**AE/ZP-27-65/22 ZAŁĄCZNIK NR 3**

##### **Wymagane i oferowane parametry techniczne**

##### **oprogramowania do zarządzania infrastrukturą IT**

Zaoferowane oprogramowanie musi zapewniać co najmniej wszystkie funkcjonalności oraz wymagania wyspecyfikowane w niniejszej tabeli. Zaoferowane oprogramowanie do zarządzania infrastrukturą IT musi zostać zainstalowane i skonfigurowane z uwzględnieniem wszystkich obecnych konfiguracji oraz w pełni zintegrowane z istniejącą infrastrukturą informatyczną Szpitala. Wykonawca wykona wszystkie konfiguracje oraz dostarczy wszelkie wymagane bezterminowe licencje. Wszystkie licencje oraz prace konfiguracyjne należy wliczyć w cenę oferty. Po wdrożeniu zaoferowanego oprogramowania Wykonawca wykona testy sprawdzające i przedłoży Zamawiającemu raport z pozytywnym wynikiem testów zawierających co najmniej informacje o wdrożonych funkcjonalnościach aplikacji zawierających mechanizmy

systemów bezpieczeństwa.

**UWAGA! W kolmnie „Parametry oferowane” należy podać parametry (w postaci cyfrowej) oferowanego przedmiotu zamówienia lub potwierdzić posiadanie funkcji i ją opisać, jeżeli nie jest opisana cyfrowo.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagania Zamawiającego. Parametry techniczne.** | **Warunek graniczny.  Punktacja w kryterium**  **„parametry techniczne”.** | **Parametry oferowane Podać wartość, zakres oferowanych parametrów, opisać** |
| Nazwa oraz Producent oprogramowania | | TAK, podać  nazwę oraz Producenta oprogramowania |  |
| 1 | **Funkcje ogólne, wspólne dla oprogramowania** | | |
| 1.1 | Interfejs graficzny użytkownika w języku polskim | TAK |  |
| 1.2 | Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. | TAK, podać |  |
| 1.3 | Aplikacja w swojej funkcjonalności musi zawierać mechanizmy systemów bezpieczeństwa oraz wspierać Krajowe Ramy interoperacyjności. | TAK, podać |  |
| 1.4 | Program powinien wykorzystywać bezpłatny silnik bazy danych z kodem źródłowym dostępnym na licencji open-source, tym samym nie jest objęty limitem ilości danych.  Baza danych winna być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania.  W przeciwnym wypadku należy dostarczyć wszystkie niezbędne licencje bezterminowe oraz bez żadnych limitów (np. ilości danych/objętości itp.). | TAK, podać |  |
| 1.5 | Serwer oraz konsole zarządzające muszą być zainstalowane na 64-bitowej wersji systemu operacyjnego Windows lub Linux. | TAK, podać |  |
| 1.6 | Prezentowanie wybranych danych powinno odbywać się  w przeglądarce internetowej za pomocą widgetów  - widgety w zakresie monitorowania infrastruktury sieciowej – co najmniej: a) liczniki wydajności, b) alarmy, c) odpowiedzi serwisów TCP/lP,  - widgety w zakresie inwentaryzacji zasobów IT – co najmniej: a) zmiany w konfiguracji sprzętowej urządzeń   z agentami, b) zmiany w liście zainstalowanego oprogramowania, c) alarmy dla zasobów,  - widgety w zakresie obsługi użytkowników – co najmniej: a) statystyki z obszaru wydruków, b) statystki użycia aplikacji, c) użycie łącza, d) aktywność WWW,  - widgety w zakresie pomocy dla użytkowników – co najmniej :  a) statystyki z obsługi zgłoszeń,  b) lista najnowszych nierozwiązanych zgłoszeń,  c) lista najstarszych nierozwiązanych zgłoszeń,  d) ostatnie zgłoszenia z przekroczonym limitem czasu SLA  statystyki z obszaru wydruków,  - widgety w zakresie ochrony danych przed wyciekiem – co najmniej :  a) ostatnio podłączone nośniki zewnętrzne,  b) ostatnie operacje na plikach. | TAK, podać |  |
| 1.7 | Widgety muszą dostosowywać się do rozdzielczości ekranu  oraz musi być możliwość zmiany rozmiaru siatki widgetów | TAK, podać |  |
| 1.8 | Automatyczne odświeżanie dashboardów | TAK, podać |  |
| 1.9 | Udostępnianie dashboardów w trybie tylko do odczytu | TAK, podać |  |
| 1.10 | Agenty muszą być dostępne co najmniej dla systemów Windows | TAK, podać |  |
| 1.11 | Ochrona agenta przed usunięciem | TAK, podać |  |
| 1.12 | Zarządzanie hierarchią użytkowników | TAK, podać |  |
| 1.13 | Dziennik dostępu administratorów | TAK, podać |  |
| 1.14 | Jednoczesna praca minimum 4 administratorów | TAK, podać |  |
| 1.15 | Zarządzanie grupami (tworzenie i przypisywanie użytkowników) | TAK, podać |  |
| 1.16 | Wyszukiwarka – wyszukiwanie urządzeń, użytkowników, zasobów oraz elementów interfejsu programu. | TAK, podać |  |
| 1.17 | Aplikacja w swojej funkcjonalności musi zawierać co najmniej jeden z poniższych mechanizmów systemów bezpieczeństwa:  - SIEM - DLP  - NAC - DAM - EDR | TAK  podać jakie systemy bezpieczeństwa   i w jakim zakresie  Punktacja:  Zaferowane oprogramawnie zawiera 1 z wymienionych mechanizmów systemów bezpieczeństwa - 0 pkt.  Zaferowane oprogramawnie zawiera 2 z wymienionych mechanizmów systemów bezpieczeństwa - 5 pkt. Zaferowane oprogramawnie zawiera 3 z wymienionych mechanizmów systemów bezpieczeństwa - 10 pkt. Zaferowane oprogramawnie zawiera 4 z wymienionych mechanizmów systemów bezpieczeństwa - 15 pkt. Zaferowane oprogramawnie zawiera 5 z wymienionych mechanizmów systemów bezpieczeństwa - 20 pkt. |  |
| 1.18 | Oprogramowanie musi wspierać w spełnianiu Krajowych Ram Interoperacyjności w zakresie np. kontroli dostępu, zarządzania ciągłością działania, organizacji bezpieczeństwa informacji, bezpieczniej eksploatacji, bezpieczeństwa komunikacji, kontroli poziomu realizacji usług i ich dostępności itp.  Funkcje tych systemów, muszą zostać spełnione  w momencie przygotowania i ustalenia zasad monitorowania, zarządzania oraz polityki do wdrożenia pod wymagania regulacji prawnych. | TAK  podać, które moduły zaoferowanego oprogramowania  i w jakim zakresie |  |
| 1.19 | Oprogramowanie musi wpierać wdrożony w 2014r system zarządzania bezpieczeństwem informacji ISO27001  w zakresie minimum monitorowania sieci oraz helpdesku | TAK  podać, które moduły zaoferowanego oprogramowania  i w jakim zakresie |  |
| 1.20 | Komunikacja pomiędzy Serwerem a agentami i konsolami itp. powinna być nawiązywana przy użyciu szyfrowanego protokołu. | TAK Podać |  |
| 1.21 | Oprogramowanie musi być zgodne z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) ( dalej „RODO”), musi umożliwiać usuwanie danych wybranego  użytkownika bez konieczności usunięcia informacji o stacji roboczej.  Dane, które dotyczą działań pracownika na komputerze takie jak historia aktywności, polityka korzystania z internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych technicznych np. informacji o stacji roboczej. Muszą one również być grupowane w osobnym, dedykowanym oknie. | TAK, podać |  |
| 1.22 | Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, ma być objęty kontrolą na poziomie Administratora. W programie musi być możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień co najmniej do funkcji programu, grup urządzeń, jak i użytkowników. | TAK, podać |  |
| 1.23 | Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. ograniczyć dostęp do wybranych opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane tzn. program musi posiadać informacje o czynnościach wykonanych przez administratorów. | TAK, podać |  |
| 2 | **Funkcjonalność oprogramowania w zakresie monitorowania infrastruktury** | | |
| 2.1 | Skanowanie sieci, wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping | TAK, podać |  |
| 2.2 | Wykrywanie urządzeń na podstawie informacji odczytanych z Active Directory | TAK, podać |  |
| 2.3 | Interaktywne mapy sieci, map użytkownika, oddziałów, mapy inteligentne | TAK, podać |  |
| 2.4 | Serwisy TCP/lP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.) | TAK, podać |  |
| 2.5 | Liczniki WMl: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp. | TAK, podać |  |
| 2.6 | Działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń | TAK, podać |  |
| 2.7 | Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoiP itp.) - monitorowanie wartości za pomocą nazw zmiennych oraz OID. | TAK, podać |  |
| 2.8 | Liczniki SNMP V1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera ) | TAK, podać |  |
| 2.9 | Oprogramowanie musi umożliwiać nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów, definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie. m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera.  Alarmy tworzone przez administratora z wykorzystaniem ciągu przyczynowo skutkowego tzn administrator może samodzielnie wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. | TAK, podać |  |
| 2.10 | Możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS | TAK, podać |  |
| 2.11 | Routery i switche: mapowanie portów; informacja, do którego przełącznika jest podłączone urządzenie | TAK, podać |  |
| 2.12 | Obsługa komunikatów syslog | TAK, podać |  |
| 2.13 | Obsługa szyfrowania AES, DES i 3DES dla protokołu SN MPv3 | TAK, podać |  |
| 2.14 | Możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca) | TAK, podać |  |
| 2.15 | Wizualizacja stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci oraz grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze. | TAK, podać |  |
| 2.16 | Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku | TAK, podać |  |
| 2.17 | Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie  w sposób manualny oraz automatyczny. | TAK, podać |  |
| 2.18 | Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie. | TAK, podać |  |
| 2.19 | Zablokowanie mapy urządzeń przed przypadkową edycją. | TAK, podać |  |
| 2.20 | Monitoring routerów i przełączników wg: zmian stanu interfejsów sieciowych, ruchu sieciowego, podłączonych stacji roboczych, ruchu generowanego przez podłączone do portów stacje robocze. | TAK, podać |  |
| 2.21 | Monitor serwisów Windows który alarmuje gdy serwis przestanie działać oraz pozwala co najmniej na jego uruchomienie, zatrzymanie, zrestartowanie. | TAK, podać |  |
| 2.22 | Wyświetlanie na mapie statystyk dla każdego urządzenia: co najmniej: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu. | TAK, podać |  |
| 2.23 | Wydajność systemów Windows – co najmniej obciążenie procesora, pamięci, zajętość dysków, transfer sieciowy. | TAK, podać |  |
| 3 | **Funkcjonalność oprogramowania w zakresie ochrony danych przed wyciekiem** | | |
| 3.1 | Blokowanie urządzeń i nośników danych. Program musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić  z nich program zewnętrzny. | TAK, podać |  |
| 3.2 | Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. | TAK, podać |  |
| 3.3 | Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth | TAK, podać |  |
| 3.4 | Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane | TAK, podać |  |
| 3.5 | Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych | TAK, podać |  |
| 3.6 | Funkcje wspierające bezpieczeństwo systemu:  - integracja i zarządzanie ustawieniami Windows Defender.  - monitorowanie stanu szyfrowania dysków Bitlocker.  - integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.  - monitorowanie stanu modułu TPM | TAK, podać |  |
| 3.7 | Zarządzanie prawami dostępu do urządzeń:  - Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.  - Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników  - Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci  - Możliwość usuwania z listy znanych urządzeń tych nośników, które są np. uszkodzone, wycofane z użytku i skasowane | TAK, podać |  |
| 3.8 | Audyt operacji na plikach na urządzeniach przenośnych:  - Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych  - Podłączenie/odłączenie urządzenia przenośnego | TAK, podać |  |
| 3.9 | Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych | TAK, podać |  |
| 3.10 | Alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym oraz na dyskach lokalnych | TAK, podać |  |
| 3.11 | Integracja bazy użytkowników i grup z Active Directory | TAK, podać |  |
| 3.12 | Integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych | TAK, podać |  |
| 3.13 | Integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania | TAK, podać |  |
| 3.14 | Metryki użytkowników prezentujące aktualne ustawienia dla danego pracownika | TAK, podać |  |
| 3.15 | Automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa | TAK, podać |  |
| 3.16 | Informacja o urządzeniach podpiętych do danego komputera | TAK, podać |  |
| 3.17 | Lista wszystkich urządzeń podłączonych do komputerów  w sieci | TAK, podać |  |
| 3.18 | Audyt podłączeń i operacji na urządzeniach przenośnych oraz udziałach sieciowych i dyskach lokalnych | TAK, podać |  |
| 3.19 | Zarządzanie prawami dostępu (np. zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników | TAK, podać |  |
| 4. | **Funkcjonalność oprogramowania w zakresie obsługi użytkowników** | | |
| 4.1 | Pełne zarządzanie użytkownikami, bazujące na grupach  i politykach bezpieczeństwa | TAK, podać |  |
| 4.2 | Blokowanie uruchamianych aplikacji | TAK, podać |  |
| 4.3 | Monitorowanie wiadomości e-mail (nagłówki) - antyphishing | TAK, podać |  |
| 4.4 | Szczegółowy czas pracy (godzina rozpoczęcia  i zakończenia aktywności oraz przerwy), | TAK, podać |  |
| 4.5 | Odwiedzane strony WWW (tytuły i adresy stron, liczba  i czas wizyt) | TAK, podać |  |
| 4.6 | Audyty wydruków - informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), koszty wydruków | TAK, podać |  |
| 4.7 | Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) | TAK, podać |  |
| 4.8 | Blokowanie stron WWW | TAK, podać |  |
| 4.9 | Zgodność z RODO - przyporządkowanie konfiguracji, uprawnień i dostępów do konkretnego użytkownika, niezależnie od urządzenia | TAK, podać |  |
| 4.10 | Dokładne wyszczególnienie aktywności oraz metryki użytkownika | TAK, podać |  |
| 4.11 | Reguły filtrowania stron WWW i blokowania aplikacji: zmiana mechanizmu tworzenia i zarządzania regułami, grupowanie reguł, powielanie reguł między grupami użytkowników | TAK, podać |  |
| 4.12 | Generowanie raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. | TAK, podać |  |
| 4.13 | Blokowanie uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami | TAK, podać |  |
| 4.14 | W ramach pomocy użytkownikom, musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania aby użytkownik został zapytany o zgodę na połączenie. Podczas dostępu zdalnego, zarówno użytkownik jak  i administrator muszą widzieć ten sam ekran. | TAK, podać |  |
| 4.15 | Baza zgłoszeń dla zgłaszanych problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie | TAK, podać |  |
| 4.16 | Moduł musi umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów  [Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii](https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2019-1937-w-sprawie-ochrony-osob-zglaszajacych-naruszenia-prawa-69247962?_ga=2.156271807.548267028.1661428839-1164647857.1661428838#xd_co_f=MjE1N2IzMTgtMDAzMi00MWVkLWFiMGMtYzc4ZjlkNDc4NWIx~) (dalej   „Dyrektywa o sygnalistach”)) oraz zawierać dokumenty prawne dotyczące ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymaganych przez Dyrektywę o sygnalistach. | TAK, podać |  |
| 4.17 | Użytkownicy muszą mieć możliwość monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. | TAK, podać |  |
| 4.18 | Komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami  i administratorami oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać prostsze, powtarzające się problemy | TAK, podać |  |
| 4.19 | Program musi pozwalać na informowanie pracowników  o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Dostęp do systemu zgłoszeń oraz bazy wiedzy musi być realizowany przez dedykowany portal dostępny  z poziomu przeglądarki internetowej (wyświetlany w trybie jasnym lub ciemnym). | TAK, podać |  |
| 4.20 | Moduł w zakresie zdalnej pomocy dla użytkowników musi umożliwiać również co najmniej:  - pobieranie listy użytkowników z Active Directory,  - zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,  - tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń  - wykonywanie operacji na wielu zgłoszeniach równocześnie,  - dołączanie załączników do zgłoszeń,  - szybki dostęp do ostatnich zgłoszeń oraz rozbudowane wyszukiwanie wszystkich zgłoszeń  - dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików msi)  - zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),  - wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików. | TAK, podać |  |
| 4.21 | Baza wiedzy z kategoryzacją artykułów, wyszukiwarką  i możliwością wstawiania grafik oraz filmów | TAK, podać |  |
| 4.22 | Możliwość dodania opisu kategorii zgłoszenia np. w celu umieszczenia klauzuli RODO | TAK, podać |  |
| 4.23 | Szczegółowe statystyki czasu pracy przy komputerze oraz historia pracy w widoku graficznym: lista aplikacji desktopowych i odwiedzanych stron WWW | TAK, podać |  |
| 4.24 | Statystyki aktywności osobistej widoczne dla pracownika | TAK, podać |  |
| 4.25 | Statystyki aktywności działu/oddziału i jej pracowników widoczne dla Kierownika działu/Ordynatora oddziału | TAK, podać |  |
| 4.26 | Dodawanie wyjątków przez administratora działu, wskazujących, że dana aplikacja w tym dziale jest uznawana za produktywną | TAK, podać |  |
| 5 | **Funkcjonalność oprogramowania w zakresie inwentaryzacji zasobów IT** | | |
| 5.1 | Umożliwia przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, | TAK, podać |  |
| 5.2 | Informacje dotyczące sprzętu – ca najmniej: modelu, procesora, pamięci, płyty głównej, napędów, kart.  Informacje muszą zawierać minimum zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na określenie dla których systemów konieczny jest upgrade. | TAK, podać |  |
| 5.3 | Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows - umożliwia audytowanie  i weryfikację użytkowania licencji w organizacji. | TAK, podać |  |
| 5.4 | Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: (np. instalacji/deinstalacji aplikacji, zmian adresu IP itp.) | TAK, podać |  |
| 5.5 | Możliwość wysyłania powiadomienia np. mailem  w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera | TAK, podać |  |
| 5.6 | Umożliwia automatyczne zarządzanie instalacjami  i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych | TAK, podać |  |
| 5.7 | Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. | TAK, podać |  |
| 5.8 | Umożliwia odczytanie numeru seryjnego (klucze licencyjne). | TAK, podać |  |
| 5.9 | Umożliwia utworzenie listy plików użytkowników  z określonym rozszerzeniem (np. filmy .MP4) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). | TAK, podać |  |
| 5.10 | Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji mają być logowane. | TAK, podać |  |
| 5.11 | Automatycznego aktualizowania zgromadzonych informacji, | TAK, podać |  |
| 5.12 | Tworzenia powiązań między zasobami a urządzeniami, | TAK, podać |  |
| 5.13 | Tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak  i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych | TAK, podać |  |
| 5.14 | Wskazania osób uprawnionych do użycia zasobów | TAK, podać |  |
| 5.15 | Definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości  dla danego urządzenia lub oprogramowania mus być możliwość dodawania dodatkowych informacji – co najmniej: numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz. | TAK, podać |  |
| 5.16 | Określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, | TAK, podać |  |
| 5.17 | Określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, | TAK, podać |  |
| 5.18 | Oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., | TAK, podać |  |
| 5.19 | Generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, | TAK, podać |  |
| 5.20 | Archiwizacji i porównywania audytów zasobów | TAK, podać |  |
| 5.21 | Tworzenia kodów kreskowych dla zasobów | TAK, podać |  |
| 5.22 | Drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, | TAK, podać |  |
| 5.23 | Inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie  i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet | TAK, podać |  |
| 5.24 | Definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”). | TAK, podać |  |

**Niespełnienie wyżej wyszczególnionych parametrów spowoduje odrzucenie oferty.**