



## Załącznik nr 2 do SWZ

### Opis przedmiotu zamówienia:

1. Przedmiotem zamówienia jest: **„Dostawa sprzętu komputerowego do wyposażenia pracowni kształcenia zawodowego branży HGT w PZS nr 2 w Kościerzynie”** w ramach projektu „Nowoczesna edukacja zawodowa w Sercu Kaszub II” współfinansowanego ze środków Europejskiego Funduszu Społecznego + w ramach programu Fundusze Europejskie dla Pomorza 2021-2027, Działanie 5.8. Edukacja Ogólna i zawodowa.
2. Przedmiot zamówienia obejmuje:
  - a. dostawę (na koszt i ryzyko Wykonawcy)
  - b. uruchomienie i sprawdzenie prawidłowości działania dostarczonych urządzeń i narzędzi (jeżeli dotyczy),
  - c. zapewnienia obsługi serwisowej przedmiotu dostawy w ramach udzielonej gwarancji.
3. Miejsce dostawy: Powiatowy Zespół Szkół nr 2, ul. Wybickiego 1, 83-400 Kościerzyna.
4. **Sprzęt stanowiący przedmiot zamówienia musi być profesjonalny i fabrycznie nowy, należytej jakości, sprawny, wolny od jakichkolwiek wad fizycznych, jak również od jakichkolwiek wad prawnych i roszczeń osób trzecich, nie używany, nie powystawowy.** Pod pojęciem fabrycznie nowy Zamawiający rozumie produkty wykonane z nowych elementów, bez śladu uszkodzenia, w oryginalnych nieotwieranych i fabrycznie zabezpieczonych opakowaniach producenta, np. z widocznym logo, symbolem produktu i terminem przydatności do użytku. Zamawiający nie zezwala na ingerencję w podzespoły i modyfikację sprzętu skonfigurowanego przez producenta przed dostawą. Wymagane podzespoły i wyposażenie muszą być fabrycznie wbudowane przez producenta. Dostarczony sprzęt musi zawierać wszystkie części niezbędne do funkcjonowania, uruchomienia i montażu, ponadto elementy w ramach zestawów muszą być ze sobą kompatybilne. Dostarczone wyposażenie musi być zgodne z obowiązującymi normami i posiadać wymagane atesty, certyfikaty, aprobaty techniczne, deklaracje zgodności wbudowanych materiałów, świadectwa bezpieczeństwa, homologacje, licencje itp. Ponadto musi mieć możliwość dostosowania do pracy dla osób niepełnosprawnych.
5. Przedmiot zamówienia należy dostarczyć pod wskazany adres, w określonym terminie wraz z wyładunkiem na własny koszt i ryzyko, własnymi siłami, w odliczonych ilościach, zgodnie z SWZ.
6. Przedmiot zamówienia zostanie wykonany zgodnie z wytycznymi w zakresie realizacji zasady równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasady równości szans kobiet i mężczyzn w ramach funduszy unijnych na lata 2021-2027, znajdującymi się na stronie internetowej: <https://www.funduszeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-realizacji-zasad-rownosciowych-w-ramach-funduszy-unijnych-na-lata-2021-2027-1/>
7. Jeżeli gdziekolwiek w SWZ oraz w jego załącznikach pojawia się nazwa, marka lub typ wskazujący na konkretnego producenta, należy to interpretować, że określenie ma jedynie charakter przykładowy, a Wykonawca sporządzając ofertę może uwzględnić wyrób każdego innego producenta, który jest równoważny, tzn. posiada co najmniej takie same lub korzystniejsze parametry jakościowe, funkcje oraz standard wykonania w stosunku do podanych w opisie przedmiotu zamówienia przykładów. Na Wykonawcy spoczywa udowodnienie równoważności zaproponowanego produktu.
8. Oferowany przez Wykonawcę sprzęt musi zapewniać racjonalne i efektywne ceny, niezawyżone w stosunku do cen i stawek rynkowych.
9. Wykonawca w formularzu ofertowym musi wskazać nazwę produktu i numer kodu producenta w celu identyfikacji zaproponowanego sprzętu i sprawdzenia wymaganych w zamówieniu parametrów.



10. **Planowany termin wykonania przedmiotu zamówienia:** Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie od daty zawarcia umowy maksymalnie do dnia 23.12.2024r.
11. **Wymogi dotyczące gwarancji dla przedmiotu zamówienia:**
- 1) Wykonawca udziela Zamawiającemu pisemnej gwarancji jakości na wykonany przedmiot umowy **na okres określony w umowie**. Bieg terminu gwarancji rozpoczyna się w dniu następnym po podpisaniu przez strony protokołu zdawczo-odbiorczego, potwierdzającego wykonanie przedmiotu umowy zgodnie z niniejszą umową.
  - 2) Z tytułu udzielonej gwarancji Wykonawca jest odpowiedzialny wobec Zamawiającego za wady przedmiotu umowy zmniejszające jego wartość lub użyteczność ze względu na cel w umowie określony lub wynikający z przeznaczenia przedmiotu umowy, a w szczególności za rozwiązania niezgodne z obowiązującymi przepisami prawa i normami technicznymi, a także wytycznymi Zamawiającego.
  - 3) W okresie gwarancji Wykonawca zobowiązany będzie, w przypadku wystąpienia awarii, usterki lub wady przedmiotu umowy do:
    - a. bezpłatnej naprawy, jeżeli wada lub usterka powstały nie z winy Zamawiającego (w tym także użytkownika przedmiotu umowy),
    - b. bezpłatnej wymiany w terminie 14 dni kalendarzowych przedmiotu dostawy w przypadku dwukrotnej awarii, jeżeli wada lub usterka powstały nie z winy Zamawiającego (w tym także użytkownika przedmiotu umowy). Wykonawca zobowiązany jest do jego wymiany na nowy o tożsamy lub lepszych parametrach technicznych określonych w SWZ,
    - c. bezpłatnej wymiany w terminie 14 dni kalendarzowych przedmiotu umowy w przypadku stwierdzenia wady lub usterki uniemożliwiającej użytkowanie i naprawę przedmiotu umowy,
    - d. w przypadku wystąpienia konieczności naprawy przedmiotu umowy poza Kościerzyną, Wykonawca zapewni jego odbiór od Zamawiającego, naprawę i dostawę naprawionego przedmiotu umowy na własny koszt, w terminie nieprzekraczającym 25 dni roboczych od dnia odebrania przedmiotu dostawy,
    - e. w przypadku braku możliwości usunięcia awarii, usterki, wady w terminie 25 dni roboczych od dnia odebrania wadliwego przedmiotu umowy od Zamawiającego, Wykonawca zobowiązuje się do dostarczenia i uruchomienia nowego sprzętu zastępczego o parametrach równoważnych z oferowanymi,
  - 4) Wykonawca zapewnia możliwość usunięcia usterki lub awarii przez Zamawiającego po uzyskaniu konsultacji telefonicznej lub za pomocą poczty elektronicznej - jeżeli pozwoli na to charakter usterki lub awarii.
  - 5) Serwis gwarancyjny wykonywany będzie w miejscu dostawy we wszystkie dni robocze, w godzinach uzgodnionych z przedstawicielem Zamawiającego. W przypadku niemożności naprawy przedmiotu zamówienia w miejscu dostawy, Wykonawca zobowiązuje się do odebrania i dostarczenia przedmiotu umowy z i do miejsca dostawy na własny koszt i ryzyko.
  - 6) Maksymalny czas reakcji liczony od momentu zgłoszenia przez Zamawiającego faksem lub drogą mailową o usterce lub awarii do czasu przybycia na miejsce Wykonawcy lub innej osoby upoważnionej, wstępne zdiagnozowanie przyczyny usterki lub awarii i oszacowanie czasu naprawy wyniesie 2 dni robocze.
  - 7) Termin usunięcia awarii, wad i usterek winien być nie dłuższy niż 14 dni roboczych od dnia powiadomienia Wykonawcy telefonicznie, faxem lub drogą elektroniczną o awarii, wadzie lub usterce.
  - 8) W przypadkach, o których mowa w ust. 3 okres gwarancji ulegnie przedłużeniu odpowiednio:
    - a. w przypadku naprawy przedmiotu umowy – o okres wykonywania naprawy,
    - b. w przypadku dokonania wymiany – o okres gwarancji – w stosunku do wymienionego przedmiotu umowy.
  - 9) W okresie gwarancji wszelkie koszty związane z usunięciem awarii, usterek i wad w tym dostarczenie uszkodzonego lub wadliwego przedmiotu umowy do punktu serwisowego, obciążają Wykonawcę.
  - 10) Umowa w części określającej obowiązki Wykonawcy z tytułu gwarancji, po odbiorze przedmiotu umowy, będzie stanowić dokument gwarancyjny w rozumieniu przepisów Kodeksu cywilnego. Podpisanie przez strony bezusterkowego protokołu zdawczo – odbiorczego zamówienia jest jednoznaczne z udzieleniem Zamawiającemu pisemnej gwarancji na całość dostarczonego przedmiotu umowy.



11) Zamawiający zastrzega sobie prawo obciążenia Wykonawcy wszystkimi kosztami usunięcia wad, usterki lub awarii jeśli Wykonawca nie przystąpi do ich usunięcia w terminie określonym w ust. 7.

12. Dla jednoznacznej identyfikacji oferowanego sprzętu należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego sprzętu. Zamawiający wymaga również podania faktycznych parametrów sprzętu, o którym mowa w opisie przedmiotu zamówienia, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany sprzęt spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane urządzenia spełniają wymagania Zamawiającego.

Kod CPV: 39162110-9

Sprzęt dydaktyczny/ urządzenia komputerowe

Kod CPV: 42962000-7

Urządzenia drukujące i graficzne

#### I. Laptopy z oprogramowaniem biurowym i antywirusowym wraz z myszką– 18 szt.

Laptop: komputer mobilny będzie wykorzystywany dla potrzeb sztuk audiowizualnych (film, grafika, materiały wideo) edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.	
Ekran	
Rozmiar	16"
Typ matrycy	matowa
Rodzaj matrycy	LED, IPS
Rozdzielczość ekran	1920 x 1200 pikseli
Częstotliwość odświeżania ekranu	min 60 Hz
Procesor	
Wymagane parametry techniczne	<p>Wynik procesor osiąga w teście Cross Mark Notebook co najmniej 1730 punktów CPU Cross Mark. Dostępny na stronie:</p> <p><a href="https://results.bapco.com/charts/facet/CrossMark/cpu/all/notebook">https://results.bapco.com/charts/facet/CrossMark/cpu/all/notebook</a></p> <p>Wydruk nie starszy niż data publikacji ogłoszenia o zamówieniu tj. 15.11.2024 r.</p> <p><b>Wydruk dołączyć do oferty.</b></p>
Pamięć Ram	
Wymagane parametry techniczne	Min. 16GB DDR4 lub DDR5
Pamięć masowa	
Rodzaj dysku	SSD
Pojemność dysku	min. 512 GB



Karta graficzna	Zintegrowany układ graficzny.
Pozostałe:	
Klawiatura	Klawiatura z podświetleniem, (układ QWERTY) z wydzieloną klawiaturą numeryczną
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo, Wbudowany mikrofon, wbudowana kamera.
Łączność bezprzewodowa	Bluetooth co najmniej wersja 5 Wi-Fi co najmniej wersja 6
Złącza	1port audio typu combo (słuchawki i mikrofon) HDMI – 1 port LAN – 1 port USB - min. 3 porty, w tym co najmniej 1 USB -C (z Thunderbolt 4)
Bateria	min. 50 Wh
Obudowa	kolorystyka czarna lub odcienie szarości
Gwarancja	min 24 miesiące on-site
	<p>Serwis gwarancyjny powinien być zlokalizowany na terytorium RP. W przypadku naprawy realizowanej poza miejscem użytkowania laptopa (opcjonalnie zestawu) wszelkie koszty związane z dostarczeniem laptopa (opcjonalnie zestawu) do serwisu i z powrotem do użytkownika powinny być pokryte przez gwaranta w ramach gwarancji.</p> <p>Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.</p> <p>Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych).</p>
	<p>Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera. 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 wydaniu numeru seryjnego komputera lub modelu komputera.</p>
Waga	Nie powinna przekraczać 2,0 kg
Certyfikaty producenta	<p>Certyfikat ISO 9001 systemu zarządzania jakością lub równoważny w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych.</p> <p>Certyfikat ISO 14001 zarządzania środowiskiem lub równoważny w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych.</p>
Certyfikaty produktu	<p>Deklaracja zgodności UE i oznakowanie CE;</p> <p>Certyfikat TCO lub równoważny odnoszący się do produkcji odpowiedzialnej społecznie i środowiskowo, zdrowia i bezpieczeństwa</p>



	<p>użytkownika, wydajności produktu, przedłużenia żywotności produktu, redukcji niebezpiecznych substancji i odzysku materiałów.</p> <p>Certyfikat EPEAT dla Polski lub innego państwa członkowskiego Unii Europejskiej lub równoważny certyfikat wydany przez akredytowaną instytucję w analogicznym zakresie dot. redukcji niebezpiecznych substancji chemicznych, zrównoważonego wykorzystania zasobów, zarządzania wycofaniem z eksploatacji, łagodzenia zmian klimatu, wydajności korporacyjnej i społecznej.</p>
Bezpieczeństwo	Moduł bezpieczeństwa TPM
System operacyjny	
<p>Zainstalowany system operacyjny Microsoft Windows 11 Professional w polskiej wersji językowej, mające zapewnić funkcjonalność i współpracę ze środowiskiem sieciowym oraz aplikacyjnym funkcjonującym w PZS Nr 2 w Kościerzynie, licencja bezterminowa, jednostanowiskowa. 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.</p> <p>Zamawiający dopuszcza system operacyjny <b>równoważny</b> spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji co najmniej:</p> <ol style="list-style-type: none"><li>1. Dostępny interfejs użytkownika umożliwiający obsługę przy pomocy klawiatury i myszy.</li><li>2. Interfejs użytkownika dostępny co najmniej w języku Polskim i Angielskim,</li><li>3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe,</li><li>4. Wbudowany system pomocy w języku polskim;</li><li>5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,</li><li>6. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.</li><li>7. 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,</li><li>8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,</li><li>9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,</li><li>10. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;</li><li>11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,</li><li>12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play, Wi-Fi),</li><li>13. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,</li><li>14. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,</li><li>15. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,</li><li>16. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</li><li>17. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.</li></ol>	





18. 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,
  19. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
  20. Obsługa standardu NFC (near field communication),
  21. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
  22. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
  23. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
  24. 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),
  25. Mechanizmy wieloelementowego uwierzytelniania.
  26. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
  27. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
  28. Wsparcie dla algorytmów Suite B (RFC 4869),
  29. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej Ipsec,
  30. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
  31. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
  32. Wsparcie dla Jscript i VBScript – możliwość uruchamiania interpretera poleceń,
  33. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
  34. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
  35. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. Quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
  36. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
  37. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
  38. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
  39. 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 np.),
  40. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
  41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
  42. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
  43. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
  44. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
- Zamawiający nie wymaga dostarczenia nośnika z systemem operacyjnym.



<b>Myszka komputerowa</b>	Rozdzielność minimalna: 1000 dpi Technologia wykrywania ruchu: Optyczny Typ przewijania (scroll type): Koło Liczba przycisków: co najmniej 3 Komunikacja z komputerem: przewodowa Profil użytkownika uniwersalny dla prawy i leworęcznych
<b>Pakiet biurowy:</b>	<p>Nowa licencja MS Office LTSC Professional 2024, bezterminowa, nie używana nigdy wcześniej, wieczysta lub <b>równoważne</b> oprogramowanie biurowe, które spełnia następujące wymagania poprzez wbudowane mechanizmy:</p> <ol style="list-style-type: none"><li>1. Licencja przeznaczona dla użytkowników edukacyjnych.</li><li>2. Wymagania odnośnie interfejsu użytkownika - pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na język angielski,</li><li>3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:<ol style="list-style-type: none"><li>3.1. posiada kompletny i publicznie dostępny opis formatu,</li><li>3.2. ma zdefiniowany układ informacji w postaci XML (standard uniwersalnego formatu tekstowego służący do zapisu danych w formie elektronicznej),</li><li>3.3. umożliwia wykorzystanie schematów XML,</li><li>3.4. wspiera w swojej specyfikacji podpis elektroniczny,</li></ol></li><li>4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców,</li><li>5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropolecień, język skryptowy),</li><li>6. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim,</li><li>7. Pakiet zintegrowanych aplikacji biurowych musi zawierać co najmniej:<ol style="list-style-type: none"><li>7.1. edytor tekstów,</li><li>7.2. arkusz kalkulacyjny,</li><li>7.3. narzędzie do przygotowywania i prowadzenia prezentacji,</li><li>7.4. narzędzie do obsługi baz danych,</li><li>7.5. narzędzie do obsługi poczty elektronicznej.</li></ol></li><li>8. Edytor tekstów musi umożliwiać:<ol style="list-style-type: none"><li>8.1. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,</li><li>8.2. wstawianie oraz formatowanie tabel,</li><li>8.3. wstawianie oraz formatowanie obiektów graficznych,</li><li>8.4. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),</li><li>8.5. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,</li><li>8.6. automatyczne tworzenie spisów treści,</li><li>8.7. automatyczne tworzenie spisów treści,</li><li>8.8. formatowanie nagłówek i stopki stron,</li></ol></li></ol>



	<p>8.9. sprawdzanie pisowni w języku polskim,</p> <p>8.10. śledzenie zmian wprowadzonych przez użytkowników,</p> <p>8.11. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,</p> <p>8.12. określenie układu strony (pionowa/pozioma),</p> <p>8.13. wydruk dokumentów,</p> <p>8.14. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,</p> <p>8.15. pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016, 2019, 2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,</p> <p>8.16. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,</p> <p>9. Arkusz kalkulacyjny musi umożliwiać:</p> <p>9.1. tworzenie raportów tabelarycznych,</p> <p>9.2. tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych,</p> <p>9.3. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,</p> <p>9.4. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),</p> <p>9.5. obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.</p> <p>9.6. narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,</p> <p>9.7. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,</p> <p>9.8. wyszukiwanie i zamianę danych,</p> <p>9.9. wykonywanie analiz danych przy użyciu formatowania warunkowego,</p> <p>9) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,</p> <p>9.10. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,</p> <p>9.11. formatowanie czasu, daty i wartości finansowych z polskim formatem,</p> <p>9.12. zapis wielu arkuszy kalkulacyjnych w jednym pliku,</p> <p>9.13. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013, 2016, 2019, 2021 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.</p> <p>9.14. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.</p> <p>10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <p>10.1. przygotowywanie prezentacji multimedialnych, które będą: a) prezentowanie przy użyciu projektora multimedialnego,</p>
--	--





	<p>10.2. drukowanie w formacie umożliwiającym robienie notatek,</p> <p>10.3. zapisanie jako prezentacja tylko do odczytu,</p> <p>10.4. nagrywanie narracji i dołączanie jej do prezentacji,</p> <p>10.5. opatrywanie slajdów notatkami dla prezentera,</p> <p>10.6. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,</p> <p>10.7. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,</p> <p>10.8. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,</p> <p>10.9. możliwość tworzenia animacji obiektów i całych slajdów,</p> <p>10.10. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,</p> <p>10.11. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007, 2010, 2013, 2016, 2019, 2021</p> <p>11. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:</p> <p>11.1. Tworzenie bazy danych przez zdefiniowanie:</p> <p>11.2. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.</p> <p>11.3. Relacji pomiędzy tabelami.</p> <p>11.4. Formularzy do wprowadzania i edycji danych.</p> <p>11.5. Raportów.</p> <p>11.6. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych.</p> <p>11.7. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów.</p> <p>11.8. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.</p> <p>12. narzędzie do obsługi poczty elektronicznej musi umożliwiać:</p> <p>12.1. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory.</p> <p>12.2. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,</p> <p>12.3. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.</p> <p>12.4. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.</p> <p>12.5. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.</p> <p>12.6. Automatyczne grupowanie poczty o tym samym tytule.</p> <p>12.7. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.</p> <p>12.8. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.</p> <p>12.9. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.</p> <p>12.10. Zarządzanie kalendarzem.</p> <p>12.11. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.</p>
--	--



	<p>12.12. Przeglądanie kalendarza innych użytkowników.</p> <p>12.13. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.</p> <p>12.14. Zarządzanie listą zadań.</p> <p>12.15. Zlecanie zadań innym użytkownikom.</p> <p>12.16. Zarządzanie listą kontaktów.</p> <p>12.17. Udostępnianie listy kontaktów innym użytkownikom.</p> <p>12.18. Przeglądanie listy kontaktów innych użytkowników.</p> <p>12.19. Możliwość przysyłania kontaktów innym użytkownikom.</p>
<b>Pakiet antywirusowy:</b>	<p>Oprogramowanie antywirusowe Eset Protect Essential lub program antywirusowy <b>równoważny</b>.</p> <p>Subskrypcja na 18 urządzeń na 5 lat.</p> <p>Zamawiający dopuszcza produkt równoważny, którego funkcjonalność pokrywa się z funkcjami ESET PROTECT Essential ON-PREM. W przypadku rozwiązania równoważnego Zamawiający wymaga przeprowadzenia przez wykonawcę wdrożenia oprogramowania (instalacja na zakupionych laptopach) oraz przeprowadzenie szkolenia informatyków (2 osoby) w zakresie obsługi oprogramowania.</p> <p>Równoważność oznacza, że:</p> <ol style="list-style-type: none"><li>oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem (Windows 11 Professional lub zaproponowanym oprogramowaniem systemowym równoważnym) ;</li><li>oprogramowanie równoważne musi zapewniać co najmniej pełną funkcjonalność oprogramowania w stosunku, do którego jest wskazywana przez wykonawcę jako równoważne i posiadać co najmniej takie same parametry techniczne i funkcjonalne;</li></ol> <p>c. warunki licencji oprogramowania równoważnego w każdym aspekcie licencjonowania muszą być nie gorsze niż licencje oprogramowania wskazanego przez Zamawiającego w stosunku do którego jest równoważna;</p> <p>d. warunki i zakres licencji dla oprogramowania równoważnego muszą być nie gorsze niż dla oprogramowania wskazanego przez Zamawiającego w stosunku do którego jest równoważna.</p> <p>Zamawiający wymaga, aby wykonawca w formularzu ofertowym opisał wszystkie dane techniczne składające się na dany asortyment zgodnym z zamówieniem.</p> <p>Oprogramowanie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.</p> <p>W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.</p> <p>Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanego oprogramowania z opisanymi warunkami równoważności spoczywa na Wykonawcy, składającym ofertę równoważną.</p>



	<p>Równoważność do oprogramowania ESET PROTECT Essential oznacza, że musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <p>1. Administracja zdalna w chmurze</p> <p>1.1 Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.</p> <p>1.2 Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu</p> <p>1.3 Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.</p> <p>1.4 Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.</p> <p>1.5 Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP</p> <p>1.6 Proxy.</p> <p>1.7 Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.</p> <p>1.8 Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.</p> <p>1.9 Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem,</p> <p>1.10 zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnień: odczyt, użyj, zapisz oraz brak.</p> <p>1.11 Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.</p> <p>1.12 Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</p> <p>1.13 Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.</p> <p>1.14 Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.</p> <p>2. Ochrona stacji roboczych</p> <p>2.1 Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11 lub zaproponowane oprogramowanie systemowe równoważne).</p> <p>2.2 Rozwiązanie musi wspierać architekturę ARM64.</p> <p>2.3 Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>2.4 Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</p> <p>2.5 Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</p> <p>2.6 Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p>
--	--



	<p>2.7 Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>2.8 Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>2.9 Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.</p> <p>2.10 Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).</p> <p>2.11 Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>2.12 Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>2.13 Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>2.14 Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.</p> <p>2.15 Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ol style="list-style-type: none"><li>tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,</li><li>tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,</li><li>tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,</li><li>tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,</li><li>tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</li></ol> <p>2.16 Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych</p>
--	---



	<p>aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>2.17 Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.</p> <p>2.18 Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>2.19 Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>2.20 Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>3. Ochrona serwera.</p> <p>3.1 Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.</p> <p>3.2 Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3.3 Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>3.4 Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>3.5 Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>3.6 Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>3.7 Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>3.8 Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>3.9 Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>3.10 Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>3.11 Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>3.12 Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>3.13 Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek</p>
--	---





	<p>USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>3.14 Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>3.15 Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>3.16 Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.</p> <p>3.17 Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>3.18 Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>3.19 Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>3.20 Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.</p> <p>3.21 Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.</p> <p>4. Ochrona urządzeń mobilnych opartych o system Android</p> <p>4.1 Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</p> <p>4.2 Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</p> <p>4.3 Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</p> <p>4.4 Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</p> <p>4.5 Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <p>4.5.1 usunięcie zawartości urządzenia,</p> <p>4.5.2 przywrócenie urządzenia do ustawień fabrycznych,</p> <p>4.5.3 zablokowania urządzenia,</p> <p>4.5.4 uruchomienie sygnału dźwiękowego,</p> <p>4.5.5 lokalizację GPS.</p> <p>4.6 Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.</p> <p>4.7 Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:</p> <p>4.7.1 nazwę aplikacji,</p> <p>4.7.2 nazwę pakietu,</p> <p>4.7.3 kategorię sklepu Google Play,</p> <p>4.7.4 uprawnienia aplikacji,</p> <p>4.7.5 pochodzenie aplikacji z nieznanego źródła.</p>
--	---



## II. Urządzenie wielofunkcyjne laserowe kolorowe

Opis parametrów minimalnych	
Urządzenie wielofunkcyjne laserowe kolorowe	<ul style="list-style-type: none"><li><input type="checkbox"/> Technologia druku laserowa - kolorowa</li><li><input type="checkbox"/> Automatyczny dupleks A4</li><li><input type="checkbox"/> Automatyczny podajnik dokumentów</li><li><input type="checkbox"/> max format druku: 216 x 356 mm</li><li><input type="checkbox"/> Rozmiary obsługiwanych nośników: co najmniej A4 /A5 /A6 / JIS B5</li><li><input type="checkbox"/> Rozmiary kopert: Międzynarodowy DL (110x220mm), Międzynarodowy C5 (162mm x 229 mm)</li><li><input type="checkbox"/> Rozdzielczość druku min. 600x 600 dpi</li><li><input type="checkbox"/> Rozdzielczość skanowania min. 600x 600 dpi</li><li><input type="checkbox"/> Interfejs: USB 2.0, LAN, USB, WIFI</li><li><input type="checkbox"/> Skanowanie do e-mail,</li><li><input type="checkbox"/> Prędkość drukowania min. 22 str/min (mono)</li><li><input type="checkbox"/> Prędkość drukowania min. 22 str/min (kolor)</li><li><input type="checkbox"/> Sterowniki drukarki: PCL6, PCL5, PostScript 3</li><li><input type="checkbox"/> Format pliku PDF, JPEG</li><li><input type="checkbox"/> Pamięć RAM minimum 512 MB</li><li><input type="checkbox"/> 2 podajniki</li><li><input type="checkbox"/> Pojemność podajnika wejściowego w formie kasety na 250 arkuszy</li><li><input type="checkbox"/> Panel sterujący z wyświetlaczem dotykowym</li><li><input type="checkbox"/> Obsługiwany system operacyjny: Współpracująca z systemem operacyjnym zainstalowanym w laptopach zaproponowanych w ofercie.</li><li><input type="checkbox"/> Deklaracja zgodności UE i oznakowanie CE</li><li><input type="checkbox"/> Kabel zasilający, kabel RJ-45 3 m. do podłączenia urządzenia z siecią komputerową.</li><li><input type="checkbox"/> Gwarancja producenta on-site 24 miesiące</li><li><input type="checkbox"/> Urządzenie musi posiadać komplet tonerów startowych.</li></ul>



Fundusze Europejskie  
dla Pomorza

Dofinansowane przez  
Unię Europejską



URZĄD MARSZAŁKOWSKI  
WOJEWÓDZTWA POMORSKIEGO