Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Nisku
ul. Kościuszki 1, 37-400 Nisko

Sygnatura: **Z.II.260.002.Zp.2023**

Nisko, dnia 20/02/2023 r.

WYKONAWCY
ubiegający się o zamówienie publiczne

P O W I A D O M I E N I E
o zmianach SWZ

Dotyczy: postępowania o udzielenie zamówienia publicznego, prowadzonego w trybie przetargu nieograniczonego na **„Modernizację infrastruktury teleinformatycznej oraz modernizację i wdrożenie e-usług medycznych realizowana w ramach projektu pn. „Rozwój e-usług medycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku** – znak sprawy **Z.II.260.002.Zp.2023**

Zamawiający, **Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej**, działając na podstawie art. 137 ust. 1 i 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2022 r. poz. 1710 z późn. zm.), informuje o dokonaniu zmian w zapisach Specyfikacji warunków zamówienia w następującym zakresie:

1. **W pkt. 14.2. Specyfikacji Warunków Zamówienia było:**
   14.2. Wadium musi zostać wniesione przed upływem terminu składania ofert, tj. do dnia **17/02/2023** do godz. 10.30, według wyboru Wykonawcy w jednej lub kilku następujących formach:
   - pieniądzu,
   - gwarancjach bankowych,
   - gwarancjach ubezpieczeniowych,
   - poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2020 r. poz. 299).

   W pkt. 14.2. Specyfikacji Warunków Zamówienia jest:
   14.2.Wadium musi zostać wniesione przed upływem terminu składania ofert, tj. do dnia **24/02/2023** do godz. 10.30, według wyboru Wykonawcy w jednej lub kilku następujących formach:
   - pieniądzu,
   - gwarancjach bankowych,
   - gwarancjach ubezpieczeniowych,
   - poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2020 r. poz. 299).

2. **W pkt. 14. 3. Specyfikacji Warunków Zamówienia było:**
   14.3. Wadium musi obejmować pełen okres związania ofertą tj. do dnia **17/05/2023**.

   W pkt. 14. 3. Specyfikacji Warunków Zamówienia jest:
   14.3. Wadium musi obejmować pełen okres związania ofertą tj. do dnia **24/05/2023**.

3. **W pkt. 15. 1. Specyfikacji Warunków Zamówienia było:**
   15.1. Wykonawca pozostaje związany ofertą do dnia **17/05/2023**.

   W pkt. 15. 1. Specyfikacji Warunków Zamówienia jest:
   15.1. Wykonawca pozostaje związany ofertą do dnia **24/05/2023**.

4. **W pkt. 17.1. Specyfikacji Warunków Zamówienia było:**
   17.1.Ofertę, wraz z załącznikami, należy złożyć za pośrednictwem Platformy w terminie do dnia **17/02/2023** do godz. **10:30**.

   W pkt. 17.1. Specyfikacji Warunków Zamówienia jest:

17.1. Ofertę, wraz z załącznikami, należy złożyć za pośrednictwem Platformy w terminie do dnia **24/02/2023** do godz. **10:30**.

5. **W pkt. 18.1. Specyfikacji Warunków Zamówienia było:**

18.1. Otwarcie ofert nastąpi w dniu: **17/02/2023** o godz. **11:00**, za pośrednictwem Platformy, na karcie **„Oferta/Załączniki”**, poprzez ich odszyfrowanie, które jest jednoznaczne z ich upublicznieniem.

W pkt. 18.1. Specyfikacji Warunków Zamówienia jest:

18.1. Otwarcie ofert nastąpi w dniu: **24/02/2023** o godz. **11:00**, za pośrednictwem Platformy, na karcie **„Oferta/Załączniki”**, poprzez ich odszyfrowanie, które jest jednoznaczne z ich upublicznieniem.

6. **W Załączniku nr 1 (Szczegółowy Opis Przedmiotu Zamówienia) w ZADANIU NR 1 – PARAMETRY MINIMALNE DOSTAWY SPRZĘTU – KOMPUTERY Z MONITORAMI (AIO) – 150 szt. było:**

KOMPUTERY Z MONITORAMI (AIO) - 150 szt.				
Lp.	**Element konfiguracji**	**Wymagania minimalne / warunek konieczny**	**Oferowane parametry (podać)**	**Potwierdzenie spełnienia minimalnych wymagań**
1.	**Typ**	W ofercie wymagane jest podanie modelu, symbolu oraz producenta.		TAK / NIE
2.	**Zastosowanie**	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Komputer wykonany z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged”, według normy Mil-Std-810H. W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez Zamawiającego, do oferty należy dołączyć: Certyfikat MIL-STD-810H lub równoważny certyfikat akredytowanej jednostki wykonującej badania wytrzymałości i odporności urządzeń potwierdzający odporność. Wymagane jest dostarczenie równoważnego certyfikatu wraz z opisem i dokumentacją fotograficzną z przeprowadzonych testów oraz informacją o pozytywnym ich zakończeniu wydaną przez akredytowaną jednostkę wydającą certyfikat. Zamawiający również akceptuje dostarczenie oświadczenia przez Wykonawcę potwierdzone oświadczeniem lub innym dokumentem pochodzącym od producenta, potwierdzającym, że komputer spełnia standardy MIL-STD-810H.		TAK / NIE
3.	**Procesor**	Min. 6-rdzeniowy, min. 3 GHz, osiągający w zaoferowanej konfiguracji w teście PassMark CPU Mark wynik min. 20000 punktów. Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów SWZ.		TAK / NIE

4.	**Pamięć operacyjna**	Minimum 8GB DDR4 3200 MHz z możliwością rozszerzenia do 64 GB. Ilość banków pamięci: minimum 2 szt.		TAK / NIE
5.	**Parametry pamięci masowej**	Minimum 256GB SSD M.2 PCIe NVMe oraz zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.		TAK / NIE
6.	**Grafika**	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.		TAK / NIE
7.	**Wyposażenie multimedialne**	Wbudowane, zgodne z HD Audio, wbudowane głośniki stereo 2 x 3W, wbudowane dwa mikrofony, wbudowana kamera o rozdzielczości 5MP z wbudowaną mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery.		TAK / NIE
8.	**Obudowa**	Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) zintegrowana z monitorem (AIO). Założona linka kensington musi jednocześnie umożliwiać przypięcie AIO do biurka oraz zabezpieczenie obudowy przed nieautoryzowanym otwarciem. Podstawa musi umożliwiać regulację kąta nachylenia w zakresie – 5° do przodu oraz 20° do tyłu, wysokości w zakresie 110 mm, PIVOT. Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością bez narzędziowego demontażu stopy. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnym, PN pozwalającym na jednoznaczna identyfikacje zaoferowanej konfiguracji.		TAK / NIE
9.	**Zgodność z systemami operacyjnymi i standardami**	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 (załączyć dokument potwierdzający zgodność lub oświadczenie producenta).		TAK / NIE
10.	**BIOS**	BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: – modelu komputera, PN, – numerze seryjnym, – numer inwentarzowy, – MAC Adres karty sieciowej, – wersja i data BIOS, – zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, – ilości pamięci RAM, – stanie pracy wentylatora, – informacja o licencji na system operacyjny. Możliwość z poziomu Bios: – wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy oraz z boku obudowy,		TAK / NIE

		– wyłączenia karty sieciowej (WIFI i LAN), karty audio, mikrofonu, kamery, czytnika kart multimedialnych, – możliwość wyłączenia wirtualizacji w BIOS, – możliwość zaprogramowania automatycznego włączenia komputera o określonej porze, – możliwość ustawienia następujących haseł: hasła administratora, hasła Power-On, hasła na dysk twardy, – dostęp do systemu logowania zdarzeń w BIOS. System musi zapewniać logowanie co najmniej takich zdarzeń jak: update BIOS, zmiany w konfiguracji, wyczyszczenie logów, – obsługa BIOS za pomocą klawiatury i myszy.		
11.	**Bezpieczeństwo**	1. BIOS musi posiadać możliwość: – skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, – możliwość ustawienia hasła na dysku (drive lock), – blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio, – blokady/wyłączenia poszczególnych kart rozszerzeń/slotów PCIe, – kontroli sekwencji boot-ącej, – startu systemu z urządzenia USB, – funkcja blokowania boot-owania stacji roboczej z zewnętrznych urządzeń. 2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 1.2). 3. Możliwość zapięcia linki typu Kensington i kłódki do dedykowanego oczka w obudowie komputera. 4. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego: – informacje o systemie, min.: – Procesor: typ procesora, jego obecna prędkość, – Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta, – Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku, – Napęd optyczny: model, wersja firmware, nr seryjny,		TAK / NIE

		– Data wydania i wersja BIOS, – Nr seryjny komputera. – możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera, – możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej, – rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii.		
12.	**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, posiadająca sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiająca: – monitorowanie konfiguracji komponentów komputera, – CPU, – pamięć, – HDD, – wersje 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, – 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 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (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,		TAK / NIE

		– wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego, – 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 1 920 x 1 080 włącznie.		
13.	**Certyfikaty i standardy**	Certyfikat ISO 9001 dla producenta sprzętu. Certyfikat ISO 14001 dla producenta sprzętu. Certyfikat ISO 50001 dla producenta sprzętu. Urządzenie musi spełniać: Deklaracja zgodności CE, TCO 9.0, TCO Edge, Zgodność z dyrektywą RoHS, TÜV Rheinland Low Blue Light, Energy Star 8.0.		TAK / NIE
14.	**Zainstalowane oprogramowanie systemowe**	Zainstalowany system operacyjny co najmniej Windows 10 Pro 64-bitowy w polskiej wersji językowej lub system równoważny wraz z nośnikiem instalacyjnym. Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu. System równoważny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem		TAK / NIE

		głosowo, wraz z modułem „uczenia się” głosu użytkownika. 8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 20. 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. 21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 22. Obsługa standardu NFC (near field communication). 23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 26. Mechanizmy logowania do domeny w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Mechanizmy wieloelementowego uwierzytelniania. 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 30. Wsparcie dla algorytmów Suite B (RFC 4869). 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający		

		większą niezawodność i pozwalający tworzyć kopie zapasowe. 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 40. Udostępnianie modemu. 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 43. 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.). 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.		
15.	**Warunki gwarancji**	1. 3 letnia gwarancja producenta świadczona na miejscu u klienta. Naprawa w miejscu instalacji urządzenia do końca następnego dnia roboczego. Uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2000 na		TAK / NIE

		świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. 2. Serwis świadczony w języku polskim (obsługa jak i zgłoszenia). 3. Zgłoszenia serwisowe realizowane poprzez nr telefonu, adres email oraz poprzez formularz zgłoszeniowy producenta komputera online. W formularzu ofertowym należy podać nr telefonu, adres email oraz link www do formularza online (Zamawiający będzie weryfikował wszystkie 3 formy zgłoszeń).		
16.	**Wsparcie techniczne producenta**	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: – weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć), – czasu obowiązywania i typ udzielonej gwarancji. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera.		TAK / NIE
17.	**Wymagania dodatkowe**	Wbudowane (minimum): DisplayPort,1 x HDMI IN/OUT, 7 x USB 3.2 (z czego jeden umożliwiający szybkie ładowanie urządzeń zewnętrznych/podłączanych nawet przy wyłączonym komputerze), 1 x RJ 45 (LAN), 1 x wyjście na słuchawki i mikrofon (Combo), Wśród portów USB wymaga się, aby przynajmniej jeden port był w standardzie USB-C 3.2 Gen 2. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Klawiatura USB w układzie polskim programisty (104 klawisze) z kablem o długości min. 1,8 m. Kolor czarny. Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m. Kolor czarny. Nagrywarka SATA DVD +/-RW SLIM.		TAK / NIE

18.	**Funkcje zdalnego sprzętowego zarządzania komputerami**	1. Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym (tzw. out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC. Wymagana jest obsługa funkcji zdalnego zarządzania przez wbudowane w komputer porty zarówno sieci przewodowej LAN, jak i bezprzewodowej WLAN (jeśli komputer jest wyposażony we wbudowaną kartę WLAN/WiFi), z wykorzystaniem protokołów TCP/IP w tym IPv6 wraz z szyfracją komunikacji zarządzania z protokołem TLS 1.2 z silnymi zestawami szyfrów TLS_RSA_WITH_AES_256_CBC_SHA (minimalna długość klucza 256 bitów) oraz TLS_RSA_WITH_AES_128_GCM_SHA256 lub silniejszymi/nowocześniejszymi. Obsługa wyłącznie protokołów TLS 1.0 i TLS 1.1 - bez ogsługi TLS 1.2 oraz słabych/przestarzałych zestawów szyfrów dla TLS 1.2: TLS_RSA_WITH_NULL_SHA, TLS_RSA_WITH_NULL_SHA256, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA jest NIEWYSTARCZAJĄCA. Technologia ta powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/). 2. Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym musi obsługiwać łącznie wszystkie następujące funkcje: monitorowanie konfiguracji komponentów komputera – model komputera i jego nr seryjny, model procesora, ilość i rodzaj modułów pamięci RAM, rodzaj i nr seryjny dysku HDD/SSD, wersja BIOS płyty głównej, nr seryjny płyty głównej: a) kontrolę zasilania komputera pozwalającą na sprawdzenie aktualnego stanu zasilania komputera (stany ACPI S0/S3/S4/S5) oraz funkcja zdalnego włączenia komputera/komputerów ze stanu pełnego wyłączenia, hibernacji lub uśpienia oraz zdalne zarządzanie stanem zasilania komputera: włączenie/wyłączenie/reset bez udziału systemu operacyjnego, b) zdalne wystartowanie komputera z alternatywnego obrazu systemu operacyjnego w postaci obrazu nośnika CD/DVD - pliku .iso lub nośnika USB - pliku .img montowanego zdalnie z konsoli zarządzania w tym zdalną reinstalację systemu operacyjnego z użyciem obrazu standardowego nośnika instalacyjnego		TAK / NIE

		zapewnianego przez producenta systemu operacyjnego, bez pomocy, interakcji ze strony użytkownika końcowego, c) zdalną konfigurację ustawień BIOS Setup, d) sprzętową kopię logu zdarzeń sprzętowych BIOS HW Event Log - zawierającego obsługiwane przez BIOS FW zdarzenia np. brak pamięci RAM w czasie inicjalizacji komputera lub brak dysku startowego uniemożliwiający załadowanie OS oraz informację o błędach samej technologii zarządzania sprzętowego np. wielokrotne nieudane próby logowania do tej technologii (tzw. Brute force atack), e) zapis i przechowywanie dodatkowych informacji oraz zdalny odczyt i zapis tych informacji również z wyłączonego komputera z wbudowanej dodatkowej pamięci nieulotnej o minimalnym rozmiarze 128 KB. Informacje te mogą zawierać dowolne dane np. o wersji zainstalowanego oprogramowania, zainstalowane uaktualnienia itp. które dodatkowe oprogramowanie pracujące na komputerze zarządzanym może pobrać z poziomu systemu operacyjnego i zapisać lokalnie w tej pamięci nieulotnej (NVM), f) zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 2560×1600 (WQXGA) włącznie. Funkcja przekierowania konsoli graficznej musi przechwytywać każdy rodzaj wyświetlanego na fizycznym lokalnym ekranie obrazu włącznie z procesem uruchamiaina komputera (POST), ładowania OS, zamykania OS oraz błędów OS BSOD (Blue Screen of Death), g) wbudowany sprzętowo log operacji zdalnego zarządzania (tzw. Security Audit Log), przechowujący informacje o wykorzystaniu funkcji technologii zdalnego zarządzania z informacją o dacie, czasie rodzaju operacji i koncie użytkownika zdalnego zarządzania który wykonał daną operacje, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego, h) obsługa niskopoziomowej autentykacje sieciowej z użyciem protokołu 802.1x (Radius) na poziomie sprzętu w celu uzyskania dostępu do sieci zabezpieczonej protokołem IEEE 802.1x, niezależnie od stanu czy obecności systemu operacyjnego oraz stanu zasilania komputera, niezależnie od takiej obsługi na poziomie systemu		

		operacyjnego, odpowiednio dla wbudowanych interfejsów LAN i WLAN, i) automatyczne nawiązywanie zdalnego szyfrowanego protokołem MTLS połączenia z predefiniowanym serwerem zarządzającym poprzez sieć Internet, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia sprzętowego (np. otwarcie obudowy z czujnikiem lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; Połączenie MTLS musi obsługiwać te same minimalne wymagania bezpieczeństwa które są wymagane dla szyfracji TLS w pkt. 1. 3. Domyślna konfiguracja fabryczna, zdalna konfiguracja funkcji zarządzania sprzętowego, narzędzia zarządzające: a) W domyślnej konfiguracji fabrycznej (factory default) funkcji zarządzania sprzętowego zdalny dostęp do funkcji zarządzania sprzętowego musi być zablokowany. Dopuszcza się możliwość wstępnej konfiguracji technologii zarządzania sprzętowego przez producenta komputera lub dostawcę wyłącznie na wyraźne życzenie zamawiającego wraz z ustawieniem haseł lokalnego (BIOS FW) i zdalnego (po sieci LAN/WLAN) dostępu do tej technologii na silne hasła zdefiniowane przez Zamawiającego. W procesie konfiguracji funkcji zdalnego zarządzania sprzętowego musi zostać wymuszona zmiana domyślnych haseł dostępu zdalnego na silne hasła zdefiniowane przez administratorów IT Zamawiającego, b) Zdalna konfiguracja ustawień funkcji zarządzania sprzętowego (rodzaju autentykacji, kont zdalnego zarządzania i ich list kontroli dostępu, szyfracji komunikacji, autentykacji 802.1x) musi być możliwa na wielu komputerach jednocześnie, poprzez sieć LAN i WLAN bez potrzeby manualnego dostępu do konfigurowanych komputerów. Narzędzia/oprogramowanie zdalnej konfiguracja ustawień funkcji zarządzania sprzętowego musi dokonywać konfiguracji tej technologii w sposób bezpieczny z wykorzystaniem szyfrowanego połączenia MTLS z certyfikatem serwera konfigurującego wystawionym przez następujące publiczne centra certyfikacji GoDaddy, Comodo, Entrust lub DigiCert i musi obsługiwać te same minimalne wymagania bezpieczeństwa które są wymagane dla szyfracji TLS w pkt. 1. Wykonawca dostarczy odpowiedni certyfikat ważny 60 miesięcy, c) Dostawca musi dostarczyć produkcyjne narzędzia/oprogramowanie służące do		

		konfiguracji ustawień funkcji zarządzania sprzętowego oraz narzędzia do zdalnego zarządzania komputerami z użyciem funkcji zdalnego zarządzania sprzętowego wraz z bezpłatną licencją, dokumentacją jego użycia oraz bezpłatnym wsparciem technicznym lub zawrzeć koszty takiego narzędzia i wsparcia technicznego w kosztach oferty. Dostawca może zamiast dostarczać ww. narzędzia i wsparcie techniczne wskazać publicznie dostępne narzędzie/oprogramowanie lub usługę chmurową z bezpłatną licencja i bezpłatne wsparcie techniczne oferowane przez producenta komputera lub producenta technologii zdalnego zarządzania sprzętowego. Narzędzia o charakterze nieprodukcyjnym (ewaluacyjnym, demo, testowym, wersje alfa/beta) lub posiadające ograniczenia ilości konfigurowanych i zarządzanych komputerów są niedopuszczalne. 4. Aktualizacja zabezpieczeń funkcji zdalnego zarządzania sprzętowego. Wymagane jest zapewnienie publicznie dostępnych bezpłatnych możliwości oraz bezpłatnych narzędzi do aktualizacji zabezpieczeń oprogramowania układowego (firmware) realizującego funkcje zdalnego zarządzania sprzętowego. Aktualizacje (nowy obraz oprogramowania firmware oraz narzędzia aktualizacji) mogą być dostarczane przez Wykonawcę, bezpośrednio przez producenta komputera lub bezpośrednio przez producenta technologii zdalnego zarządzania sprzętowego. Wymagane jest wskazanie przez dostawcę publicznego sposobu publikacji informacji o wykrytych podatnościach bezpieczeństwa technologii zdalnego zarządzania sprzętowego oraz sposobu dostępu i wykonania tych aktualizacji – np. przez podanie linku URL/strony WWW publicznie dostępnego portalu, gdzie udostępniane są takie informacje oraz aktualizacje. Preferowanym sposobem aktualizacji jest obsługiwany przez MS Windows 10 tzw. UEFI Capsule Firmware Update https://docs.microsoft.com/pl-pl/windows-hardware/drivers/bringup/windows-uefi-firmware-update-platform 5. Testy weryfikujące spełnianie przez oferowane komputery wymogów dotyczących funkcji zdalnego sprzętowego zarządzania komputerami. Zamawiający zastrzega sobie prawo do żądania przeprowadzenia na wezwanie demonstracji działania zaoferowanego rozwiązania zdalnego, sprzętowego zarządzania wraz z obsługą ww. wymaganych funkcji przez		

		dostawcę na koszt dostawcy oraz możliwość przeprowadzenia takich testów we własnym zakresie. W tym celu dostawca będzie zobowiązany do bezpłatnego dostarczenia przed podpisaniem umowy po jednej sztuce każdego z oferowanych modeli komputerów w celu przeprowadzenia testów przez Zamawiającego. Po przeprowadzeniu testów Zamawiający zwróci Dostawcy testowane komputery lub zaliczy dostarczone modele na poczet częściowej dostawy zamówionych komputerów. 6. Zgodność oferowanej i dostarczonej technologii zarządzania i monitorowania komputerami na poziomie sprzętowym z istniejącym środowiskiem zamawiającego. Wymagana jest pełna zgodność technologii zarządzania i monitorowania komputerami na poziomie sprzętowym w oferowanych i dostarczonych komputerach na poziomie mechanizmów konfiguracji i zarządzania z już zaimplementowanym w środowisku Zamawiającego rozwiązaniem opartym o oprogramowanie Intel® Setup and Configuration Software (Intel® SCS) w wersji 12.2.0.152 oraz Intel® Manageability Commander w wersji 2.1.133 lub nowszymi używanym obecnie do konfiguracji i zarządzania ponad 2000 komputerów. Wymagana jest też pełna zgodność na poziomie mechanizmów konfiguracji i zarządzania przez sieć Internet dla komputerów przeznaczonych do pracy zdalnej z domu z planowanym do wdrożenia rozwiązaniem opartym o Intel® Endpoint Management Assistant (Intel® EMA) w wersji 1.4 lub nowszej. 7. Instalacja i konfiguracja konsoli zdalnego dostępu do komputerów.		
19.	**Zakres prac**	Dostarczenie, wniesienie urządzeń, rozstawienie urządzeń w miejscach wskazanych przez Zamawiającego. Konfiguracja urządzeń. Instalacja wymaganego oprogramowania.		TAK / NIE

W Załączniku nr 1 (Szczegółowy Opis Przedmiotu Zamówienia) w ZADANIU NR 1 – PARAMETRY MINIMALNE DOSTAWY SPRZĘTU – KOMPUTERY Z MONITORAMI (AIO) – 150 szt. jest:

KOMPUTERY Z MONITORAMI (AIO) - 150 szt.				
Lp.	**Element konfiguracji**	**Wymagania minimalne / warunek konieczny**	**Oferowane parametry (podać)**	**Potwierdzenie spełnienia minimalnych wymagań**
1.	**Typ**	W ofercie wymagane jest podanie modelu, symbolu oraz producenta.		TAK / NIE
2.	**Zastosowanie**	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać		TAK / NIE

		nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Komputer wykonany z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged", według normy Mil-Std-810H. W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez Zamawiającego, do oferty należy dołączyć: Certyfikat MIL-STD-810H lub równoważny certyfikat akredytowanej jednostki wykonującej badania wytrzymałości i odporności urządzeń potwierdzający odporność. Wymagane jest dostarczenie równoważnego certyfikatu wraz z opisem i dokumentacją fotograficzną z przeprowadzonych testów oraz informacją o pozytywnym ich zakończeniu wydaną przez akredytowaną jednostkę wydającą certyfikat. Zamawiający również akceptuje dostarczenie oświadczenia przez Wykonawcę potwierdzone oświadczeniem lub innym dokumentem pochodzącym od producenta, potwierdzającym, że komputer spełnia standardy MIL-STD-810H.		
3.	**Procesor**	Min. 6-rdzeniowy, min. 3 GHz, osiągający w ~~zaoferowanej konfiguracji~~ w teście PassMark CPU Mark wynik min. 20000 punktów. Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów SWZ.		TAK / NIE
4.	**Pamięć operacyjna**	Minimum 8GB DDR4 3200 MHz z możliwością rozszerzenia do 64 GB. Ilość banków pamięci: minimum 2 szt.		TAK / NIE
5.	**Parametry pamięci masowej**	Minimum 256GB SSD M.2 PCIe NVMe oraz zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.		TAK / NIE
6.	**Grafika**	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.		TAK / NIE
7.	**Wyposażenie multimedialne**	Wbudowane, zgodne z HD Audio, wbudowane głośniki stereo 2 x 3W, wbudowane dwa mikrofony, wbudowana kamera o rozdzielczości 5MP z wbudowaną mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery.		TAK / NIE
8.	**Obudowa**	Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) zintegrowana z monitorem (AIO). Założona linka kensington musi jednocześnie umożliwiać przypięcie AIO do biurka oraz zabezpieczenie obudowy przed nieautoryzowanym otwarciem. Podstawa musi umożliwiać regulację kąta nachylenia w zakresie – 5° do przodu oraz 20° do tyłu, wysokości w zakresie 110 mm, PIVOT. Możliwość		TAK / NIE

		zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością bez narzędziowego demontażu stopy. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnym, PN pozwalającym na jednoznaczna identyfikacje zaoferowanej konfiguracji.		
9.	**Zgodność z systemami operacyjnymi i standardami**	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 (załączyć dokument potwierdzający zgodność lub oświadczenie producenta).		TAK / NIE
10.	**BIOS**	BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: – modelu komputera, PN, – numerze seryjnym, – numer inwentarzowy, – MAC Adres karty sieciowej, – wersja i data BIOS, – zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, – ilości pamięci RAM, – stanie pracy wentylatora, – informacja o licencji na system operacyjny. Możliwość z poziomu Bios: – wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy oraz z boku obudowy, – wyłączenia karty sieciowej (WIFI i LAN), karty audio, mikrofonu, kamery, czytnika kart multimedialnych, – możliwość wyłączenia wirtualizacji w BIOS, – możliwość zaprogramowania automatycznego włączenia komputera o określonej porze, – możliwość ustawienia następujących haseł: hasła administratora, hasła Power-On, hasła na dysk twardy, – dostęp do systemu logowania zdarzeń w BIOS. System musi zapewniać logowanie co najmniej takich zdarzeń jak: update BIOS, zmiany w konfiguracji, wyczyszczenie logów, – obsługa BIOS za pomocą klawiatury i myszy.		TAK / NIE
11.	**Bezpieczeństwo**	5. BIOS musi posiadać możliwość: – skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, – możliwość ustawienia hasła na dysku (drive lock), – blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio, – blokady/wyłączenia poszczególnych kart rozszerzeń/slotów PCIe,		TAK / NIE

		– kontroli sekwencji boot-ącej, – startu systemu z urządzenia USB, – funkcja blokowania boot-owania stacji roboczej z zewnętrznych urządzeń. 6. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 1.2). 7. Możliwość zapięcia linki typu Kensington i kłódki do dedykowanego oczka w obudowie komputera. 8. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego: – informacje o systemie, min.: – Procesor: typ procesora, jego obecna prędkość, – Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta, – Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku, – Napęd optyczny: model, wersja firmware, nr seryjny, – Data wydania i wersja BIOS, – Nr seryjny komputera. – możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera, – możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej, – rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii.		
12.	**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, posiadająca sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiająca: – monitorowanie konfiguracji komponentów komputera,		TAK / NIE

		– CPU, – pamięć, – HDD, – wersje 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, – 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 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (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, – 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 1 920 x 1 080 włącznie.		
13.	**Certyfikaty i standardy**	Certyfikat ISO 9001 dla producenta sprzętu. Certyfikat ISO 14001 dla producenta sprzętu. Certyfikat ISO 50001 dla producenta sprzętu. Urządzenie musi spełniać: Deklaracja zgodności CE, TCO 9.0, TCO Edge, Zgodność z dyrektywą RoHS, TÜV Rheinland Low Blue Light, Energy Star 8.0.		TAK / NIE
14.	**Warunki gwarancji**	1. 3 letnia gwarancja producenta świadczona na miejscu u klienta. Naprawa w miejscu instalacji urządzenia do końca następnego dnia roboczego. Uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera –		TAK / NIE

		dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. 2. Serwis świadczony w języku polskim (obsługa jak i zgłoszenia). 3. Zgłoszenia serwisowe realizowane poprzez nr telefonu, adres email oraz poprzez formularz zgłoszeniowy producenta komputera online. W formularzu ofertowym należy podać nr telefonu, adres email oraz link www do formularza online (Zamawiający będzie weryfikował wszystkie 3 formy zgłoszeń).		
15.	**Wsparcie techniczne producenta**	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: − weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć), − czasu obowiązywania i typ udzielonej gwarancji. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera.		TAK / NIE
16.	**Wymagania dodatkowe**	Wbudowane (minimum): DisplayPort,1 x HDMI IN/OUT, 7 x USB 3.2 (z czego jeden umożliwiający szybkie ładowanie urządzeń zewnętrznych/podłączanych nawet przy wyłączonym komputerze), 1 x RJ 45 (LAN), 1 x wyjście na słuchawki i mikrofon (Combo), Wśród portów USB wymaga się, aby przynajmniej jeden port był w standardzie USB-C 3.2 Gen 2. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Klawiatura USB w układzie polskim programisty (104 klawisze) z kablem o długości min. 1,8 m. Kolor czarny. Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m. Kolor czarny. Nagrywarka SATA DVD +/-RW SLIM.		TAK / NIE
17.	**Funkcje zdalnego sprzętowego zarządzania komputerami**	1. Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym (tzw. out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia		TAK / NIE

		komputera podczas pracy na zasilaczu sieciowym AC. Wymagana jest obsługa funkcji zdalnego zarządzania przez wbudowane w komputer porty zarówno sieci przewodowej LAN, jak i bezprzewodowej WLAN (jeśli komputer jest wyposażony we wbudowaną kartę WLAN/WiFi), z wykorzystaniem protokołów TCP/IP w tym IPv6 wraz z szyfracją komunikacji zarządzania z protokołem TLS 1.2 z silnymi zestawami szyfrów TLS_RSA_WITH_AES_256_CBC_SHA (minimalna długość klucza 256 bitów) oraz TLS_RSA_WITH_AES_128_GCM_SHA256 lub silniejszymi/nowocześniejszymi. Obsługa wyłącznie protokołów TLS 1.0 i TLS 1.1 - bez ogsługi TLS 1.2 oraz słabych/przestarzałych zestawów szyfrów dla TLS 1.2: TLS_RSA_WITH_NULL_SHA, TLS_RSA_WITH_NULL_SHA256, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA jest NIEWYSTARCZAJĄCA. Technologia ta powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/). 2. Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym musi obsługiwać łącznie wszystkie następujące funkcje: monitorowanie konfiguracji komponentów komputera – model komputera i jego nr seryjny, model procesora, ilość i rodzaj modułów pamięci RAM, rodzaj i nr seryjny dysku HDD/SSD, wersja BIOS płyty głównej, nr seryjny płyty głównej: a) kontrolę zasilania komputera pozwalającą na sprawdzenie aktualnego stanu zasilania komputera (stany ACPI S0/S3/S4/S5) oraz funkcja zdalnego włączenia komputera/komputerów ze stanu pełnego wyłączenia, hibernacji lub uśpienia oraz zdalne zarządzanie stanem zasilania komputera: włączenie/wyłączenie/reset bez udziału systemu operacyjnego, b) zdalne wystartowanie komputera z alternatywnego obrazu systemu operacyjnego w postaci obrazu nośnika CD/DVD - pliku .iso lub nośnika USB - pliku .img montowanego zdalnie z konsoli zarządzania w tym zdalną reinstalację systemu operacyjnego z użyciem obrazu standardowego nośnika instalacyjnego zapewnianego przez producenta systemu operacyjnego, bez pomocy, interakcji ze strony użytkownika końcowego, c) zdalną konfigurację ustawień BIOS Setup,		

		d) sprzętową kopię logu zdarzeń sprzętowych BIOS HW Event Log - zawierającego obsługiwane przez BIOS FW zdarzenia np. brak pamięci RAM w czasie inicjalizacji komputera lub brak dysku startowego uniemożliwiający załadowanie OS oraz informację o błędach samej technologii zarządzania sprzętowego np. wielokrotne nieudane próby logowania do tej technologii (tzw. Brute force atack), e) zapis i przechowywanie dodatkowych informacji oraz zdalny odczyt i zapis tych informacji również z wyłączonego komputera z wbudowanej dodatkowej pamięci nieulotnej o minimalnym rozmiarze 128 KB. Informacje te mogą zawierać dowolne dane np. o wersji zainstalowanego oprogramowania, zainstalowane uaktualnienia itp. które dodatkowe oprogramowanie pracujące na komputerze zarządzanym może pobrać z poziomu systemu operacyjnego i zapisać lokalnie w tej pamięci nieulotnej (NVM), f) zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 2560×1600 (WQXGA) włącznie. Funkcja przekierowania konsoli graficznej musi przechwytywać każdy rodzaj wyświetlanego na fizycznym lokalnym ekranie obrazu włącznie z procesem uruchamiaina komputera (POST), ładowania OS, zamykania OS oraz błędów OS BSOD (Blue Screen of Death), g) wbudowany sprzętowo log operacji zdalnego zarządzania (tzw. Security Audit Log), przechowujący informacje o wykorzystaniu funkcji technologii zdalnego zarządzania z informacją o dacie, czasie rodzaju operacji i koncie użytkownika zdalnego zarządzania który wykonał daną operacje, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego, h) obsługa niskopoziomowej autentykacje sieciowej z użyciem protokołu 802.1x (Radius) na poziomie sprzętu w celu uzyskania dostępu do sieci zabezpieczonej protokołem IEEE 802.1x, niezależnie od stanu czy obecności systemu operacyjnego oraz stanu zasilania komputera, niezależnie od takiej obsługi na poziomie systemu operacyjnego, odpowiednio dla wbudowanych interfejsów LAN i WLAN, i) automatyczne nawiązywanie zdalnego szyfrowanego protokołem MTLS połączenia z predefiniowanym serwerem zarządzającym		

		poprzez sieć Internet, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia sprzętowego (np. otwarcie obudowy z czujnikiem lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; Połączenie MTLS musi obsługiwać te same minimalne wymagania bezpieczeństwa które są wymagane dla szyfracji TLS w pkt. 1. 3. Domyślna konfiguracja fabryczna, zdalna konfiguracja funkcji zarządzania sprzętowego, narzędzia zarządzające: a) W domyślnej konfiguracji fabrycznej (factory default) funkcji zarządzania sprzętowego zdalny dostęp do funkcji zarządzania sprzętowego musi być zablokowany. Dopuszcza się możliwość wstępnej konfiguracji technologii zarządzania sprzętowego przez producenta komputera lub dostawcę wyłącznie na wyraźne życzenie zamawiającego wraz z ustawieniem haseł lokalnego (BIOS FW) i zdalnego (po sieci LAN/WLAN) dostępu do tej technologii na silne hasła zdefiniowane przez Zamawiającego. W procesie konfiguracji funkcji zdalnego zarządzania sprzętowego musi zostać wymuszona zmiana domyślnych haseł dostępu zdalnego na silne hasła zdefiniowane przez administratorów IT Zamawiającego, b) Zdalna konfiguracja ustawień funkcji zarządzania sprzętowego (rodzaju autentykacji, kont zdalnego zarządzania i ich list kontroli dostępu, szyfracji komunikacji, autentykacji 802.1x) musi być możliwa na wielu komputerach jednocześnie, poprzez sieć LAN i WLAN bez potrzeby manualnego dostępu do konfigurowanych komputerów. Narzędzia/oprogramowanie zdalnej konfiguracja ustawień funkcji zarządzania sprzętowego musi dokonywać konfiguracji tej technologii w sposób bezpieczny z wykorzystaniem szyfrowanego połączenia MTLS z certyfikatem serwera konfigurującego wystawionym przez następujące publiczne centra certyfikacji GoDaddy, Comodo, Entrust lub DigiCert i musi obsługiwać te same minimalne wymagania bezpieczeństwa które są wymagane dla szyfracji TLS w pkt. 1. Wykonawca dostarczy odpowiedni certyfikat ważny 60 miesięcy, c) Dostawca musi dostarczyć produkcyjne narzędzia/oprogramowanie służące do konfiguracji ustawień funkcji zarządzania sprzętowego oraz narzędzia do zdalnego zarządzania komputerami z użyciem funkcji zdalnego zarządzania sprzętowego wraz z bezpłatną licencją, dokumentacją jego użycia oraz bezpłatnym wsparciem technicznym lub		

		zawrzeć koszty takiego narzędzia i wsparcia technicznego w kosztach oferty. Dostawca może zamiast dostarczać ww. narzędzia i wsparcie techniczne wskazać publicznie dostępne narzędzie/oprogramowanie lub usługę chmurową z bezpłatną licencja i bezpłatne wsparcie techniczne oferowane przez producenta komputera lub producenta technologii zdalnego zarządzania sprzętowego. Narzędzia o charakterze nieprodukcyjnym (ewaluacyjnym, demo, testowym, wersje alfa/beta) lub posiadające ograniczenia ilości konfigurowanych i zarządzanych komputerów są niedopuszczalne. 4. Aktualizacja zabezpieczeń funkcji zdalnego zarządzania sprzętowego. Wymagane jest zapewnienie publicznie dostępnych bezpłatnych możliwości oraz bezpłatnych narzędzi do aktualizacji zabezpieczeń oprogramowania układowego (firmware) realizującego funkcje zdalnego zarządzania sprzętowego. Aktualizacje (nowy obraz oprogramowania firmware oraz narzędzia aktualizacji) mogą być dostarczane przez Wykonawcę, bezpośrednio przez producenta komputera lub bezpośrednio przez producenta technologii zdalnego zarządzania sprzętowego. Wymagane jest wskazanie przez dostawcę publicznego sposobu publikacji informacji o wykrytych podatnościach bezpieczeństwa technologii zdalnego zarządzania sprzętowego oraz sposobu dostępu i wykonania tych aktualizacji – np. przez podanie linku URL/strony WWW publicznie dostępnego portalu, gdzie udostępniane są takie informacje oraz aktualizacje. Preferowanym sposobem aktualizacji jest obsługiwany przez MS Windows 10 tzw. UEFI Capsule Firmware Update https://docs.microsoft.com/pl-pl/windows-hardware/drivers/bringup/windows-uefi-firmware-update-platform 5. Testy weryfikujące spełnianie przez oferowane komputery wymogów dotyczących funkcji zdalnego sprzętowego zarządzania komputerami. Zamawiający zastrzega sobie prawo do żądania przeprowadzenia na wezwanie demonstracji działania zaoferowanego rozwiązania zdalnego, sprzętowego zarządzania wraz z obsługą ww. wymaganych funkcji przez dostawcę na koszt dostawcy oraz możliwość przeprowadzenia takich testów we własnym zakresie. W tym celu dostawca będzie zobowiązany do bezpłatnego dostarczenia przed podpisaniem umowy po jednej sztuce każdego z oferowanych modeli komputerów w celu		

		przeprowadzenia testów przez Zamawiającego. Po przeprowadzeniu testów Zamawiający zwróci Dostawcy testowane komputery lub zaliczy dostarczone modele na poczet częściowej dostawy zamówionych komputerów. 6. Zgodność oferowanej i dostarczonej technologii zarządzania i monitorowania komputerami na poziomie sprzętowym z istniejącym środowiskiem zamawiającego. Wymagana jest pełna zgodność technologii zarządzania i monitorowania komputerami na poziomie sprzętowym w oferowanych i dostarczonych komputerach na poziomie mechanizmów konfiguracji i zarządzania z już zaimplementowanym w środowisku Zamawiającego rozwiązaniem opartym o oprogramowanie Intel® Setup and Configuration Software (Intel® SCS) w wersji 12.2.0.152 oraz Intel® Manageability Commander w wersji 2.1.133 lub nowszymi używanym obecnie do konfiguracji i zarządzania ponad 2000 komputerów. Wymagana jest też pełna zgodność na poziomie mechanizmów konfiguracji i zarządzania przez sieć Internet dla komputerów przeznaczonych do pracy zdalnej z domu z planowanym do wdrożenia rozwiązaniem opartym o Intel® Endpoint Management Assistant (Intel® EMA) w wersji 1.4 lub nowszej. 7. Instalacja i konfiguracja konsoli zdalnego dostępu do komputerów.		
18.	**Zakres prac**	Dostarczenie, wniesienie urządzeń, rozstawienie urządzeń w miejscach wskazanych przez Zamawiającego. Konfiguracja urządzeń. Instalacja wymaganego oprogramowania.		TAK / NIE

7. W Załączniku nr 1 (Szczegółowy Opis Przedmiotu Zamówienia) w ZADANIU NR 1 – PARAMETRY MINIMALNE DOSTAWY SPRZĘTU – OPROGRAMOWANIE SYSTEMOWE DO KOMPUTERÓW – 150 szt. było:

OPROGRAMOWANIE SYSTEMOWE DO KOMPUTERÓW - 150 szt.				
Lp.	**Element konfiguracji**	**Wymagania minimalne / warunek konieczny**	**Oferowane parametry (podać)**	**Potwierdzenie spełnienia minimalnych wymagań**
1.	**Oprogramowanie systemowe komputerów**	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na		TAK / NIE

		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 tylko do uruchamiania wybranej aplikacji - tryb „kiosk”. 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 – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 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. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 24. Wbudowany mechanizm wirtualizacji typu hypervisor. 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 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. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM. 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot). 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN, e. Certyfikat/Klucz i uwierzytelnienie biometryczne. 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.		

		43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.		

8. W Załączniku nr 1 (Szczegółowy Opis Przedmiotu Zamówienia) w ZADANIU NR 1 – PARAMETRY MINIMALNE DOSTAWY SPRZĘTU – OPROGRAMOWANIE SYSTEMOWE DO KOMPUTERÓW – 150 szt. było:

OPROGRAMOWANIE SYSTEMOWE DO KOMPUTERÓW - 150 szt.				
Lp.	**Element konfiguracji**	**Wymagania minimalne / warunek konieczny**	**Oferowane parametry (podać)**	**Potwierdzenie spełnienia minimalnych wymagań**
2.	**Oprogramowanie systemowe komputerów**	System operacyjny co najmniej Windows 10 Pro 64-bitowy w polskiej wersji językowej lub system równoważny wraz z nośnikiem instalacyjnym. Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w 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		TAK / NIE

		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 tylko do uruchamiania wybranej aplikacji - tryb „kiosk”. 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 – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 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. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 24. Wbudowany mechanizm wirtualizacji typu hypervisor. 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 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. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM. 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych.		

		35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot). 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN, e. Certyfikat/Klucz i uwierzytelnienie biometryczne. 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń. 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń.		

Zmodyfikowana treść SWZ została zamieszczona na stronie internetowej prowadzonego postępowania pod adresem https://e-propublico.pl w dniu 20/02/2023 r.

Dyrektor
SPZZOZ w Nisku

Paweł Tofil

/podpisano elektronicznie/