (WiFi)	• 2,400-2,4835 GHz**:** <23 dBm (FCC), <20 dBm (CE / SRRC / MIC); • 5,150-5,250 GHz: <23 dBm (FCC / CE / SRRC / MIC); • 5,725-5,850 GHz: <23 dBm (FCC / SRRC), <14 dBm (CE);
Wersja Bluetooth	4.2
Częstotliwość robocza (Bluetooth)	2,400-2,4835 GHz
Moc transmitera (Bluetooth)	<10 dBm
Rozdzielczość ekranu	1920x1080
Przekątna	5,5”
Liczba klatek na sekundę	60 FPS
Jasność	700 nitów
Obsługa dotykowa	10-punktowy multi-touch
Typ akumulatora	Li-ion
Pojemność akumulatora	Minimum 5200 mAh (3,6 V)
Sposób ładowania	Ładowarka 5 V / 2 A lub lepsza
Moc znamionowa	4,5 W
Pamięć	Możliwość rozszerzenia (za pomocą karty microSD)
Czas ładowania	Średni maksymalny 1,5 h

Czas pracy	Minimum 4 godziny
GNSS	GPS + BeiDou + Galileo
Kompatybilne drony	DJI Mini 3 Pro, DJI Mavic 3, DJI Mavic 3 Cine
Obsługiwane karty microSD	Klasa prędkości UHS-I Speed Grade 3 lub lepsze
Gwarancja	Minimum 12 miesięcy