Załącznik nr 6 do SWZ

Opis Przedmiotu Zamówienia (OPZ)

**OPIS WYMAGAŃ**

Dostawa i wdrożenie system do zarządzania zasobami, procesami, uprawnieniami i kontrolą dostępu administracyjnego IT. W zakresie realizacji przedmiotu zamówienia obowiązkiem wykonawcy jest:

a). dostarczenie systemu do zarządzania zasobami, procesami, uprawnieniami i kontrolą dostępu administracyjnego IT wraz z niezbędnymi ilościami wieczystych licencji systemowych i dostępowych,

b). dostarczenie wieczystych licencji bezpłatnego lub komercyjnego systemu serwerowego obsługi bazy danych i niezbędnych wieczystych licencji dostępowych do tego serwera,

c). dostarczenie serwerów fizycznych dla instalacji systemu do zarządzania zasobami, procesami, uprawnieniami i kontrolą dostępu administracyjnego IT oraz wydzielonego środowiska bazy danych obsługującej ten system,

d). dostarczenie rocznego wsparcia serwisowego dla zaoferowanego systemu,

e). wdrożenie i uruchomienie zaoferowanego systemu wraz z przeszkoleniem personelu technicznego Zamawiającego (wskazani pracownicy Działu Informatyki) w zakresie konfiguracji, parametryzacji i obsługi.

System do zarządzania zasobami, procesami, uprawnieniami i kontrolą dostępu administracyjnego IT powinien obsługiwać co najmniej następujące procesy:

a). automatyczna inwentaryzacja konfiguracji sprzętowo-systemowej zarejestrowanych jednostek komputerowych, w tym posiadanie wbudowanego mechanizmu analizy zmian konfiguracji oraz odczytu parametrów wraz z automatycznym powiadamianiem administratorów o wykrytych nieprawidłowościach;

b). inwentaryzacja zainstalowanych i wdrożonych w środowisku Zamawiającego aplikacji oraz analiza zawartości dysków komputerowych umożlwiająca precyzyjną identyfikację zainstalowanego oprogramowania w połączeniu z możliwością ewidencji zakupionych licencji dla celów prowadzenia wewnętrznego audytu legalności oprogramowania;

c). pozwalać na zdalne połączenie z dowolnym wybranym stanowiskiem komputerowym w formie przejęcia pulpitu, operacji zdalnych oraz transferów plików w sieci LAN/WAN w celu np. globalnej i zdalnej instalacji aplikacji oraz wykonywania określonych skryptów, zarządzania procesami tworzenia kopii zapasowych (backup) użytkowników;

d). zarządzać centralnie posiadanymi zasobami (tworzenie dowolnych wewnętrznych kategorii zasobów, opisywanie go wymaganymi atrybutami oraz powiązywanie go z dowolnymi innymi obiektami zewidencjowanymi w systemie);

e). portal zgłoszeniowy typu ServiceDesk, zarządzający incydentami i problemami w organizacji Zamawiającego, posiadający funkcjonalność bazy wiedzy oraz nadzoru nad zarejestrowanymi w systemie umowami klasy SLA, oparty o interfejs webowy WWW, pozwalający na prosty sposób rejestracji oraz obsługi zgłoszeń;

f). posiadający wbudowany, bezpieczny (szyfrowana komunikacja) i wydajny komunikator, dla realizacji procesów wymiany komunikatów wewnętrznych w oparciu o wymianę treści tekstowych, wykonywanie połączeń audio-wideo, udostępnianie ekranu oraz tworzenie telekonferencji;

g). cyklicznego skanowania siec i lokalnej LAN wraz z analizą wykrytych urządzeń m.in. w oparciu o protokół SNMP i tworzeniem map sieci;

h). zarządzania wnioskami ogólnymi i wnioskami o nadawanie uprawnień dostępowych, poprzez wsparcie procesów obsługi (obiegu) wniosków wymagających wieloetapowej akceptacji osób decyzyjnych, przykładowo: wnioski nadawanie uprawnień do systemów informatycznych Zamawiającego w tym wsparcie dla procesów RODO, wnioski obiegowe dla przyjęcia i zwolnienia pracownika (zarządzanie sprzętem przypisanym do pracownika), wnioski zakupowe sprzętu od pracownika;

i). odczytywanie informacji o aktywności personelu Zamawiającego w systemach IT, w tym pełny podgląd procesów logowania, uruchamianych aplikacji, kopiowania danych, odwiedzanych stron internetowych, analizy realizowanych wydruków;

j). kontrola i zarządzanie dostępem do urządzeń zewnętrznych typu USB Storage;

k). wsparcia dla automatyzacji zadań.

System do zarządzania zasobami, procesami, uprawnieniami i kontrolą dostępu administracyjnego IT powinien być zbudowany w oparciu o trójwarstwowy model systemowy, wspierany przez logiczne i fizyczne rozdzielenie modułów systemu pomiędzy warstwy prezentacji, logiki biznesowej oraz danych. Powinien posiadać zaimplementowane mechanizmy zabezpieczenia transmisji danych pomiędzy tymi warstwami np. w oparciu o szyfrowanie typu AES256.

Wraz z dostawą samego rozwiązania środowiska sprzętowo-programowego systemu do zarządzania zasobami, procesami, uprawnieniami i kontrolą dostępu administracyjnego IT należy dostarczyć odpowiadające mu wydajne środowisko sprzętowo-programowe systemu obsługi bazy danych (bezpłatne lub komercyjne) wraz z wymaganymi wieczystymi licencjami serwerowymi i dostępowymi, a także niezbędne licencje wieczyste serwerowych systemów operacyjnych niezbędnych do implementacji wyżej wskazanych systemów na urządzeniach serwerowych dostarczony w ramach wdrożenia.

**Wymagania formalne**

a). Wszystkie dostarczone licencje dla systemów i oprogramowanie muszą być bezterminowe i wystawione na dane Zamawiającego.

b). Wszystkie dostarczone licencje dla systemów i oprogramowania muszą być dostarczone z **co najmniej 12 miesięcznym wsparciem (support) producenta**, liczonym od daty podpisania protokołu zdawczo – odbiorczego

c). Obsługa serwisowa oferowanego systemu w zakresie obsługi błędów realizowana ma być z czasem reakcji do 8 godzin roboczych oraz czasem naprawy do 80 godzin roboczych.

d). W ramach wsparcia (supportu) oferowanego systemu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

e). Dostarczone licencje na oprogramowanie muszą objąć co najmniej **2000 stanowisk komputerowych z systemem klasy Microsoft Windows**, **100 urządzeń mobilnych z systemem klasy Android**. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp.). Ponadto dostarczony system musi posiadać **co najmniej 30 administracyjnych licencji dostępowych** do centralnej konsoli zarządzającej systemem.

g). Zamawiający wymaga od wykonawcy, **aby w terminie** **do 10 dni roboczych od podpisania umowy** **(nie później jednak niż do 01.12.2022 r.) przeprowadził wdrożenie i uruchomienie systemu** (wymagana co najmniej 4 sesje - 3 godziny/każda).

h). Zamawiający wymaga od wykonawcy, **aby w terminie do 14 dni roboczych (nie później jednak niż do 01.12.2022 r.) od podpisania umowy przeprowadził szkolenie** z administracyjnej obsługi systemu dla wskazanego personelu Działu Informatyki – co najmniej 5 osób (wymagana co najmniej 4 sesje - 3 godziny/każda).

**A. Szczegółowe wymagania ogólne dla systemu zarządzania**

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
6. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
7. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
8. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
9. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
10. Oprogramowanie musi współpracować z wydajnym i dostarczonym w ramach zamówienia serwerem bazodanowym klasy SQL, bezpłatnym lub komercyjnym rozwiązaniem (w zakresie rozwiązania komercyjnego konieczne jest dostarczenie najnowszej wersji handlowej danego rozwiązania wraz z bezterminowymi licencjami serwerowymi oraz dostępowymi oraz wsparciem serwisowym producenta).
11. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
12. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych.
13. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty.
14. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi).
15. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Microsoft Windows.
16. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
17. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
18. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
19. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
20. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
21. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
22. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
23. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
24. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
25. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
26. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień, predefiniowane atrybuty komputera.
27. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
28. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
29. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
30. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

**B. Inwentaryzacja konfiguracji komputerów**

1. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
2. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
3. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
4. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
5. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
6. Oprogramowanie Agenta musi umożliwiać audyt offline, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
7. Oprogramowanie musi umożliwiać analizę sprzętową:
	1. płyty głównej w zakresie model, producent, nr. seryjny,
	2. CPU w zakresie nazwy, modelu, producenta, częstotliwości,
	3. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
	4. RAM w zakresie wielkości pamięci,
	5. karty sieciowej w zakresie model, adres IP, adres MAC,
	6. karty graficznej w zakresie model.
8. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
9. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
10. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
11. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
12. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
13. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
14. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

**C. Inwentaryzacja oprogramowania**

1. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
2. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
3. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
4. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
5. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
6. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
7. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
8. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
9. Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
10. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
11. Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

**D. Zarządzanie licencjami, audyt oprogramowania**

1. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
2. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
3. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
4. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
5. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

**E. Zarządzanie zasobami oraz użytkownikami**

1. Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów
2. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
3. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
4. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
5. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
6. Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów.
7. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
8. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
9. Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
10. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
11. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
12. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.

**F. Zdalny pulpit, zdalne zarządzanie komputerem**

1. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
2. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
3. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
4. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-On-LAN.
5. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
6. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
7. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
8. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
9. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
10. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
11. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
12. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
13. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
14. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Microsoft Windows
15. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
16. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
17. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

**G. Automatyzacja**

1. Oprogramowanie musi umożliwiać zdalną instalację pakietów \*.msi, plików \*.cmd, \*.bat, \*.reg, \*.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
2. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
3. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
4. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
5. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
6. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
7. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
8. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
9. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
10. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
11. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
12. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
13. Oprogramowanie musi umożliwiać optymalizację dystrybucji zadań oraz plików na komputery, pobierając brakujące fragmenty plików od agentów z tej samej podsieci (mechanizm peer-to-peer).
14. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
15. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Microsoft Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
16. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Microsoft Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
17. Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Microsoft Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
18. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Microsoft Windows 10, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
19. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
20. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
21. Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
22. Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
23. Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
24. Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
25. Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
26. Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

**H. Backup danych użytkownika**

1. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
2. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
3. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. \*.doc, które mają być archiwizowane.
4. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
5. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
6. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
7. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

**I. Zarządzanie urządzeniami USB Storage**

1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
2. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
3. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USB Storage.
4. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USB Storage
5. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

**J. Monitoring użytkowników**

1. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
2. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
3. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
4. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
5. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
6. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
7. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
8. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
9. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
10. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (fokus okna), hibernacji, uśpienia oraz wylogowania
11. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
12. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
13. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
14. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
15. Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
16. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

**K. ServiceDesk – Zarządzanie zgłoszeniami**

1. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:
	1. Zarządzanie problemem
	2. Zarządzanie incydentem
	3. Obsługa procesów poprzez mechanizm workflow (wnioski o usługi, uprawnienia, zakupy)
	4. Zarządzanie umowami serwisowymi
	5. Definicje poziomów SLA (reakcja, naprawa, reklamacja)
2. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
3. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
4. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
5. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
6. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
7. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
8. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
9. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
10. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
11. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
12. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
13. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
14. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
15. Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
16. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
17. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
18. Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
19. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
20. Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
21. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
22. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
23. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
24. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
25. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
26. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
27. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
28. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefonicznie informuje, że zepsuł mu się komputer).
29. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
30. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
31. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
32. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
33. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
34. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
35. Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
36. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji
37. mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
38. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
39. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
40. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
41. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
42. Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:
	1. Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
	2. Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
	3. Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
	4. Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
	5. Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
	6. Zamykanie zgłoszenia po upływie czasu reklamacji.
	7. Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
	8. Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
	9. Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
	10. Systemowe potwierdzanie realizacji zgłoszenia.
	11. Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.
43. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
44. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
45. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
46. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
47. Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
48. Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
49. Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
50. Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem
51. Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
52. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
53. Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
54. Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
55. Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
56. Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
57. Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
58. Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
59. Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
60. Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

**L. ServiceDesk – Zarządzanie wnioskami**

1. Oprogramowanie musi zapewnić obsługę workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
2. Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
3. Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

**M. ServiceDesk – Zarządzanie uprawnieniami**

1. Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
2. Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
3. Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
4. Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
5. Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
6. Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
7. Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
8. Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
9. Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
10. Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
11. Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
12. Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

**N. ServiceDesk – Zarządzanie rezerwacjami**

1. Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
2. Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
3. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
4. Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
5. Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
6. Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

**O.** **System zarządzania urządzeniami mobilnymi z systemami Android**

1. Dostarczone licencje na oprogramowanie do zarządzania urządzeniami mobilnymi muszą być bezterminowe.
2. Oprogramowanie w zakresie zarządzania urządzeniami mobilnymi musi współpracować z dostarczonym serwerem bazy danych.
3. Oprogramowanie musi umożliwiać centralne zarządzanie urządzeniami mobilnymi
4. Oprogramowanie musi umożliwiać zdalne przywracanie system do ustawień fabrycznych
5. Oprogramowanie musi umożliwiać wykonanie zrzutu ekranu urządzenia.
6. Oprogramowanie musi umożliwiać pobranie logów urządzenia.
7. Oprogramowanie musi umożliwiać skanowanie plików urządzenia
8. Oprogramowanie musi umożliwiać zarządzenie politykami bezpieczeństwa np. hasłami
9. Oprogramowanie musi umożliwiać backup kontaktów, połączeń, smsów, rejestru połączeń
10. Oprogramowanie musi umożliwiać automatyczne pozyskiwanie informacji w zakresie m.in.: nazwa, model, wersja systemu, model urządzenia, rodzaj procesora, ilość pamięci RAM, pamięci na karcie SD, karta Sim, nr telefonu, numer IMEI, nr seryjny, ostatnia aktywność agenta
11. Oprogramowanie musi umożliwiać informacje o rodzaju komunikacji uruchomionej na urządzeniu
12. Oprogramowanie musi umożliwiać dostęp do mapy z aktualną lokalizacją urządzenia
13. Oprogramowanie musi umożliwiać inwentaryzację zainstalowanych aplikacji na urządzeniu
14. Oprogramowanie musi umożliwiać inwentaryzację plików znajdujących się na urządzeniu
15. Oprogramowanie musi umożliwiać zarządzenie listą wykonanych zadań
16. Oprogramowanie musi posiadać wbudowane raporty dotyczące urządzeń mobilnych, w zakresie minimalnie: wg producenta, wersji, ostatniej aktywności, systemu operacyjnego

**P. SERWER APLIKACYJNY – 1 komplet**

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Obudowa | Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi umożliwiającymi wysunięcie, do celów serwisowych, serwera z szafy bez konieczności odłączania kabli zasilających i sygnałowych (kable LAN SAN)Serwer z dostępnym, jako opcja (możliwość instalacji), czujnik otwarcia obudowy współpracującego z BIOS/UEFI.  |
| Procesor | Procesor min. szesnastordzeniowy, x86 - 64 bity, działający z częstotliwością min. 3.0GHz, osiągający w testach SPECrate2017\_int\_base wynik nie gorszy niż 154 punktów, dla oferowanego modelu serwera z jednym procesorem. Wynik testu opublikowany na stronie www.spec.org |
| Liczba procesorów | Min. 1 procesor, płyta główna min. jednoprocesorowa |
| Pamięć operacyjna | 32 GB RDIMM DDR4 min.3200 MT/s w modułach o pojemności min. 16GB każdy.Płyta główna z minimum 16 slotami na pamięć i umożliwiająca instalację minimum 2TB.Obsługa zabezpieczeń: ECC. |
| Sloty rozszerzeń | Serwer musi być wyposażony w:- 2 aktywne gniazda PCI-Express generacji 4, każde gniazdo x16 i pozwalać na rozbudowę do 3 aktywnych gniazd PCI-Express generacji 4, każde gniazdo x16 (szybkość slotu – bus width) Serwer musi mieć dodatkowo dedykowane dwa sloty PCI-Express:- na kontroler dyskowy;- na kartę sieciową niezajmującą slotów PCI-Express. |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania min.8 dysków 2.5” typu Hot Swap, SAS/SATA/SSD. Wszystkie zatoki dyskowe dostępne z przodu serwera.Zainstalowane:- 2 x dysk 480GB SSD RI (Read Intensive) 2.5” typu hot swap - 2 x dysk 2.4YB SAS 10K typu hot swap  |
| Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie |
| Interfejsy sieciowe | Karta, minimum 4 porty Ethernet 1Gb które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 4 x USB 3.1 (w tym min. 1 porty wewnętrzny)1x VGA Możliwość rozbudowy/rekonfiguracji o:- port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne)
* wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
* dostęp do karty zarządzającej poprzez
	+ dedykowany port RJ45 z tyłu serwera lub
	+ przez współdzielony port zintegrowanej karty sieciowej serwera
* dostęp do karty możliwy
	+ z poziomu przeglądarki webowej (GUI)
	+ z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
	+ poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego
* obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
* obsługa zdalnego serwera logowania (remote syslog)
* wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów
* mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
* funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy)
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
* zdalna aktualizacja oprogramowania (firmware)
* zarządzanie grupami serwerów, w tym:
	+ tworzenie i konfiguracja grup serwerów
	+ sterowanie zasilaniem (wł/wył)
	+ ograniczenie poboru mocy dla grupy (power caping)
	+ aktualizacja oprogramowania (firmware)
	+ wspólne wirtualne media dla grupy
* możliwość równoczesnej obsługi przez min. 2 administratorów
* autentykacja dwuskładnikowa (Kerberos)
* wsparcie dla Microsoft Active Directory
* obsługa TLS i SSH
* wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API
* możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
 |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2019 lub nowszyRed Hat Enterprise Linux (RHEL) 7.X lub nowszySUSE Linux Enterprise Server (SLES) 12 lub nowszyVMware ESXi 6.5 U3 lub nowszy |
| Wsparcie techniczne | 3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji w ciągu następnego dnia roboczego od zgłoszenia. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.Wymagane jest aby oferowane urządzenia były produkowane zgodnie z normami ISO 14001 lub równoważnymi. |

**R. SERWER BAZODANOWY – 1 komplet**

|  |  |
| --- | --- |
| Element konfiguracji | Wymagania minimalne |
| Obudowa | Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)  |
| Procesor | Jeden procesor dziesięciordzeniowy x86 - 64 bity, Intel Xeon 4210R (2.4GHz/10-core/13,75MB) lub równoważne procesor dziesięciordzeniowy, osiągający w testach PassMark CPU Mark wynik nie gorszy niż 15155 punktów. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie [www.cpubenchmark.net](http://www.cpubenchmark.net)Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.  |
| Liczba procesorów | 1 procesor |
| Pamięć operacyjna | 16 GB RDIMM DDR4 2633 MT/s w modułach o pojemności 16GB.Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC i Online Spare.Serwer z obsługą pamięci typu NVDIMM |
| Sloty rozszerzeń | 2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy o dodatkowy, trzeci slot PCI-Express generacji 3 x16 (prędkość slotu – bus width). |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy oraz możliwość zainstalowania 1 dysku SFF SAS/SATA/SSD, 2,5” z tyłu serweraW przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 11 zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD 2,5”typu Hot Swap.Serwer wyposażony w 2 dyski 240GB SSD RI Hot Plug  |
| Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie |
| Interfejsy sieciowe | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.Opcja rozbudowy o dodatkowe 2 porty obsługujące prędkości 10/40 Gb/s (możliwość konfiguracji pracy z prędkościami 10 i 40Gb/s), przez zastosowanie karty nie zajmującej gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 5 x USB 3.0 (w tym 2 porty wewnętrzne)1x VGA Wewnętrzny slot na kartę micro SD.Możliwość rozbudowy o:- dodatkowy port typu DisplayPort dostępny z przodu serwera- port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plugMożliwość skonfigurowania serwera do pracy w temperaturze otoczenia równej 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4 |
| Napęd | Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW |
| Diagnostyka | Elektroniczny panel diagnostyczny dostępny z przodu serwera pozwalający uzyskać informacje o stanie: procesora, pamięci, wentylatorów, kary sieciowej, zasilaczy, kartach rozszerzeń, temperaturze. |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe
* wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
* dostęp do karty zarządzającej poprzez
	+ dedykowany port RJ45 z tyłu serwera
	+ przez współdzielony port zintegrowanej karty sieciowej serwera

 dostęp do karty możliwy * + z poziomu przeglądarki webowej (GUI)
	+ z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
	+ z poziomu skryptu (XML/Perl)
	+ poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego
* obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
* obsługa zdalnego serwera logowania (remote syslog)
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów
* mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
* funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
* zdalna aktualizacja oprogramowania (firmware)
* zarządzanie grupami serwerów, w tym:
	+ tworzenie i konfiguracja grup serwerów
	+ sterowanie zasilaniem (wł/wył)
	+ ograniczenie poboru mocy dla grupy (power caping)
	+ aktualizacja oprogramowania (firmware)
	+ wspólne wirtualne media dla grupy
* możliwość równoczesnej obsługi przez 6 administratorów
* autentykacja dwuskładnikowa (Kerberos)
* wsparcie dla Microsoft Active Directory
* obsługa SSL i SSH
* enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli
* wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API
* wsparcie dla Integrated Remote Console for Windows clients
* możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
 |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2012 R2, 2016Red Hat Enterprise Linux (RHEL) 6.9 oraz 7.3SUSE Linux Enterprise Server (SLES) 11 SP4 oraz 12 SP2ClearOSCentOSVMware ESXi 6.0 U3VMware ESXi 6.5 oraz U1 |
| Wsparcie techniczne | 3-letnia gwarancja producenta w miejscu instalacji.Czas reakcji w miejscu instalacji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.Wymagane jest aby oferowane urządzenia były produkowane zgodnie z normami ISO 14001 lub równoważnymi. |

**OŚWIADCZENIE WYKONAWCY:**

Oświadczamy pod rygorem odpowiedzialności karnej z art 297 Kodeksu Karnego, iż zaoferowane przez nas rozwiązanie spełnia wszystkie opisane powyżej wymogi i parametry techniczne.

|  |
| --- |
| **Osoby upoważnione do podpisania oświadczenia w imieniu Wykonawcy**  |
| Imię i Nazwisko | Data | Podpis |
|  |  |  |
|  |  |  |