Załącznik nr 1b) do Opisu przedmiotu zamówienia

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zadania: Dostawa wyposażenia do pracowni multimedialnej w Centrum Kultury w Kamiennej Górze

Część 2 zamówienia: Dostawa sprzętu komputerowego wraz z oprogramowaniem do pracowni multimedialnej

CPV:

30 20 00 00 – 1 Urządzenia komputerowe

30 21 33 00 – 8 Komputer biurkowy

30 21 32 00 – 7 Komputer tablet

30 23 72 80 – 5 Akcesoria zasilające

48 00 00 00 -8 Pakiety oprogramowania i systemy komputerowe

Przedmiotem zamówienia w zakresie części 2 jest dostawa:

1. słuchawek z mikrofonem – 7 szt.,
2. routera – 1 szt.,
3. splitera – 1 szt.,
4. tableta – 1 szt.,
5. zasilacza awaryjnego UPS – 7 szt.,
6. oprogramowania – pakiet obróbki video – 1 szt.,
7. oprogramowania – pakiet graficzno – fotograficzny – 1 szt.,
8. komputera lidera z oprogramowaniem biurowym – 1 szt.,
9. komputera grafika z oprogramowaniem biurowym – 1 szt.,
10. komputer adepta z oprogramowaniem biurowym – 6 szt.

o niżej określonych parametrach.

SŁUCHAWKI Z MIKROFONEM

Minimalne parametry sprzętowe słuchawek z mikrofonem:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Słuchawki	
Czułość [dB]	95
Impedancja [Ω]	32
Pasmo przenoszenia min. [Hz]	42
Pasmo przenoszenia max. [Hz]	17 000
Typ	Nauszne
Mikrofon	
Czułość [dB]	-40
Pasmo przenoszenia min. [Hz]	90
Pasmo przenoszenia max. [Hz]	15 000
Aktywna redukcja szumów	Tak
Ogólne	
Złącze	2×3.5 mm
Długość kabla min. [m]	2
Okres gwarancji	min. 24 miesiące gwarancji producenta na urządzenie

ROUTER

Minimalne parametry sprzętowe routera:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Zakres częstotliwości [GHz]	2.4, 5
Typ anteny	4 × antena dookólna – zewnętrzna 1 × antena wewnętrzna
Standardy	IEEE 802.11 b/g/n @ 2.4 GHz IEEE 802.11 a/n/ac @ 5 GHz
Prędkość transmisji [Mb/s]	300 + 867
Porty LAN	4 × 10/100/1000 Mbps LAN 1 × 1/10/100/1000 Mbps Uplink
Kontrolki LED	Power, 2.4 GHz WLAN, 5 GHz WLAN, 4 × Ethernet, WAN, WPS
Czułość odbiornika	2. GHz: 11 g 5M: -78 dBm 11 n HT20: -74 dBm 11 n HT40: -71 dBm 5 GHz: 11a 6M: -93 dBM 11a 54M: -78 dBm

	11ac HT20: -69 dBm 11ac HT40: -65dBm 11ac HT80: -62dBm
Zabezpieczenia	WEO 64/128-bit, WPA/WPA2, WPA-PSK/WPA2-PSK, ochrona prze atakami DoS, zapora sieciowa SPI, filtrowanie domen, adresów IP i MAC, wiązanie adresów IP i MAC
Moc nadajnika	max. 20 dBm @ 2.4GHz max. 23 dBm @ 5GHz
Zasilanie:	12 V DC/ 1 A (zasilacz w komplecie)
Okres gwarancji	min. 24 miesiące gwarancji producenta na urządzenie

SPLITER

Minimalne parametry sprzętowe spliter (switch sieciowy):

Nazwa komponentu	Wymagane minimalne parametry techniczne
Szybkość transmisji	1 Gbit/s
Ilość portów	10/100/100 Mbit/s 16×
Auto-Uplink na każdym porcie	Tak
Interfejsy (komputerowe/multimedialne)	RJ45
Przyłącza	16 Port RJ45
Okres gwarancji	min. 24 miesiące gwarancji producenta na urządzenie

TABLET

Minimalne parametry sprzętowe tableta:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Przekątna wyświetlacza/ rozdzielczość	39,6 cm (15,6”) / Full HD (1920 × 1080)
Technologia wyświetlacza	a-Si Active Matrix TFT LCD - IPS
Kąt widzenia	176˚
Kontrast/ czas reakcji	1000:1 / 25 ms
Współczynnik proporcji/ jasność	16:9 / 210 cd/m2
Odwzorowanie kolorów	16,7 mln (8 bitów), 72% NTSC (CIE1931)
Połączenia	Przewód 3 w 1
Pióro	Niewymagające baterii, z dwoma konfigurowalnymi przyciskami bocznymi i 8192 poziomami nacisku zarówno końcówki pióra jak i gumki (opatentowana metoda z użyciem rezonansu elektromagnetycznego)
Okres gwarancji	min. 24 miesiące gwarancji producenta na urządzenie

ZASILACZ AWARYJNY UPS

Minimalne parametry sprzętowe UPS:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ obudowy	Tower
Moc pozorna	750 VA
Moc skuteczna	500 W
Napięcie wyjściowe	151 - 302 V
Kształt napięcia wyjściowego	Sinusoidalny
Czas przełączania	6 ms
Złącza wyjściowe	6 × IEC 320 C13
Czas podtrzymania przy 50% obciążeniu	min. 15 min
Czas podtrzymania przy 100% obciążeniu	min. 4 min
Średni czas ładowania	3 h
Sygnalizacja pracy	Dźwiękowa, wskaźniki LED, wyświetlacz LCD
Porty komunikacyjne	Min. 1x USB, RJ-45

Zabezpieczenia	Przeciwzwarciowe, przeciążeniowe, przeciwprzepięciowe, termiczne
Okres gwarancji	min. 24 miesiące gwarancji producenta na urządzenie, min. 24 miesiące gwarancji producenta na akumulator.

OPROGRAMOWANIE – PAKIET OBRÓBKI VIDEO

Program do tworzenia filmów (**Corel Draw Video Studio Pro)**.
Program musi umożliwiać co najmniej korzystanie z następujących funkcji:

- przygotowanie animacji za pomocą funkcji animacji poklatkowej,
- łączenie i edytowanie materiałów zarejestrowany za pomocą min. 4 kamer,
- dodawanie tekstu lub grafiki podążającej za wybranym ruchomym obiektem,
- edycja filmu na min. 24-ścieżkowej osi czasu z dokładnością co do jednej klatki w jakości HD i 3D,
- precyzyjne przycinanie klipów oraz dodawanie efektów i przejść w wybrane miejsce,
- możliwość wyboru min. 1000 efektów specjalnych 2D i 3D,
- ustawianie przezroczystości ścieżek,
- dodawanie i dopasowywanie ścieżki dźwiękowej,
- automatyczne wyciszanie dźwięków tła, aby lepiej było słychać dialogi.

W opisie przedmiotów zamówienia użyto nazw producentów (licencjodawców) z następujących przyczyn:

a) Zamawiający planuje wykorzystanie określonych produktów z serii CorelDRAW, od jednego z wiodących producentów oprogramowania w branży.
b) Utrzymanie jednolitego standardu i użytkowanie konkretnego oprogramowania jest kluczowe dla Zamawiającego, gdyż ewentualne zmiany łączyłyby się dodatkowym kosztem obsługi nowego oprogramowania, związanym m.in. z instalacją, szkoleniem itp.
c) Szczegółowy opis funkcjonalny lub opis cech jest zbyt złożony, by można było określić go w dostatecznie dokładny a zarazem zwięzły sposób.
d) Zamawiający dopuszcza produkty - licencje równoważne pod warunkiem zgodności innego produktu pod względem funkcjonalnym (zakres operacji) i obsługi (menu) opisanych w powyżej, oraz takich które nie wymagają ponownej instalacji.

OPROGRAMOWANIE – PAKIET GRAFICZNO – FOTOGRAFICZNY

Oprogramowanie graficzne (**Corel Draw Suite**).
Program do projektowania graficznego, edycji zdjęć oraz tworzenia logotypów, broszur, grafik internetowych, reklam do serwisów społecznościowych i innych projektów.
Oprogramowanie musi umożliwiać co najmniej:

- dostosowanie obszaru roboczego do indywidualnych potrzeb poprzez zmianę wyglądu często używanych elementów,
- pracę z wykorzystaniem rysika w czasie rzeczywistym,
- ukrywanie i pokazywanie poszczególnych obiektów bądź ich grup znajdujących się na warstwie bez konieczności ukrycia całej warstwy,
- kopiowanie, wklejanie i duplikowanie części istniejących krzywych z możliwością ponownego wykorzystania segmentów krzywych w tworzonych projektach,
- usuwanie niedoskonałości przez nakładanie otaczających kolorów i tekstur.

W opisie przedmiotów zamówienia użyto nazw producentów (licencjodawców) z następujących przyczyn:

a) Zamawiający planuje wykorzystanie określonych produktów z serii CorelDRAW, od jednego z wiodących producentów oprogramowania w branży.

b) Utrzymanie jednolitego standardu i użytkowanie konkretnego oprogramowania jest kluczowe dla Zamawiającego, gdyż ewentualne zmiany łączyłyby się dodatkowym kosztem obsługi nowego oprogramowania, związanym m.in. z instalacją, szkoleniem itp.
c) Szczegółowy opis funkcjonalny lub opis cech jest zbyt złożony, by można było określić go w dostatecznie dokładny a zarazem zwięzły sposób.
d) Zamawiający dopuszcza produkty - licencje równoważne pod warunkiem zgodności innego produktu pod względem funkcjonalnym (zakres operacji) i obsługi (menu) opisanych w powyżej, oraz takich które nie wymagają ponownej instalacji.

KOMPUTER LIDERA i GRAFIKA

Nazwa	Wymagane minimalne parametry techniczne	
Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie nowy i wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.	
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, programów graficznych i dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.	
Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 17400 punktów według wyników ze strony https://www.cpubenchmark.net. Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.	
Pamięć RAM	16GB DDR4 możliwość rozbudowy do 64GB, jeden slot wolny.	
Pamięć masowa	512GB SSD M.2 NVMe. Możliwość instalacji dodatkowego dysku twardego.	
Wydajność grafiki	Dedykowany układ graficzny z własną pamięcią min. 3GB GDDR5 osiągająca w teście PassMark Video card wynik min. 5200 punktów według wyników ze strony https://www.cpubenchmark.net.	
Matryca	Rozmiar matrycy / plamki	min.23,8” / max. 0,275mm
	Rozdzielczość	FHD (1920x1080)
	Jasność typowa	min. 250 cd/m²
	Kontrast typowy	700:1
	Barwa koloru (typowa)	72% NTSC
	Kąty Horizontal/Vertical	178(+/- 89) / 178 (+/-89)
	Rodzaj matrycy	Matowa IPS
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP z diodą LED informującą użytkownika o pracy. Mechaniczna chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy). Wbudowane w obudowę dwa mikrofony.	
Obudowa	Typu All-in-One zintegrowana z monitorem min. 24”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100,	

	Suma wymiarów obudowy z zainstalowanym standem nie może przekraczać: 114 cm Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 94 cm Zasilacz wewnętrzny o mocy min. 220W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80 plus Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa jednostki typu All – in – One musi umożliwiać: Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. Regulację wysokości w zakresie minimum 10 cm. Ustawienie jednostki w trybie Pivot. Obrót podstawy w lewą oraz prawą stronę.
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).
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 min.: – 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, – 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/).
Bezpieczeństwo	Płyta główna zawierająca 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. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.

	Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: – administratora [hasło nadrzędne], – użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej. Możliwość włączenia/wyłączenia kontrolera SATA. Możliwość włączenia/wyłączenia kontrolera audio. Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych. Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy. Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [musi umożliwiać znaki specjalne (@#$%^)] Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach: codziennie lub w wybrane dni tygodnia. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty) Certyfikat ISO 50001 dla producenta sprzętu Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram

	Certyfikat TCO - do oferty załączyć certyfikat lub wydruk ze strony http://tcocertified.com/product-finder/
System operacyjny	Zainstalowany system operacyjny równoważny do Windows 10 Professional, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Pakiet biurowy obejmujący co najmniej: edytor tekstu, arkusz kalkulacyjny, program do prezentacji, klient poczty. W ofercie należy podać pełna nazwę oferowanego oprogramowania.
Wymagania dodatkowe	Wbudowane porty: 1 × DP++ 1.4/HDCP 2.3 port (rear) 1 × USB 3.2 Gen 2 Type-C port 3 × USB 3.2 Gen 1 Type-A port 2 × USB 2.0 Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp. 1 × Universal audio jack 1 × One Line-out audio 1 × RJ-45 port 10/100/1000 Mbps Czytnik kart SD 4.0 Karta WiFi ac+ bluetooth 5 Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącze M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi Czytnik kart multimedialnych SD 4 Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Nagrywarka DVD +/-RW wbudowana w obudowie lub w podstawie standu
Bezpieczeństwo i oprogramowanie dodatkowe	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją 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, – sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, – dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne, – włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, – sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania), – dostęp do wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml, – dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml

	Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać pełną nazwę oferowanego oprogramowania System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: – wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, – wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, – stosowanie kwarantanny, – wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear), – skanowanie urządzeń USB natychmiast po podłączeniu, – automatyczne odłączanie zainfekowanej końcówki od sieci, – skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji, – zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach, – musi posiadać moduł ochrony IDS/IPS, – musi posiadać mechanizm wykrywania skanowania portów, – musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów, – moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości. Szyfrowanie danych: – oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows, – zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

	Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przed niezamierzonymi manipulacjami – ataki ransomware. Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: – Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli, – Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory, – Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux, – Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. – Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich, – Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji. Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach. 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury. 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur. 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy. 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach. 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń. 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer. 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: – różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie, – funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD , – funkcje regulowania połączeń WiFi i Bluetooth,

	– funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe, – funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi, – funkcje blokowania dostępu dowolnemu urządzeniu, – możliwość tymczasowego dodania dostępu do urządzenia przez administratora, – zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu, – możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka, – możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora, – możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry, – możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich, – funkcję wirtualnej klawiatury, – możliwość blokowania każdej aplikacji , – możliwość zablokowania aplikacji w oparciu o kategorie, – możliwość dodania własnych aplikacji do listy zablokowanych, – zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze, – dodawanie innych aplikacji, – dodawanie aplikacji w formie portable, – możliwość wyboru pojedynczej aplikacji w konkretnej wersji , – dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB, – kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool, – możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki, – możliwość zablokowania funkcji Printscreen, – funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx, – funkcje monitorowania i kontroli przepływu poufnych informacji, – możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików, – możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj, – możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe, – ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe, – ochrona zawartości schowka systemu, – ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL, – możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych, – ochrona plików zamkniętych w archiwach , – Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem, – możliwość tworzenia profilu DLP dla każdej polityki,

	– wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania, – ochrona przez wyciekiem plików poprzez programy typu p2p. Monitorowanie zmian w plikach: – możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych, – funkcje monitorowania określonych rodzajów plików, – możliwość wykluczenia określonych plików/folderów dla procedury monitorowania, – generator raportów do funkcjonalności monitora zmian w plikach, – możliwość śledzenia zmian we wszystkich plikach, – możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach, – możliwość definiowana własnych typów plików. Optymalizacja systemu operacyjnego stacji klienckich: – usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku, – optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem, – możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich, – instruktaż stanowiskowy pracowników Zamawiającego, – dokumentacja techniczna w języku polskim. Wspierane platformy i systemy operacyjne: 1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit), 2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit), 3. Mac OS X, Mac OS 10, 4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat. Platforma do zarządzania dla Android i iOS: – musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę, – funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem – musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email, – musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika, – musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi, – musi posiadać możliwość eksportu danych użytkownika. Zarządzanie urządzeniem – musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO, – musi umożliwiać import listy urządzeń z pliku CSV, – musi umożliwiać dodanie urządzeń prywatnych oraz firmowych, – musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta,

	– musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał, – musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres, – musi zawierać podgląd aktualnie zainstalowanych aplikacji, – musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, – musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł, – moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres. Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową. 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących. 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie. 6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów, b) zablokowania możliwości zmiany konfiguracji widgetów, c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów, d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności, e) eksport wszystkich skanów podatności do pliku CSV.
Warunki gwarancji Wsparcie techniczne	Min. 2-letnia gwarancja producenta świadczona na miejscu u klienta. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera.

	Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

KOMPUTER ADEPTA

Nazwa	Wymagane minimalne parametry techniczne	
Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie nowy i wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.	
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, programów graficznych i dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna	
Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 17400 punktów według wyników ze strony https://www.cpubenchmark.net Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego	
Pamięć RAM	8GB DDR4 możliwość rozbudowy do 64GB, jeden slot wolny.	
Pamięć masowa	256GB SSD M.2 NVMe Możliwość instalacji dodatkowego dysku twardego	
Wydajność grafiki	Dedykowany układ graficzny z własną pamięcią min. 3GB GDDR5 osiągająca w teście PassMark Video card wynik min. 5200 punktów według wyników ze strony https://www.cpubenchmark.net	
Matryca	Rozmiar matrycy / plamki	min.23,8” / max. 0,275mm
	Rozdzielczość	FHD (1920x1080)
	Jasność typowa	min. 250 cd/m²
	Kontrast typowy	700:1
	Barwa koloru (typowa)	72% NTSC
	Kąty Horizontal/Vertical	178(+/- 89) / 178 (+/-89)
	Rodzaj matrycy	Matowa IPS
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP z diodą LED informującą użytkownika o pracy. Mechaniczna chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy). Wbudowane w obudowę dwa mikrofony.	
Obudowa	Typu All-in-One zintegrowana z monitorem min. 24”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100, Suma wymiarów obudowy z zainstalowanym standem nie może przekraczać: 114 cm Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 94 cm Zasilacz wewnętrzny o mocy min. 220W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%,	

	Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80 plus Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa jednostki typu All – in – One musi umożliwiać: Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. Regulację wysokości w zakresie minimum 10 cm. Ustawienie jednostki w trybie Pivot. Obrót podstawy w lewą oraz prawą stronę.
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).
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 min.: – 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, – 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/).
Bezpieczeństwo	Płyta główna zawierająca 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. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.

BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: – administratora [hasło nadrzędne], – użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej. Możliwość włączenia/wyłączenia kontrolera SATA. Możliwość włączenia/wyłączenia kontrolera audio. Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych. Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy. Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [musi umożliwiać znaki specjalne (@#$%^)] Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach: codziennie lub w wybrane dni tygodnia. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty) Certyfikat ISO 50001 dla producenta sprzętu Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Certyfikat TCO - do oferty załączyć certyfikat lub wydruk ze strony http://tcocertified.com/product-finder/

System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Pakiet biurowy obejmujący co najmniej: edytor tekstu, arkusz kalkulacyjny, program do prezentacji, klient poczty W ofercie należy podać pełną nazwę oferowanego oprogramowania.
Wymagania dodatkowe	Wbudowane porty: 1 × DP++ 1.4/HDCP 2.3 port (rear) 1 × USB 3.2 Gen 2 Type-C port 3 × USB 3.2 Gen 1 Type-A port 2 × USB 2.0 Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp. 1 × Universal audio jack 1 × One Line-out audio 1 × RJ-45 port 10/100/1000 Mbps Czytnik kart SD 4.0 Karta WiFi ac+ bluetooth 5 Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącze M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi Czytnik kart multimedialnych SD 4 Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Nagrywarka DVD +/-RW wbudowana w obudowie lub w podstawie standu
Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją 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, – sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, – dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne, – włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, – sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania), – dostęp do wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml, – dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania

	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: – wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, – wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, – stosowanie kwarantanny, – wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear), – skanowanie urządzeń USB natychmiast po podłączeniu, – automatyczne odłączanie zainfekowanej końcówki od sieci, – skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji, – zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach, – musi posiadać moduł ochrony IDS/IPS, – musi posiadać mechanizm wykrywania skanowania portów, – musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów, – moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości. Szyfrowanie danych: – oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows, – zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.

	Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przed niezamierzonymi manipulacjami – ataki ransomware. Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: – Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli, – Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory, – Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux, – Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. – Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich, – Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji. Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach. 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury. 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur. 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy. 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach. 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń. 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer. 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: – różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie, – funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD , – funkcje regulowania połączeń WiFi i Bluetooth, – funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe, – funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi,

	– funkcje blokowania dostępu dowolnemu urządzeniu, – możliwość tymczasowego dodania dostępu do urządzenia przez administratora, – zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu, – możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka, – możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora, – możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry, – możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich, – funkcję wirtualnej klawiatury, – możliwość blokowania każdej aplikacji , – możliwość zablokowania aplikacji w oparciu o kategorie, – możliwość dodania własnych aplikacji do listy zablokowanych, – zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze, – dodawanie innych aplikacji, – dodawanie aplikacji w formie portable, – możliwość wyboru pojedynczej aplikacji w konkretnej wersji , – dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB, – kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool, – możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki, – możliwość zablokowania funkcji Printscreen, – funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx, – funkcje monitorowania i kontroli przepływu poufnych informacji, – możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików, – możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj, – możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe, – ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe, – ochrona zawartości schowka systemu, – ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL, – możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych, – ochrona plików zamkniętych w archiwach , – Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem, – możliwość tworzenia profilu DLP dla każdej polityki, – wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania, – ochrona przez wyciekiem plików poprzez programy typu p2p. Monitorowanie zmian w plikach:

	– możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych, – funkcje monitorowania określonych rodzajów plików, – możliwość wykluczenia określonych plików/folderów dla procedury monitorowania, – generator raportów do funkcjonalności monitora zmian w plikach, – możliwość śledzenia zmian we wszystkich plikach, – możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach, – możliwość definiowana własnych typów plików. Optymalizacja systemu operacyjnego stacji klienckich: – usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku, – optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem, – możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich, – instruktaż stanowiskowy pracowników Zamawiającego, – dokumentacja techniczna w języku polskim. Wspierane platformy i systemy operacyjne: 1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit), 2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit), 3. Mac OS X, Mac OS 10, 4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat. Platforma do zarządzania dla Android i iOS: – musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę, – funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem – musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email, – musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika, – musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi, – musi posiadać możliwość eksportu danych użytkownika. Zarządzanie urządzeniem – musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO, – musi umożliwiać import listy urządzeń z pliku CSV, – musi umożliwiać dodanie urządzeń prywatnych oraz firmowych, – musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta, – musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał, – musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres, – musi zawierać podgląd aktualnie zainstalowanych aplikacji,

	– musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, – musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł, – moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres. Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową. 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących. 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie. 6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: f) przegląd wybranych danych na podstawie konfigurowalnych widgetów, g) zablokowania możliwości zmiany konfiguracji widgetów, h) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów, i) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności, j) eksport wszystkich skanów podatności do pliku CSV.
Warunki gwarancji Wsparcie techniczne	nin. 2-letnia gwarancja producenta świadczona na miejscu u klienta. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.