ZAPYTANIE OFERTOWE

w postępowaniu prowadzonym
zgodnie z zasadą konkurencyjności

Zamówienie w ramach projektu pn *„Wdrożenie do firmy Paged Morąg SA. kompletnego cyberfizycznego systemu, umożliwiającego cyfryzację i robotyzację produkcji sklejki i wprowadzenie założeń przemysłu 4.0. na rzecz zwiększenia odporności do działania w warunkach kryzysowych”* współfinansowane z **KRAJOWEGO PLANU ODBUDOWY, A2.1.1 - Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach**

PRZEDMIOT ZAMÓWIENIA:
Zintegrowany system ESM/ITSM/MDM

ZAMAWIAJĄCY:
Paged Morąg S. A.
14-300 Morąg, ul. Mazurska 1,
NIP 7411378488, REGON 510445569

Zakład Morąg

kody CPV:
72260000-5 - Usługi w zakresie oprogramowania
48000000-8 Pakiety oprogramowania i systemy informatyczne
72268000-1 Usługi dostawy oprogramowania
32420000-3 - Urządzenia sieciowe,
48820000-2 – Serwery
48420000-8 Pakiety oprogramowania do zarządzania urządzeniami i zestawy pakietów oprogramowania

1. OPIS PRZEDMIOTU ZAMÓWIENIA

Załącznik „Specyfikacja Istotnych Warunków Zamówienia” opisuje szczegółowe wymagania dotyczące zamawianego systemu. W szczególności zapytanie obejmuje:

- dostawę licencji wieczystych na kompleksowy system zarządzania środowiskiem programowosprzętowym dla stacji roboczych i serwerów**;**
- dostawę sprzętu komputerowego i sieciowego umożliwiającego instalację dostarczanych systemów;

- przeprowadzenie niezbędnych szkoleń;
- zapewnienie wsparcia powdrożeniowego i rozwojowego.

W przypadku, gdzie Zamawiający posługuje się w opisie przedmiotu zamówienia, we wszystkich dokumentach i załącznikach opisujących przedmiot zamówienia nazwami konkretnych producentów, nazwami konkretnych produktów, znakami towarowymi, patentami czy pochodzeniem, należy to traktować jedynie jako pomoc w opisie przedmiotu zamówienia – mają one jedynie przybliżyć wymagania, których nie można było opisać przy użyciu dostatecznie dokładnych i zrozumiałych określeń. W każdym przypadku dopuszcza się użycie produktu równoważnego, który spełni minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcji i walorów użytkowych produktu wskazanego z nazwy.

W każdym przypadku dopuszcza się możliwość zastosowania materiałów, komponentów równoważnych wobec wskazanych w opisie przedmiotu zamówienia oraz załącznikach pod warunkiem zachowania ich zgodności z planowanym przeznaczeniem i obowiązującymi przepisami, które spełniają minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcje i walory użytkowe.

W związku z przyjętym harmonogramem realizacji inwestycji, w przypadku pytań lub wątpliwości co do przedmiotu zamówienia, prosimy o kierowanie zapytań najpóźniej do pięciu dni przed terminem składania ofert.

2. WARUNKI UDZIAŁU W POSTĘPOWANIU

Oferty mogą składać Wykonawcy, którzy:

3.1. dysponują potencjałem technicznym, koniecznym do należytego wykonania zamówienia;
3.2. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;
3.3. posiadają wykwalifikowaną kadrę, gotową do realizacji zamówienia;
3.4. Maksymalny czas realizacji zamówienia 20 tygodnie od dnia podpisania umowy.
3.5. posiadają niezbędną wiedzę i doświadczenie oraz zdolności techniczne i organizacyjne umożliwiające prawidłowe wykonanie przedmiotu zamówienia;
3.6. 3.6. nie są powiązani osobowo lub kapitałowo z Zamawiającym – przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Beneficjenta lub osobami wykonującymi w imieniu Beneficjenta czynności związanych z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:
   2.5.1. uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
   2.5.2. posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
   2.5.3. pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   2.5.4. pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
   2.5.5. pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

3. KRYTERIA OCENY OFERTY

Oferty będą oceniane wg następujących kryteriów:

3.1. 75% – cena;
3.2. 25% – termin dostawy i realizacji.

Z postępowania zostaną wykluczone oferty, które:

3.3. nie spełniają warunków umieszczonych w zapytaniu ofertowym, w tym w specyfikacji istotnych warunków zamówienia;
3.4. pochodzą od wykonawców mających powiązania osobowe lub kapitałowe z Zamawiającym;
3.5. zawierają istotne błędy w obliczeniu ceny lub cena oferty jest rażąco niska – w takiej sytuacji Zamawiający może poprosić o uzupełnienie oferty o dokumenty potwierdzające możliwość realizacji oferty w tej cenie;
3.6. zostaną złożone po wskazanym terminie;
3.7. będą zawierały zbyt długi termin realizacji uniemożliwiający finansowanie w ramach projektu KPO.

4. OPIS SPOSOBU PRZYZNAWANIA PUNKTACJI ZA SPEŁNIENIE DANEGO KRYTERIUM OCENY OFERTY.

4.1. kryterium ceny uwzględniające wszystkie niewykluczone oferty, zgodnie ze wzorem:
$C_{\%} = \frac{3(C_n - C_{min})}{4(C_{max} - C_{min})}$, w szczególności: najniższa cena 75%, najwyższa cena 0%;

4.2. termin dostawy i realizacji liczony od dnia podpisania umowy:
   a. 25% – do 7 tygodni;
   b. 15% – 7-10 tygodni;
   c. 5% – 10-14 tygodni;
   d. 0% – powyżej 14 tygodni.

5. TERMIN SKŁADANIA OFERT

Oferty prosimy składać do 28 lutego 2025 r na adresy:

tomasz.wisniewski@paged.pl
tomasz.oldakowski@paged.pl
krzysztof.mykowski@paged.pl

6. INFORMACJA O MOŻLIWOŚCI SKŁADANIA OFERT CZĘŚCIOWYCH

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

7. INFORMACJĘ O PLANOWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH

Zadamawiający nie planuje zamówień uzupełniających.

8. TERMIN REALIZACJI UMOWY

Maksymalnie 20 tygodni od dnia podpisania umowy.

9. ISTOTNE POSTANOWIENIA UMOWY I WARUNKI ZMIANY ISTOTNYCH POSTANOWIEŃ UMOWY

Zamawiający wymaga, aby Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, zawarł umowę zgodnie z treścią zapytania. Wykonawca ma prawo zaproponować wzór umowy stosowany w praktyce handlowej. Zamawiający dopuszcza wypłatę zaliczki na poczet realizacji zamówienia w kwocie uzgodnionej z Wykonawcą nie wyższą niż 50% ceny ujawnionej przez Wykonawcę w ofercie.
Podstawą rozliczeń między stronami będą faktury.

10. WARUNKI EWENTUALNEGO ODSTĄPIENIA OD ZAWARCIA UMOWY

W przypadku gdy zaoferowana cena przekracza kwotę środków przeznaczonych przez Zamawiającego na realizację zamówienia, Zamawiający może unieważnić postępowanie i odstąpić od podpisania umowy.

11. ZAŁĄCZNIKI

1. Formularz oferty;
2. Oświadczenie o spełnieniu wszystkich warunków udziału w postępowaniu;
3. Oświadczenie o braku powiązań osobowych i kapitałowych;
4. Specyfikacja istotnych warunków zamówienia (SIWZ);

Załącznik 1 – Formularz oferty

W odpowiedzi na Zapytanie Ofertowe dot. Zintegrowanego systemu ESM/ITSM/MDM składamy poniższą ofertę:

Dane oferenta	
Nazwa	
Adres	
NIP / REGON	
Nr KRS lub CEIDG	
Nr rejestrowy dla kraju innego niż PL	
Rodzaj podmiotu	
Dane osoby kontaktowej	
Imię i nazwisko	
Adres e-mail	
Telefon	
Określenie przedmiotu oferty (zakres i szczegółowy opis oferowanych usług / produktów)	
Określenie do kryteriów wyboru ofert	
Wartość oferty netto w PLN	
Termin realizacji liczony w tygodniach od daty podpisania umowy	

Załącznik 2 – Oświadczenie o spełnieniu wszystkich warunków udziału w postępowaniu

……,dn……

Wykonawca
(Nazwa, adres)

……..

……..

Oświadczenie o spełnieniu wszystkich warunków udziału w postępowaniu

do zapytania ofertowego dot. Zintegrowanego systemu ESM/ITSM/MDM

1. Dysponuję potencjałem technicznym, koniecznym do należytego wykonania zamówienia.
2. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
3. Posiadam wykwalifikowaną kadrę, gotową do realizacji zamówienia.
4. Posiadam niezbędną wiedzę i doświadczenie oraz zdolności techniczne i organizacyjne umożliwiające prawidłowe wykonanie przedmiotu zamówienia.
5. Oświadczam(y), że nie jestem(eśmy) powiązani z Zamawiającym osobowo lub kapitałowo.

……
data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik 3 – Oświadczenie o braku powiązań osobowych i kapitałowych

Wykonawca/pieczątka:

……,dn……

NIP ……

REGON ……

Oświadczenie o braku powiązań osobowych i kapitałowych

w odpowiedzi na zapytanie ofertowe dot. Zintegrowanego systemu ESM/ITSM/MDM

Oświadczam(y), że nie jestem(eśmy) powiązani z Zamawiającym osobowo lub kapitałowo.

Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w mieniu zamawiającego lub osobami wykonującymi w imieniu zamawiającego czynności związane z przygotowaniem i przeprowadzaniem procedury wyboru wykonawcy, a wykonawcą, polegające w szczególności na:

1) uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
2) posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
3) pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
4) pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
5) pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

……
data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik 4. – Specyfikacja istotnych warunków zamówienia (SIWZ)

……,dn……

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Wszystkie poniższe wymagania opisują minimalne parametry, które musi spełniać oferta.

1. Przedmiotem zamówienia są:
   - 1.1. dostawa licencji wieczystej na kompleksowy system zarządzania środowiskiem programowosprzętowym dla stacji roboczych i serwerów składający się z niżej wymienionych grup funkcjonalności (zwanych dalej pojedynczo **modułem**, lub łącznie **modułami**):
     - 1.1.1. moduł do zarządzania środowiskiem programowo-sprzętowym ze wsparciem producenta na 60 miesięcy;
     - 1.1.2. licencje wieczyste wraz z 60-miesięcznym okresem wsparcia producenta – w okresie wsparcia Zamawiający będzie miał prawo do aktualizacji systemu zgodnie ze wsparciem producenta;
     - 1.1.3. moduł do obsługi zgłoszeń serwisowych i zarządzania usługami IT;
     - 1.1.4. moduł tworzenia raportów z infrastruktury informatycznej;
     - 1.1.5. moduł/aplikacja do analizy i raportowania infrastruktury Active Directory;
     - 1.1.6. moduł/aplikacja do zarządzania i audytu serwera pocztowego Exchange- serwerów lokalnych („on-premise") oraz w chmurze („online").
   - 1.2. dostawa sprzętu komputerowego i sieciowego umożliwiającego instalację dostarczanego oprogramowania oraz wykorzystanie w pełni wdrażanych funkcjonalności wraz z licencjami;
   - 1.3. przeprowadzenie szkolenia dla max. 20 osób w czasie ustalonym z Zamawiającym lecz nie później niż w dniu zakończenia wdrożenia licencji;
   - 1.4. zapewnienie 60 miesięcznego wsparcia powdrożeniowego, w tym 70 roboczogodzin na prace rozwojowe Systemu;
   - 1.5. wdrożony system i moduły muszą być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf- COTS).
2. Ogólne wymagania odnośnie wdrażanego systemu
   - 2.1. System musi umożliwiać:
     - 2.1.1. zarządzanie minimum 800 stacjami roboczymi (komputery stacjonarne i przenośne) oraz urządzeniami mobilnymi;
     - 2.1.2. zarządzanie urządzeniami mobilnymi (Android, iOS) wymiennie do stacji roboczych w ramach tej samej licencji;
     - 2.1.3. jednoczesną pracę 12 techników.
   - 2.2. Wszystkie składniki systemu będą używały oprogramowania zainstalowanego lokalnie („on premise"), nie dopuszcza się realizacji jakichkolwiek funkcji poprzez rozwiązania chmurowe.
   - 2.3. W okresie wsparcia Wykonawcy, Zamawiający będzie miał prawo do aktualizacji systemu zgodnie ze wsparciem producenta.
   - 2.4. Wszystkie licencje dostarczone w ramach wdrażanego systemu będą wieczyste, niewyłączne, możliwe do wykorzystania w ramach organizacji Zamawiającego.
   - 2.5. Oprogramowanie niezbędne do pracy systemu będzie instalowane na serwerach z rodziny Windows Server 2019 lub nowszym, na które Zamawiający posiada licencje. Konfiguracja

serwerów zostanie wprowadzona wg zaleceń producenta i doświadczenia Wykonawcy, co zostanie ustalone na spotkaniu przed wdrożeniem.

2.6. Wszystkie funkcjonalności po stronie technika będą realizowane przez przeglądarkę internetową. Nie dopuszcza się, by funkcje wymagane były realizowane przy użyciu narzędzi innych niż dostarczonych w ramach wdrożenia systemu.

2.7. System zapewni funkcję udzielania zdalnego wsparcia poprzez możliwość przejęcia pulpitu urządzenia w sieciach LAN/WAN jak również dla klientów zdalnych, poza LAN/WAN:

2.7.1. zestawienie sesji zdalnej z użytkownikiem będzie wymagało jego zgody poprzez akceptację stosownego komunikatu;

2.7.2. system umożliwi rejestrację zestawianych sesji zdalnych;

2.7.3. zestawianie sesji zdalnych nie będzie wymagało od operatora konieczności posiadania podwyższonych uprawnień, a w szczególności uprawnień administratora systemu;

2.7.4. system musi zapewnić poprawną obsługę mechanizmu podnoszenia uprawnień (UAC).

2.8. System do pracy będzie wykorzystywał silnik bazy danych, na posiadanej przez Zamawiającego licencji Microsoft SQL Serwer 2019 Standard lub PostgreSQL, nie wymagającą płatnej licencji (ograniczenia bezpłatnej dystrybucji nie mogą zakłócać lub ograniczać funkcjonowania systemu).

2.9. System będzie posiadał wbudowany mechanizm backupu bazy danych oraz jej odtwarzania.

2.10. System będzie poprawnie działał z systemami:

2.10.1. Windows (Vista i nowsze);

2.10.2. Linux (Ubuntu 10.04, Red Hat Enterprise Linux 8, Debian 7, Linux Mint 13, OpenSuse 11, Suse Linux Enterprise Server 11 i nowsze);

2.10.3. macOS (wersja 10.7 i nowsze).

2.11. Opisane oprogramowanie będzie posiadało to samo centrum kompetencyjne i deweloperskie.

3. Wymagania funkcjonalne dla modułu do zarządzania środowiskiem aktualizacji dla stacji roboczych i serwerów

3.1. Interfejs rozwiązania musi być w języku polskim lub angielskim.

3.2. Zarządzanie powinno się odbywać z wykorzystaniem agenta instalowanego na urządzeniu:

3.2.1. wykrywanie oraz instalacja agentów powinna się odbywać automatycznie na podstawie synchronizacji z Active Directory, dla wybranego zakresu adresacji sieci IPv4;

3.2.2. powinny istnieć reguły dopuszczające zarządzanie urządzeniem w systemie na podstawie m.in. jego członkostwa w dopuszczonej domenie Active Directory;

3.2.3. instalacja agenta powinna skutkować rejestracją zarządzanego urządzenia w module do zarządzania środowiskiem sprzętowym.

3.3. Każda lokalizacja w ramach infrastruktury Zamawiającego, będzie mogła być (w ramach nabytej licencji) wyposażona w serwer lokalny modułu zarządzania środowiskiem programowosprzętowym służący do dystrybucji niezbędnych instalatorów pobieranych przez agentów. Zamawiający przewiduje możliwość instalacji w 4 lokalizacjach na serwerach opartych o Windows Server.

3.4. Do zarządzania wszystkimi zarejestrowanymi urządzeniami będzie służyć jedna konsola administracyjna www, bez względu na przypisanie do podsieci LAN/WAN.

3.5. Automatyczne wdrażanie poprawek dla Windows, Mac, Linux i aplikacji firm trzecich:

3.5.1. Posiada możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym;
3.5.2. Funkcje wdrażania poprawek obejmują co najmniej: systemy operacyjne Microsoft Windows, pakiet Microsoft Office, Microsoft Edge, Microsoft Teams, Google Chrome, Mozilla Firefox, Adobe Reader; 7 zip, winrar itp.
3.5.3. Posiada wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia, w oparciu o brakujące poprawki systemowe;
3.5.4. Monitorowanie statusów poprawności dystrybucji i implementacji na stacji roboczej.

3.6. Centralne zarządzanie oprogramowaniem:
3.6.1. Możliwość definiowania prostych i sekwencyjnych instalacji (ciągu poleceń składających się na wieloetapowe wdrożenie oprogramowania);
3.6.2. Możliwość importu definicji/komend z pliku msi generujący możliwe parametry instalacji oprogramowania: na urządzenie (widoczny instalator dla użytkownika), na urządzenie ukryte, na urządzenie odinstalowanie, na użytkownika (widoczny instalator), na użytkownika ukryte, na użytkownika odinstalowanie;
3.6.3. Możliwość uruchamiania instalatorów w kontekście zalogowanego użytkownika, lub zalogowanego użytkownika z uprawnieniami administratora;
3.6.4. Możliwość automatycznego odinstalowywania oprogramowania na podstawie czarnych list;
3.6.5. Możliwość zablokowania uruchamiania aplikacji na podstawie ścieżki uruchamiania lub wartości hash;
3.6.6. Dystrybucja oprogramowania względem tworzonych kolekcji komputerów lub użytkowników, tworzonych w systemie lub na podstawie członkostwa w grupie Active Directory;
3.6.7. Monitorowanie statusów poprawności dystrybucji i implementacji na stacji roboczej.

3.7. Możliwość zarządzania systemami operacyjnymi MS Windows, Linux oraz Mac OS:
3.7.1. Dla zarządzanych urządzeń będzie wykrywał sprzęt i zainstalowane oprogramowanie;
3.7.2. Możliwość wdrażania polityk konfiguracji dla systemów Windows, w szczególności polityk dostępu do interfejsu USB, zużycia energii, konfiguracji drukarek i przeglądarek Mozilla Firefox, Google Chrome oraz Microsoft Edge;
3.7.3. Możliwość konfiguracji polityk dostępu do USB, w szczególności urządzeń do przechowywania danych, ustawianych względem rodzaju urządzeń, ich indywidualnym identyfikatorze, producencie, pozwalające na zastosowanie ustawień przynajmniej: brak dostępu, tylko odczyt, pełny dostęp;
3.7.4. Możliwość zdalnego uruchamiania i wyłączania stacji roboczych w LAN;
3.7.5. Możliwość uruchamiania zdalnego zarządzania dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, który pozwoli m.in. na:
- podgląd i zamykanie uruchomionych procesów na stacji roboczej;
- podgląd, uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej;
- uruchamianie zdalnego wiersza poleceń;
- podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej;
- przegląd logów systemowych stacji roboczej;
- podgląd menedżera urządzeń;
- podgląd udziałów sieciowych.

3.8. Moduł do zarządzania środowiskiem programowo-sprzętowym powinien umożliwiać raportowanie:

3.8.1. Active Directory – aktualnie zalogowani użytkownicy, nieaktywni użytkownicy, historia logowania użytkownika, historia logowania użytkowników na stacji roboczej.

3.8.2. Poprawki- brak zainstalowanych poprawek względem stacji roboczej lub poprawki, lista obsługiwanych poprawek, poprawki wymagające zatwierdzenia, systemy wymagające ponownego uruchomienia.

3.8.3. Inwentaryzacja:

- sprzęt – komputery wg systemu operacyjnego, wg producenta, pamięci, wykorzystania dysku, okresu użytkowania, typu urządzenia, zmapowane dyski, kończąca się gwarancja, wygasła gwarancja, ostatnia data komunikacji z serwerem;
- oprogramowanie – lista zainstalowanego oprogramowania wg komputera, oprogramowanie wg daty instalacji, oprogramowanie z czarnej listy, używane oprogramowanie, klucze produktów, komputery wg wymaganego oprogramowania;
- bezpieczeństwo – szczegóły oprogramowania antywirusowego, szczegóły BitLocker, szczegóły zapory sieciowej;
- pliki multimedialne – szczegóły plików wg kategorii, szczegóły plików wg rozszerzeń;
- USB – wykorzystanie urządzeń USB.

3.8.4. Generowanie raportów w formatach PDF, XLSX, z możliwością wysyłania na mail wg ustawionego harmonogramu.

3.8.5. Tworzenie niestandardowych raportów na podstawie danych przechowywanych przez Moduł do zarządzania środowiskiem programowo-sprzętowym.

3.9. Moduł do zarządzania środowiskiem programowo-sprzętowym powinien umożliwiać dystrybucję systemów operacyjnych:

3.9.1. Realizowane za pomocą zintegrowanego modułu, umożliwiającego przechwycenie obrazu systemu i dystrybucję na stacje robocze;

3.9.2. Instalacja systemu operacyjnego przez PXE, wygenerowane ISO oraz utworzony bootowalny nośnik USB;

3.9.3. Tworzenie i edytowanie obrazów na podstawie wskazanego obrazu ISO;

3.9.4. Tworzenie i aktualizacja bazy sterowników i stosowanie wraz z dystrybucją obrazu systemu operacyjnego;

3.9.5. W przypadku gdy obraz ISO zawiera w sobie kilka edycji tego samego systemu operacyjnego, oprogramowanie będzie miało możliwość jego wyboru w definicji dystrybucji (np. Windows 11 Pro, lub Enterprise);

3.9.6. Umożliwia tworzenie sekwencji zadań, w której można zdefiniować sposób partycjonowania dysku, instalację wskazanego systemu operacyjnego, użycie wybranych sterowników względem specyfikacji stacji roboczej, zastosowanie aktualizacji, wgranie wymaganego oprogramowania, nadanie nazwy, dodanie do domeny;

3.9.7. Możliwe do skonfigurowania uruchamianie instalacji z PXE po wprowadzeniu hasła;

3.9.8. Możliwość stosowania filtrów dla stacji roboczej, by w PXE wyświetlały się wyłączenie obrazy spełniające wymagania np. określony MAC, nazwa, model komputera itp.;

3.9.9. Możliwość migrowania profili użytkownika (zabezpieczenie danych na jednym komputerze i wgranie na drugim podczas instalacji systemu operacyjnego);
3.9.10. Zapisywanie logów z instalacji systemu operacyjnego i wskazywanie statusów jego powodzenia.

3.10. Moduł do zarządzania środowiskiem programowo-sprzętowym powinien umożliwiać zarządzanie bezpieczeństwem:
3.10.1. Zarządzanie i kontrola funkcji BitLocker w tym zarządzanie kluczami i odzyskiwaniem:
- tworzenie polis, w tym określenie które dyski i urządzenia mają być szyfrowane, metoda szyfrowania, uwzględnienie stacji roboczych bez TPM, miejsce przechowywania kluczy i harmonogram aktualizacji klucza;
- przypisywanie polis do komputerów lub grup komputerów;
- statusy szyfrowania stacji roboczych;
- obsługa odzyskiwania kluczy.

3.11. Moduł do zarządzania środowiskiem programowo-sprzętowym powinien umożliwiać podział ról administracyjnych w szczególności:
3.11.1. administrator,
3.11.2. użytkownik z dostępem do odczytu (audytor),
3.11.3. gość,
3.11.4. zarządzający urządzeniami,
3.11.5. zarządzający poprawkami,
3.11.6. zarządzający oprogramowaniem,
3.11.7. zarządzający dystrybucją systemów operacyjnych,
3.11.8. zarządzający bezpieczeństwem.

3.12. Logowanie do oprogramowania powinno być możliwe z wykorzystaniem konta lokalnego, lub Active Directory (w tym umożliwiać logowanie SSO).
3.13. Oprogramowanie powinno umożliwiać ustawienie logowania dwuskładnikowego.
3.14. Blokowanie uruchamiania określonego typu plików i rozszerzeń.
3.15. Raporty z użytkowania oprogramowania.
3.16. Logowanie do systemu poprzez MFA
3.17. System musi posiadać interfejs programistyczny API do dalszej obsługi logów typu SIEM.
3.18. System powinien posiadać funkcje Geofencing oraz Conditional Exchange Access.
3.19. System rozpoznaje stacje robocze w ramach Active Directory
3.20. System powinien umożliwiać instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.
3.21. System powinien umożliwiać tworzenie list aplikacji, które będą mogły być instalowane przez samego użytkownika z poziomu stacji roboczej, tzw. Portal samoobsługowy/ sklep
3.22. System powinien posiadać wbudowane funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach, w szczególności rozpoznaje sekwencje instalacji.
3.23. Funkcje wdrażania łat obejmują co najmniej oprogramowanie: systemy operacyjne Windows: 10, 11, Windows Server 2008, 2012, 2016, 2022, Systemy MacOS (wersja 10.7 i wyższe), Microsoft Office, Google Chrome, Opera, Skype, Mozilla Firefox, Adobe Reader, Adobe Acrobat, Adobe Shockwave Player, Adobe Flash Player, Java, inne
3.24. System powinien posiadać możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.

3.25. System powinien posiadać wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.
3.26. Architektura systemu umożliwia zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego.
3.27. System powinien posiadać wbudowane narzędzia zarządzania zasobami IT, w szczególności rozpoznaje komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.
3.28. System powinien posiadać wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz ma możliwość włączenia opcji nagrywania tych sesji.
3.29. System powinien umożliwiać wdrażanie polityk konfiguracji dla systemów Windows, w szczególności polityk dostępu do interfejsu USB, zużycia energii, konfiguracji drukarek i przeglądarek Internet Explorer, Mozilla Firefox, Google Chrome oraz Microsoft Edge.
3.30. Konfiguracja polityk dostępu do USB umożliwia blokowanie co najmniej poniższych typów urządzeń, a także ma możliwość wykluczania z listy zablokowanych konkretnych urządzeń o danym identyfikatorze urządzenia lub danego dostawcy, a dla dysków przenośnych tych, które są szyfrowane za pomocą rozwiązania BitLocker: Mysz, Stacja dysków (takie jak napędy USB, zewnętrzne dyski twarde), CD ROM, Urządzenia przenośne (takie jak telefony komórkowe, kamery cyfrowe i przenośne odtwarzacze multimedialne), Dyskietka, Bluetooth, Obraz (takie jak kamery USB i skanery), Drukarka, Modem, Urządzenia USB Apple (takie jak iPad, iPhone i iPod, łączące się z programem iTunes)
3.31. System powinien posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.
3.32. System powinien posiadać rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami.
3.33. System powinien posiadać możliwość dodania nowego użytkownika systemu z uwierzytelnianiem lokalnym lub Active Directory wraz z obsługą SSO oraz przy wykorzystaniu autoryzacji SAML
3.34. System powinien posiadać możliwość włączenia opcji uwierzytelniania dwuskładnikowego, dzięki któremu dostęp do systemu odbywać się będzie poprzez podanie swojego hasła dostępu (lokalnego lub Active Directory) oraz drugiego składnika w postaci jednorazowego hasła wysyłanego na maila (funkcja OTP) lub tokenu z aplikacji uwierzytelniającej (np. Google Authenticator).
3.35. System powinien posiadać możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.
3.36. System powinien posiadać mechanizm dwuskładnikowej autoryzacji dla opcji odinstalowania manualnego agenta.
3.37. System powinien umożliwiać dodawanie i rozliczanie licencji aplikacji.
3.38. System powinien umożliwiać wykrywanie zakazanego oprogramowania i uruchamia działania naprawcze, w tym automatyczne odinstalowanie niepożądanej aplikacji.
3.39. System powinien posiadać możliwość włączenia pomiaru wykorzystania wskazanej aplikacji.
3.40. System powinien posiadać możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na ścieżce aplikacji lub wartości hash.
3.41. System powinien umożliwiać uruchamianie zdalnego Menedżera Systemu dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, który pozwoli na: podgląd i zamykanie uruchomionych procesów na stacji roboczej, podgląd,

uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej, uruchamianie zdalnego wiersza poleceń, podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej, przegląd logów systemowych stacji roboczej, podgląd menedżera urządzeń, podgląd udziałów sieciowych.

3.42. System powinien umożliwiać generowanie następujących raportów:
- 3.42.1. raporty Active Directory, aktualnie zalogowani użytkownicy, często zalogowani użytkownicy, rzadko logujący się użytkownicy, nieaktywni Użytkownicy, historia logowania użytkownika, historia logowania użytkowników na poszczególnych komputerach;
- 3.42.2. wykorzystania aplikacji w skali całej organizacji;
- 3.42.3. raporty dotyczące poprawek – Narażone poprawki, Obsługiwane poprawki, Brakujące poprawki czekające na zatwierdzenie, Systemy wymagające ponownego uruchomienia;
- 3.42.4. raporty inwentaryzacji – Komputery wg systemu operacyjnego, Komputery wg producenta, Komputery wg pamięci, Komputery wg wykorzystania dysku, Komputery wg wieku, Komputery wg typu urządzenia, Zmapowane dyski logiczne;
- 3.42.5. raporty dotyczące oprogramowania – Oprogramowanie według producenta, Ostatnio zainstalowane oprogramowanie, Niedozwolone oprogramowanie, Wykorzystanie oprogramowania przez komputer, Klucze produktu oprogramowania;
- 3.42.6. raporty dotyczące licencji – Zgodność licencji, Licencje do odnowienia;
- 3.42.7. raporty dotyczące gwarancji – Gwarancja niedługo wygaśnie, Gwarancja wygasła Niezidentyfikowane komputery;
- 3.42.8. raporty bezpieczeństwa – szczegóły Antivirus, szczegóły BitLocker, szczegóły firewall.

3.43. System powinien umożliwiać planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres mailowy.

3.44. System powinien umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.

3.45. System powinien umożliwiać zarządzanie flotą urządzeń mobilnych typu smartfony i tablety z zainstalowanymi systemami operacyjnymi: Android 4.0 i wyższe, iOS 4 i wyższe, Windows Phone 8.1 i wyższe, Chrome OS 57.0 i wyższe, tvOS 7.0 i wyższe.

3.46. System powinien pozwalać zatwierdzać uprawnienia żądane przez aplikacje Mac, konfigurując zasady kontroli preferencji polityki prywatności.

3.47. System powinien posiadać moduł zarządzania profilami.

3.48. System powinien umożliwiać konfigurację polis/profili- konfiguracja ustawień polis dostępu do zasobów organizacyjnych.

3.49. System powinien umożliwiać nakładanie restrykcji – szyfrowanie pamięci wewnętrznej urządzenia, ograniczanie użytkowania kamery, Youtube, przeglądarki Safari, itp.

3.50. System powinien posiadać funkcję Organizacyjny dostęp - zapewnia dostęp do organizacyjnych zasobów jak mail, Wi-Fi, VPN..

3.51. System powinien umożliwiać tworzenie grup urządzeń- tworzenie logicznych grup urządzeń w oparciu o departamenty, lokalizacje, w celu rozróżnienia urządzeń organizacyjnych od BYOD (Bring Your Own Device) i wdrażania polis, restrykcji i dystrybucji aplikacji do wszystkich urządzeń.

3.52. System powinien posiadać moduł zarządzania aplikacjami pozwalający na: zarządzanie i dystrybucja własnych aplikacji i AppStore, integracja z programem Apple VPP, publikacja aplikacji w katalogu aplikacji dla użytkowników na potrzeby samodzielnej instalacji.

3.53. System powinien pozwalać na dystrybucję certyfikatów CA na urządzenia z systemem iOS oraz Android, przy użyciu profilu certyfikatu.
3.54. System powinien pozwalać na konteneryzację urządzeń z Androidem w wersji 5.0 lub nowszej, używając Android for Work.
3.55. System powinien pozwalać na konfiguracje uprawnień i konfiguracje aplikacji za pomocą Android for Work.
3.56. System powinien pozwalać na cichą instalację aplikacji Sklepu Play przy użyciu Android for Work.
3.57. System powinien pozwalać na rejestrację urządzeń mobilnych z systemem Windows.
3.58. System powinien pozwalać na reset urządzenia nawet po wygaśnięciu poświadczeń AD.
3.59. System powinien pozwalać na powiadamia Administratorów pocztą, gdy zarządzanie urządzeniem zostało odwołane przez użytkowników.
3.60. System powinien pozwalać na obsługę Trybu kiosku dla urządzeń, które nie obsługują Android for Work.
3.61. System powinien pozwalać na zmianę nazwy urządzenia podczas przekazywania urządzenia.
3.62. System powinien pozwalać na nawiązanie sesji zdalnej na urządzenia Android oraz IOS.
3.63. System powinien pozwalać na import certyfikatów SSL z rozszerzeniami takimi jak .jks i .keystore.
3.64. System powinien pozwalać na dystrybucję certyfikatów CA na urządzenia Windows.
3.65. System powinien umożliwiać wybór pomiędzy domyślnym programem uruchamiającym urządzenia a programem uruchamiającym MDM dla Kiosku na urządzeniach z Androidem.
3.66. System powinien umożliwiać zdalne ponowne uruchamianie urządzeń za pomocą jednego kliknięcia.
3.67. System powinien umożliwiać konfigurację ustawień prywatności urządzenia, określenie rodzaju danych, które można gromadzić, poleceń do wykonania na urządzeniu itp.
3.68. System powinien posiadać możliwość tworzenia zadań dystrybucji pozwalających na automatyzacje procesu dystrybucji obrazów systemów.
3.69. System powinien posiadać możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalający na dystrybucję obrazu przy użyciu kodu, lub wybieranych systemów z dostępnej listy komputerów.
3.70. System powinien pozwalać na Import komputerów z pliku – CSV.
3.71. System wspiera następujące metody dystrybucji obrazów: Multicast, Unicast oraz pozwala na tworzenie harmonogramu tejże dystrybucji.
3.72. System powinien posiadać możliwość przechowywania wcześniej zapisanych obrazów w swoim repozytorium.
3.73. System powinien posiadać możliwość przechowywania informacji o sterownikach, a także zapewnia ich dystrybucje w obrazach.
3.74. System powinien posiadać możliwość tworzenia bootowalnych mediów a także ich edycję: · PXE, · ISO,· USB.
3.75. System powinien posiadać repozytorium możliwych do zainstalowania aplikacji po procesie dystrybucji obrazu a także posiada możliwość edycji tychże aplikacji System powinien posiadać możliwość migrowania profili użytkownika podczas dystrybucji obrazów System powinien posiadać możliwość generowania logów a także wyświetlania listy statusów i wykonanych akcji.

4. Moduł/aplikacja dla powyższego oprogramowania dotyczący bezpieczeństwa do zarządzania środowiskiem IT Zamawiającego powinien umożliwiać
   4.1. Zarzadzanie i kontrola rozwiązania BitLocker służących do zabezpieczania dysków twardych na stacjach roboczych.

4.2. Interfejs oprogramowania oraz konfiguracji jest w całości dostępny z poziomu przeglądarki internetowej (Internet Explorer w wersji 10 lub nowszej, Mozilla 44 lub nowszej, Chrome 47 lub nowszej) bez potrzeby instalacji tzw. grubego klienta.
4.3. Dopuszczalnym językiem interfejsu jest język polski.
4.4. Architektura systemu powinna być agentowa.
4.5. System powinien pozwalać na zarządzanie i kontrolę nad urządzeniami zewnętrznymi w zakresie:
  4.5.1. blokowania, zezwalania i zezwalania zaufanym urządzeniom takim jak:
    - wymienne urządzenia pamięci masowej;
    - CDROM;
    - urządzenia przenośne systemu Windows;
    - urządzenia Apple;
    - bluetooth;
    - drukarka;
    - modem;
    - adapter sieci bezprzewodowej;
    - urządzenia do przetwarzania obrazów;
    - porty szeregowe (COM);
    - czytnik kart inteligentnych;
    - mysz i klawiatura;
  4.5.2. system powinien pozwalać na śledzenie plików w zakresie:
    - utworzenia;
    - otwarcia;
    - usunięcia;
    - zmiany nazwy;
    - modyfikacji;
    - przeniesienia;
    - kopiowania;
  4.5.3. system powinien pozwalać na generowanie alertów;
  4.5.4. system powinien pozwalać na tworzenie listy zaufanych urządzeń;
  4.5.5. system powinien pozwalać na tworzenie dostępu tymczasowego dla zaufanych urządzeń.
4.6. System powinien pozwalać na zarzadzanie dyskami z wykorzystaniem technologii BitLocker:
  4.6.1. system powinien pozwalać:
    - zaszyfrować dysk;
    - wybrać zakres szyfrowania – całego dysku lub tylko użytej przestrzeni dyskowej;
    - szyfrować urządzenia, które nie posiadają TPM (Trusted Platform Module);
    - wymuszać opóźnienie restartu przez użytkownika po dokonanym szyfrowaniu;
    - przechowywać klucze do odtworzenia (odszyfrowania) na kontrolerze domeny;
    - tworzenie grup z wyszczególnionymi systemami podlegającym pod konkretne polisy;
    - weryfikację w pulpicie nawigacyjnym wszystkich zarządzanych systemów wraz z aktualnym statusem szyfrowania;
    - weryfikację systemów z TPM;
    - odzyskiwanie tzw. Recovery Key;
    - wdrażanie oparte na kryteriach przy użyciu dynamicznej grupy niestandardowej;
  4.6.2. aplikacja powinna wymuszać rotacyjne zmiany klucza w określonym przedziale czasowym.

5. Moduł/aplikacja do analizy i raportowania infrastruktury Active Directory

5.1. System powinien działać bezagentowo;
5.2. Aplikacja musi pochodzić od tego samego producenta co całość zamawianego systemu;
5.3. Aplikacja powinna objąć audytem 5 kontrolerów domeny i 2 serwery plików zamawiającego działające w ramach jednej domeny.
5.4. Moduł do analizy i raportowania infrastruktury Active Directory powinien zostać dostarczony ze wsparciem producenta na 60 miesięcy;
5.5. System powinien działać na systemach z rodziny Windows;
5.6. System powinien pozwalać na podłączenie certyfikatu, w formacie .PFX oraz Java keystore;
5.7. System powinien działać w formie aplikacji Internetowej;
5.8. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych;
5.9. System powinien działać na pojedynczej bazie danych;
5.10. System powinien posiadać wbudowane skrypty, które pozwalają na: backup bazy danych, odtworzenie bazy danych, zmianę bazy danych;
5.11. System powinien używać jednego konta do połączenia z domeną;
5.12. System powinien posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację Aplikacji.
5.13. System powinien pozwalać na zmianę portu HTTP / HTTPS z poziomu interfejsu graficznego.
5.14. System powinien umożliwiać audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące:
    5.14.1. wszystkich zmian plików i folderów;
    5.14.2. plikach zmodyfikowanych;
    5.14.3. plikach usuniętych;
    5.14.4. plikach przeniesionych;
    5.14.5. plikach utworzonych.
5.15. System powinien umożliwiać analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie , a w szczególności:
    5.15.1. nietypową aktywność danego użytkownika;
    5.15.2. nietypową aktywność użytkownika na serwerze;
    5.15.3. nietypową ilość prób np. logowań, Nietypowe godziny logowań użytkowników;
    5.15.4. nietypowe działania na plikach.
5.16. System powinien umożliwiać zbiorcze audytowanie środowiska Active Directory oraz posiada wbudowane raporty dotyczące:
    5.16.1. nieudanych próby zalogowania do środowiska domenowego;
    5.16.2. sumaryczny raport dotyczący nieudanych prób logowania w domenie na podstawie przyczyny błędu logowania;
    5.16.3. stacji roboczych;
    5.16.4. serwerów;
    5.16.5. kontrolerów domen;
    5.16.6. poprawne logowanie użytkowników wraz z pełną historią logowania;
    5.16.7. nieudane próby logowania na serwery Radius oraz historię logowań.
5.17. Zmiany dokonywane na kontach użytkowników, a w szczególności:
    5.17.1. tworzenie kont;
    5.17.2. usuwanie kont;
    5.17.3. dezaktywacja kont;
    5.17.4. modyfikacja haseł;

5.17.5. spis zablokowanych użytkowników;
5.17.6. historię użytkowników;
5.17.7. audyt zmian w grupie obiektów;
5.17.8. w grupie bezpieczeństwa;
5.17.9. operacje związane z tworzeniem i usuwaniem grup.

5.18. Raportowanie użytkowników zagnieżdżonych w innych grupach.
5.19. Raport aktywności użytkowników oraz dezaktywacji stacji roboczych przez wylogowanie lub wygaszacz ekranu.
5.20. Zmiany dokonane na obiektach komputerów, a w szczególności:
5.20.1. tworzenie kont,
5.20.2. usuwanie kont;
5.20.3. dezaktywację kont;
5.20.4. historię kont.
5.21. Audyt zmian w OU, a w szczególności:
5.21.1. tworzenie OU;
5.21.2. usuwanie OU;
5.21.3. listę modyfikowanych OU;
5.21.4. historię OU.
5.22. Audyt zmian w zasadach grupowych, a w szczególności:
5.22.1. tworzenie GPO;
5.22.2. usuwanie GPO;
5.22.3. listę zmodyfikowanych GPO;
5.22.4. historia GPO;
5.22.5. zaawansowane zmiany w GPO.
5.23. System musi umożliwiać przesłanie zaawansowanych raportów GPO do systemu SIEM,
5.24. System musi umożliwiać Audyt zmian uprawnień, a w szczególności:
5.24.1. uprawnienia dotyczące poziomu dostępu do domeny;
5.24.2. uprawnienia zmian OU;
5.24.3. uprawnienia zmian w kontenerach;
5.24.4. uprawnienia zmian w GPO;
5.24.5. uprawnienia zmian użytkowników;
5.24.6. uprawnienia zmian grup;
5.24.7. uprawnienia zmian komputerów;
5.24.8. uprawnienia zmian DNS;
5.24.9. zmiany w DNS'ach;
5.24.10. śledzenie zmian nazw użytkowników / komputerów / grup.
5.25. System powinien pozwalać na zbiorcze audytowanie zmian na serwerach plików, a w szczególności:
5.25.1. Windows;
5.25.2. Windows file Cluster;
5.25.3. EMC;
5.25.4. Net App;
5.25.5. Hitachi NAS;
5.25.6. QNAP.
5.26. System powinien posiadać możliwość budowania własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania.
5.27. System potrafi audytować wydruki, w tym:
5.27.1. kto wykonywał wydruk;

5.27.2. jaki plik drukował;
5.27.3. kiedy wykonał wydruk;
5.27.4. ile kopii wykonał;
5.27.5. jaki był rozmiar pliku;
5.27.6. ile stron pliku zostało wydrukowane;
5.27.7. użytą drukarkę;
5.27.8. na którym serwerze znajduje się drukarka.

5.28. Raporty zgodności dla audytów, a w szczególności: RODO/GDPR.

5.29. System powinien pozwalać na audyt:
5.29.1. Zmian na serwerach członkowskich;
5.29.2. Audyt stacji roboczych.

5.30. System powinien posiadać moduł powiadomień w formie alertów;
5.30.1. widocznych w systemie;
5.30.2. wysyłanych drogą mailową;
5.30.3. wysyłanych poprzez SMS.

5.31. System powinien umożliwiać podczas tworzenia profili alertów e-mail i SMS, listy mailingowej na podstawie wielu zmiennych (np., Nazwa użytkownika, SID itp.).

5.32. System powinien umożliwiać wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast.

5.33. System powinien posiadać alerty o przekroczonej przestrzeni dyskowej.

5.34. Narzędzie umożliwia zwolnienie zajętej przestrzeni dyskowej.

5.35. System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i ma możliwość dokładnego ustawiania czasu przeniesienia do archiwum.

5.36. System powinien pozwalać na audyt Azure Active Directory, a w szczególności:
5.36.1. poprawne logowanie użytkownika;
5.36.2. niepoprawne logowanie użytkownika;
5.36.3. niepoprawne logowanie użytkownika bazowane na nieprawidłowym podaniu hasła;
5.36.4. aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej.

5.37. System powinien pozwalać na audyt zmian na kontach użytkowników Azure Active Directory, a w szczególności posiada wbudowane raporty dotyczące użytkownika, któremu ostatnio:
5.37.1. utworzono lub usunięto konto;
5.37.2. zaktualizowano konto;
5.37.3. aktywowano lub dezaktywowano konto;
5.37.4. zmieniono lub zresetowano hasło.

5.38. System powinien pozwalać na Audyt nadanych ról w Azure Active Directory, a w szczególności przygotowane raporty dotyczące:
5.38.1. ostatnio przypisany członek do roli;
5.38.2. ostatnio odłączony członek od roli.

5.39. System powinien pozwalać na audyt zmian grup w Azure Active Directory, a w szczególności:
5.39.1. ostatnio utworzona grupa;
5.39.2. ostatnio usunięta grupa;
5.39.3. ostatnio zaktualizowana grupa;
5.39.4. ostatnio dodani członkowie do grup;
5.39.5. ostatnio usunięci członkowie z grup.

5.40. System powinien umożliwiać audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące:
5.40.1. wszystkich zmian plików i folderów;

5.40.2. plikach zmodyfikowanych;
5.40.3. plikach usuniętych;
5.40.4. plikach przeniesionych;
5.40.5. plikach utworzonych.

5.41. System powinien posiadać możliwość oceny ryzyka, opartego o uczenie maszynowe:
5.41.1. użytkownicy połączeni z dużą ilością zasobów;
5.41.2. konta o dużej aktywności;
5.41.3. konta o nadmiernej aktywności;
5.41.4. konta z wysokim % niepowodzeń logowania;
5.41.5. ostatnia aktywność użytkownika;
5.41.6. uśpione konta administratorów;
5.41.7. uprawnienia wykorzystane przez użytkowników;
5.41.8. pierwsze użycie przydzielonego uprawnienia;

5.42. System obsługuje szyfrowane (SSL) połączenie LDAP.

5.43. System powinien pozwalać na eksportowanie raportów/danych do formatów: CSV, PDF, XLS, HTML.

5.44. System dostarcza informacje o bezpiecznych powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów.

5.45. System dodatkowo obsługuje raportowanie z ADLDS oraz LAPS'a.

5.46. System potrafi przetworzyć dane do systemu SIEM'owego, w formacie RFC 3164 lub RFC 5424, w tym obsługuje wysyłanie danych po UDP jak i TCP.

5.47. System potrafi archiwizować dane do plików .zip oraz dołączać je do bazy danych, na żądanie administratora.

5.48. System potrafi zaimportować pliki .evt oraz .evtx, przetworzyć je wg. własnych filtrów oraz prezentować, jak resztę danych.

5.49. System powinien pozwalać na określenie godzin biznesowych, w celu filtrowania prezentowania raportów, na podstawie godzin pracy, jak i godzin poza pracą.

5.50. System powinien pozwalać na uruchomienie dowolnego programu, w momencie wystąpienia alertu.

5.51. System powinien pozwalać na pobieranie danych z AzureAD, w tym przetworzenia ich wg własnych wbudowanych reguł.

5.52. System powinien posiadać możliwość wyszukiwania własnych, wbudowanych raportów, na podstawie słów kluczowych.

5.53. System powinien posiadać możliwość śledzenia wiersza poleceń użytych przez proces.

5.54. System powinien umożliwiać konfigurację wysokiej wydajności.

5.55. System powinien posiadać raport zmian uprawnień NetApp i EMC w celu dostarczenia informacji o wartościach uprawnień przed i po.

5.56. System powinien posiadać możliwość konfiguracji ustawień agenta.

5.57. System powinien umożliwiać pojedyncze logowanie (SSO) za pośrednictwem NTLM lub SAML.

5.58. System powinien pozwalać na prezentację wszystkich działań użytkowników w jednym raporcie w obszarze Account Management.

5.59. System powinien umożliwiać przeprowadzenie audytu i raportu na temat wykorzystania podatnego na Netlogon połączenie Schannel przez urządzenia z systemem Windows.

5.60. System powinien umożliwiać śledzenie stanu usługi DNS, działania oczyszczania, zmiany strefy, zmiany rekordów, zmiany konfiguracji i inne powiązane z DNS'ami.

5.61. System powinien pozwalać monitorować czas rozpoczęcia i zakończenia replikacji usługi AD; śledzić zmiany replikacji, awarie i inne.

5.62. System powinien posiadać konfigurację umożliwiającą automatyczną zmianę trybu pobierania zdarzeń na tryb czasu rzeczywistego, gdy agent jest instalowany ręcznie.
5.63. System powinien pozwalać na łączenie się przez Internet agenta z serwerem bez korzystania z VPN, podając w pełni klasyfikowaną internetową nazwę hosta.
5.64. System powinien umożliwiać skonfigurowanie ustawień urządzenia do translacji adresów sieciowych (NAT) z interfejsu użytkownika. Urządzenia NAT są używane w komunikacji agent – serwer.
5.65. System powinien pozwalać na otrzymywanie alertów e-mail, gdy ilość miejsca na dysku jest mała i gdy produkt zostanie wyłączony z powodu małej ilości miejsca.
5.66. System obsługuje następujące technologie pulpitu zdalnego i wirtualnego poprzez instalację agenta: Dostęp bezpośredni, Trwałe i nietrwałe VDI, Połączony klon i pełny klon VDI, Pulpit wirtualny platform Azure.
5.67. System powinien pozwalać skonfigurować Azure Active Directory (Azure AD) bez konfiguracji lokalnej domeny Active Directory.
5.68. System obsługuje VBScript podczas wykonywania skryptów alertów.
5.69. System obsługuje audyt wydruku.
5.70. System powinien posiadać informacje o aplikacji klienckiej i zastosowanych zasadach dostępu warunkowano w inspekcji usługi Azure AD.
5.71. System powinien posiadać wykresy do raportów usługi Azure AD.
5.72. System obsługuje politykę haseł dla techników aplikacji.
5.73. System powinien posiadać możliwość resetowania hasła dla techników aplikacji przez administratorów aplikacji.
5.74. System powinien posiadać możliwość personalizacji ustawień oparte o techników aplikacji.
5.75. System powinien posiadać możliwość instalacji agenta podczas automatycznego dodawania serwerów członkowskich i stacji roboczych w aplikacji.
5.76. System powinien posiadać możliwość obsługi agenta aplikacji dla inspekcji grup roboczych.
5.77. System powinien posiadać możliwość zmiany trybu pobierania zdarzeń na RealTime dla wszystkich serwerów członkowskich i stacji roboczych jednocześnie.
5.78. System powinien posiadać możliwość wyświetlenia wyników inspekcji zasad dla kontrolerów domeny, serwerów członkowskich i stacji roboczych.
5.79. System powinien umożliwiać pobieranie informacji na temat woluminów serwera z pliku konfiguracyjnego podczas audytu NetApp.
5.80. System powinien posiadać interfejs API dla usługi inspekcji Azure AD, który używa uwierzytelnienia opartego o token podczas konfigurowania usługi Azure AD za pośrednictwem konta Office 365.
5.81. System powinien posiadać obsługę wersje beta interfejsu Microsoft Graph API dla szczegółów usługi MFA w inspekcji usługi Azure AD.
5.82. System powinien umożliwiać ustawienie niestandardowych adresów URL dla dostawców usług podczas logowania jednokrotnego SAML.
5.83. System powinien posiadać autentykację podczas komunikacji agenta do serwera.
5.84. System powinien pozwalać na tworzenie oraz zarządzanie własnymi raportami dla zdarzeń z Azure AD.
5.85. System powinien pozwalać na przeszukiwanie zdarzeń archiwalnych dla platformy Azure AD.
5.86. System powinien pozwalać na monitorowanie wszystkich certyfikatów.
5.87. System powinien posiadać możliwość audytowania serwera plików QNAP.

6. System do zarządzania i audytu serwera pocztowego Exchange on premise i Exchange online

6.1. System powinien posiadać możliwość działania na systemie bazodanowym Microsoft SQL Server, również w konfiguracji klastra.

6.2. System powinien działać na systemach z rodziny Windows.
6.3. Dostarczona instancja systemu powinna obsługiwać minimum 700 skrzynek pocztowych.
6.4. System powinien działać na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore.
6.5. System powinien analizować dane pochodzące z logów serwerów Exchange.
6.6. System powinien analizować dane, które samodzielnie pobiera z serwerów IIS.
6.7. System powinien działać bezagentowo.
6.8. System potrafi przechowywać zarchiwizowany zbiór logów z audytowanego środowiska i mieć możliwość dokładnego ustawiania czasu przeniesienia do archiwum.
6.9. System potrafi przypominać użytkownikom o wygaśnięciu hasła.
6.10. System powinien pozwalać na podłączenie certyfikatu, w formacie .PFX
6.11. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
6.12. System powinien posiadać wbudowane skrypty, które pozwalają na:
  6.12.1. backup bazy danych;
  6.12.2. odtworzenie bazy danych;
  6.12.3. zmianę bazy danych.
6.13. System powinien używać jednego konta do połączenia z domeną.
6.14. System powinien posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
6.15. System powinien pozwalać na zmianę portu HTTP / HTTPS z poziomu interfejsu graficznego.
6.16. System powinien obsługiwać serwery Microsoft Exchange w wersjach: 2000, 2003, 2007, 2010, 2013, 2016, 2019.
6.17. System powinien posiadać wbudowany dashboard, pokazujący najważniejsze dane z całego środowiska Exchange oraz dodatkowy dashboard dla Exchange Online, w którym prezentuje:
  6.17.1. wszystkie serwery Exchange, wraz z:
    - Statusem ich usług,
    - Zużyciem ich dysku,
    - Zdrowia przepływu wiadomości e-mail,
    - Zdrowia kolejki wiadomości e-mail,
  6.17.2. raporty graficzne, dotyczące:
    - użycia dysku, w rozbiciu na: wolne miejsce, miejsce zajęte przez bazy danych, miejsce zajęte przez inne pliki;
    - największych skrzynek pocztowych;
    - ilości wysłanych wiadomości e-mail;
    - ilości odebranych wiadomości e-mail;
    - wielkości odebranych wiadomości e-mail;
    - wielkości wysłanych wiadomości e-mail;
    - ilość wysłanych wiadomości e-mail per serwer Exchange;
    - ilość odebranych wiadomości e-mail per serwer Exchange;
    - ilość skrzynek z włączoną opcją prześlij dalej;
    - typy skrzynek, z podziałem na skrzynki: użytkownika, pokojów, publicznych folderów, udostępnione, skrzynki przedmiotów oraz ilości skrzynek na każdy serwer;
  6.17.3. Mailbox Traffic Report;
  6.17.4. liczba wiadomości według nadawcy na podstawie statusu odbiorcy.
6.18. System powinien posiadać raporty dostępów do Exchange Online dla:
  6.18.1. skrzynek pocztowych;

6.18.2. udostępnionych skrzynek pocztowych;
6.18.3. publicznych folderów;
6.18.4. kalendarza;
6.18.5. raport pozwalający na weryfikowanie tempa wzrostu zarchiwizowanych skrzynek pocztowych w określonym okresie;
6.18.6. raport przedstawiający stan zdalnego programu PowerShell dla programu Exchange Server 2013 i nowszych wersji;

6.19. System powinien posiadać dashboard dla serwerów Skype, w którym prezentuje raporty graficzne, dotyczące użytkowników, którzy:
6.19.1. wykonali największą ilość połączeń;
6.19.2. przesłali najwięcej plików wewnątrz organizacji;
6.19.3. przesłali najwięcej plików poza organizację.

6.20. Aplikacja umożliwia użytkownikom możliwość analizy, raportowania i audytu serwerów Microsoft Exchange, a w szczególności posiada wbudowane raporty dotyczące:
6.20.1. przychodzących i wychodzących wiadomości e-mail;
6.20.2. wielkości skrzynek pocztowych;
6.20.3. ruchu na skrzynkach pocztowych;
6.20.4. zawartości skrzynek pocztowych;
6.20.5. liczby wiadomości wysłanych i odbieranych przez każdy serwer programu Exchange, używając raportów o ruchu na serwerze;
6.20.6. istotnych statystyk folderów publicznych serwera programu Exchange, za pomocą raportów o folderze publicznym;
6.20.7. list dystrybucyjnych i ruchu na każdej z list;
6.20.8. uprawnień do skrzynek pocztowych;
6.20.9. uprawnień do folderów publicznych wraz z podfolderami;
6.20.10. usługi OWA (Outlook Web Access);
6.20.11. logowania do skrzynek pocztowych;
6.20.12. zmian uprawnień na skrzynkach pocztowych;
6.20.13. zmian ustawień na skrzynkach pocztowych;
6.20.14. zmian uprawnień na folderach publicznych;
6.20.15. zmian bazy danych;
6.20.16. zmian w grupach dystrybucyjnych;
6.20.17. zmian w członkostwie grup dystrybucyjnych;

6.21. System powinien umożliwiać monitoring i raportowanie aktywności serwerów Exchange w wersji 2010, 2013, 2016, 2019, a w szczególności komponentów:
6.21.1. Serwer Exchange, a w szczególności raportowanie stanu:
- zdrowia usług Exchange;
- zdrowia usług replikacji skrzynek pocztowych (MRS);
- zdrowia przepływu poczty email;
- wykorzystania CPU i pamięci RAM;
- połączeń serwerów Exchange z innymi komponentami i protokołami;

6.21.2. DAG (Database Availability Group), a w szczególności raportowanie stanu:
- zdrowia usług replikacji;
- wykonania kopii zapasowej bazy danych;

6.21.3. Baza danych Exchange, a w szczególności raportowanie stanu:
- zdrowia funkcji Exchange Search;
- połączeń z MAPI;
- wykonania backupów bazy danych;

6.21.4. System powinien umożliwiać monitorowanie i raportowanie z Exchange Online, w tym raportowanie o:
- ilości użytkowników;
- nieaktywnych skrzynkach;
- użytkownikach, z uprawnieniami „wyślij jako” / „wyślij w imieniu”;
- niedawno utworzonych skrzynkach;
- odłączonych skrzynkach;
- regułach poczty przychodzącej;
- wyszukiwaniu po tytule wiadomości;
- niedostarczonych wiadomościach;
- wiadomościach wysłanych do niewłaściwych adresatów;
- dostarczonych i niedostarczonych wiadomościach;
- ilości logowań do OWA per użytkownik;
- ilości urządzeń mobilnych;
- nieaktywnych / aktywnych urządzeniach mobilnych;
- urządzeniach mobilnych, z podziałem na system operacyjny;
- skrzynkach udostępnionych;
- niedawno utworzonych wydarzeniach w kalendarzu;
- niedawno zmodyfikowanych wydarzeniach w kalendarzu;
- nieaktywnych listach dystrybucji;
- nieaktywnych urządzeniach ActiveSync;
- dziennych działaniach liczonych według typu;
- dziennej liczbie unikalnych użytkowników według aktywności e-mail;
- dziennej liczbie aktywnych skrzynek pocztowych;
- dziennej liczbie skrzynek pocztowych według stanu przydziału pamięci;
- dziennej liczbie unikalnych użytkowników według aplikacji e-mail;
- dziennym użyciu miejsca przez skrzynki pocztowe.

6.22. System powinien posiadać możliwość audytowania zmian w Exchange Online, takich jak:
6.22.1. akcje wykonane przez administratorów Exchange;
6.22.2. aktywności typu „wyślij jako”;
6.22.3. zmiany w kalendarzach;
6.22.4. utworzenie, usunięcie oraz modyfikacja kontaktu;
6.22.5. zmiany w limitach miejsce (quota);
6.22.6. utworzenie, usunięcie oraz modyfikację folderu publicznego;
6.22.7. aktywność przesunięcia lub usunięcia wiadomości;
6.22.8. zmiany ustawień connectorów.

6.23. System powinien posiadać możliwość modyfikacji interwału odpytywania Exchange Online, od minimalnie 5 minut, do 24 godzin oraz posiada możliwość wymuszenia pobrania danych.

6.24. System powinien umożliwiać filtrowanie wszystkich akcji audytowych, na bazie:
6.24.1. godzin biznesowych;
6.24.2. kolumn w prezentowanym w raporcie, na wszystkich typach danych.

6.25. System powinien posiadać możliwość wykonania raportów zgodności, w standardzie SOX, HIPAA, PCI, GLBA, GDPR.

6.26. System powinien umożliwiać monitoring i raportowanie konfiguracji skrzynek pocztowych, w szczególności skrzynek:
6.26.1. z włączoną opcją przekazywania poczty na domenę zewnętrzną;
6.26.2. z włączoną opcją przekazywania poczty na domenę wewnętrzną;
6.26.3. bez włączonej opcji przekazywania poczty;

6.26.4. bez ustawionego zdjęcia;
6.26.5. które mają możliwość wykorzystania ActiveSync;
6.26.6. które posiadają reguły poczty przychodzącej;
6.26.7. które mają konfigurację wiadomości śmieci.

6.27. System powinien umożliwiać monitoring i raportowanie:
6.27.1. tworzenia, usuwania i modyfikacji list dystrybucyjnych;
6.27.2. skrzynek, które posiadają nieprzeczytane wiadomości e-mail;

6.28. System powinien umożliwiać raportowanie użytkowników z uprawnieniami "wyślij jako" oraz "wyślij w imieniu".

6.29. System powinien umożliwiać raportowanie aplikacji Skype for business, w szczególności:
6.29.1. polityk kodów PIN;
6.29.2. konferencji wszystkich lub per użytkownik;
6.29.3. nieaktywnych użytkowników;
6.29.4. konfiguracji konferencji;
6.29.5. aktywności wiadomości IM;
6.29.6. rozmów audio-video;
6.29.7. nieprzypisanych numerów;
6.29.8. polityk głosowych;
6.29.9. przesyłania plików.

6.30. System powinien umożliwiać utworzenie własnych niestandardowych raportów, na bazie istniejących raportów w systemie, które mogą zostać zabezpieczone hasłem.

6.31. System powinien umożliwiać na utworzenie zaplanowanych raportów, które będą wysyłane co cykliczny, określony przez użytkownika, okres czasu:
6.31.1. w następujących formatach: PDF, CSV, XLS, HTML;
6.31.2. w następujących, możliwych konfiguracjach cyklicznego wysyłania: codziennie, raz na tydzień, raz na miesiąc.

6.32. System powinien umożliwiać na automatyczne zarządzenie dostępną pulą licencji, w wybranych godzinach, w oparciu o atrybuty skrzynki, takie jak:
6.32.1. nazwa serwera;
6.32.2. domena i jednostka organizacyjna (OU);
6.32.3. atrybuty „ukryta" i „wyłączona";
6.32.4. baza danych.

6.33. System dodatkowo zapisuje wszystkie zaplanowane raporty na dysku.

6.34. System powinien umożliwiać:
6.34.1. audytowanie raportów weksportowanych przez użytkowników aplikacji;
6.34.2. eksportowanie raportów do plików XLS, CSV, PDF, HTML zabezpieczonych opcjonalnym hasłem;
6.34.3. dołączanie niestandardowych atrybutów ze schematu Active Directory do raportów;
6.34.4. wymuszenie złożoności haseł dla nowych administratorów i operatorów.

6.35. System powinien posiadać możliwość działania na systemie bazodanowym Microsoft SQL, również w architekturze klastra.

6.36. System powinien działać na podłączenie certyfikatu, w formacie „PFX" (PKCS12).

6.37. System powinien samodzielnie analizować dane pochodzące serwerów Exchange, pobranych przy pomocy:
6.37.1. Powershell;
6.37.2. EventLog serwera Exchange;
6.37.3. Logów serwerów IIS.

6.38. System powinien pozwalać na wybranie niestandardowej ścieżki logów IIS oraz logów ról transportowych.
6.39. System powinien działać bezagentowo.
6.40. Administratorzy mogą stworzyć i zdefiniować role dla operatorów systemu.
6.41. System potrafi przechowywać zarchiwizowany zbiór logów z audytowanego środowiska i mieć możliwość dokładnego ustawiania czasu przeniesienia do archiwum.
6.42. System potrafi przypominać użytkownikom o wygaśnięciu hasła.
6.43. System powinien pozwalać na podłączenie certyfikatu, w formacie „PFX".
6.44. System powinien obsługiwać bazy danych PostgreSQL oraz Microsoft SQL, jako instancje do przechowywania danych.
6.45. System powinien posiadać wbudowane skrypty, które pozwalają na:
    6.45.1. backup bazy danych;
    6.45.2. odtworzenie bazy danych;
    6.45.3. zmianę bazy danych.
6.46. System powinien używać jednego konta do połączenia z domeną.
6.47. System powinien posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
6.48. System powinien pozwalać na zmianę portu HTTP / HTTPS z poziomu interfejsu graficznego.
6.49. System powinien umożliwiać filtrowanie danych w oparciu o grupy administracyjne, grupy routingu i inne kryteria.
6.50. System powinien posiadać moduł powiadomień, w formie informacji: widocznych w systemie oraz wysyłanych drogą mailową.
6.51. Moduł powiadomień, pozwala na utworzenie alertów dla wszystkich akcji, na środowisku Exchange i Exchange Online, oraz na filtrowanie ich na bazie parametrów eventu i / lub wartości brzegowych ilości wydarzeń.
6.52. System powinien pozwalać na przesyłanie zebranych przez siebie logów, do zewnętrznego systemu SIEM.
6.53. System powinien posiadać możliwość:
    6.53.1. audytu akcji techników;
    6.53.2. tworzenia harmonogramów dla automatycznego zarządzania licencjami;
    6.53.3. włączenia podwójnej autentykacji techników do oprogramowania.
6.54. System powinien pozwalać wyszukać określoną zawartość skrzynki pocztowej Exchange.
6.55. System umożliwia, podczas tworzenia raportów niestandardowych uwzględnić jednocześnie wszystkie foldery z wyjątkiem domyślnych.
6.56. System obsługuje bezpieczną komunikację za pomocą szyfrowanego połączenia SSL z bazą danych Microsoft SQL.
6.57. System powinien posiadać możliwość delegowania uprawnień użytkowników do tworzenia nowego szablonu powiadomień e-mail, przy planowaniu raportów Exchange Online.
6.58. System powinien posiadać możliwość powiadomień o alertach dla ruchu e-mail na podstawie kryteriów:
    6.58.1. liczba wysyłanych wiadomości e-mail;
    6.58.2. liczba otrzymanych wiadomości e-mail;
    6.58.3. liczba odbiorców;
    6.58.4. rozmiar wysłanej wiadomości;
    6.58.5. rozmiar odebranej poczty;
    6.58.6. niedostarczone wiadomości e-mail.
6.59. System powinien pozwalać śledzić tworzenie i usuwanie folderów publicznych na serwerach Exchange oraz audytować wymienione działania.

6.60. System powinien używać Elastic Search, do którego pobiera wszystkie raporty, w celu zwiększenia szybkości pobierania jak i prezentowania danych.
6.61. System powinien informować administratora o proponowanym wzmocnieniu zabezpieczeń po zalogowaniu do aplikacji, jeżeli konfiguracja ustawień bezpieczeństwa nie jest wystarczająca.
6.62. System powinien używać weryfikacji adresów URL produktów, aby uniemożliwić nieuwierzytelnionym użytkownikom dostęp do narzędzia.
6.63. System powinien posiadać możliwość planowania raportów, aby umożliwić użytkownikom planowanie wielu raportów jednocześnie, przeglądanie historii harmonogramów i sprawdzanie szczegółów harmonogramów wraz z czasem działania i stanem
6.64. System powinien posiadać możliwość wyszukiwania zawartości maili w usłudze Exchange Online.
6.65. System powinien pozwalać na migrację maili, kontaktów, kalendarza i zadań z lokalnej skrzynki pocztowej Exchange do środowiska Exchange Online.

7. System do zarządzania usługami IT (ITSM)

7.1. Ogólna charakterystyka systemu:
7.1.1. Powinien być systemem heterogeniczny i posiadać możliwość instalacji na systemie operacyjnym Windows x64, jak również Linux;
7.1.2. powinien pracować w oparciu o bazę danych Microsoft SQL lub z darmową bazą danych PostgreSQL;
7.1.3. powinien posiadać własny wbudowany interfejs przez który odbywa się konfiguracja bazy danych;
7.1.4. powinien integrować się z dowolną skrzynką pocztową działająca na protokole POP, POPS, IMAP, IMAPS, SMTP, SMTPS, Exchange Online z wykorzystaniem Microsoft Graph;
7.1.5. powinien wspierać możliwość logowania bez potrzeby ponownego używania poświadczeń do aplikacji dzięki autentykacji poprzez SAML 2.0 Single Sign On (SAML SSO);
7.1.6. powinien dzięki wbudowanemu interfejsowi pozwalać na:
- łatwe wykonywanie backupu, bez potrzeby dodatkowego edytowania plików konfiguracyjnych, również z możliwością jednoczesnego backupowania załączników;
- konfigurację powiadomień, bez potrzeby dodatkowego edytowania plików konfiguracyjnych;

7.1.7. powinien posiadać wbudowane funkcjonalności, bez potrzeby dokupienia dodatków / rozszerzeń:
- „Chat”;
- moduł ankietowania;

7.1.8. funkcjonalność „Chat” powinna pozwalać na podjęcie rozmowy z grupą wsparcia z możliwością rejestracji zgłoszenia przez technika na podstawie rozmowy inicjowanej przez usługę „Chat”;
7.1.9. system powinien posiadać własną wersje darmowej aplikacji mobilnej, na systemy Android i iOS;
7.1.10. powinien posiadać moduły z certyfikatami PinkVERIFY wydanymi przez organizację Pink Elephant przynajmniej w zakresie wniosków o usługę, incydentów, zarządzania usługami;
7.1.11. powinien posiadać możliwość integracji z rozwiązaniem Teams firmy Microsoft.

7.1.12. powinien pozwalać na tworzenie skryptów przy użyciu języków: Java, Powershell, Python, Deluge;
7.1.13. powinien posiadać możliwość uruchomienia dwuskładnikowego logowania przy użyciu adresu e-maila lub aplikacji Google Authenticator;
7.1.14. powinien pozwalać na integrację z kalendarzem Microsoft;
7.1.15. powinien pozwalać na integrację z rozwiązaniem Outlook;
7.1.16. powinien pozwalać na konfigurację serwera pocztowego Exchange Online z wykorzystaniem Microsoft Graph;
7.1.17. powinien integrować się z modułem / systemem do zarządzania stacjami roboczymi oferowanym w niniejszym postępowaniu;
7.1.18. powinien pozwalać na wysłanie linku do resetu hasła;
7.1.19. powinien wspierać certyfikaty RSA oraz ECC;
7.1.20. powinien posiadać portal ESM (Enterprise Service Management).

7.2. Wymagania podstawowe systemu:
7.2.1. powinien posiadać własny wbudowany moduł raportowania wzbogacony o możliwość kwerendowania do bazy danych;
7.2.2. powinien wspierać przeglądarki: Edge, Chrome, Firefox;
7.2.3. dostęp do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej lub z aplikacji mobilnej;
7.2.4. wszystkie funkcjonalności systemu są dostępne w momencie instalacji oprogramowania;
7.2.5. system powinien posiadać wgląd w strukturę bazy danych dostępny z poziomu aplikacji, wraz z możliwością ograniczenia widoku na dane moduły aplikacji;
7.2.6. powinien pozwalać na konfigurację wspólnego serwera aplikacji i bazy danych, a w przypadkach szczególnych na ich rozdzielenie;
7.2.7. jako opcja dodatkowa, system powinien posiadać wbudowany mechanizm, który zapewnienia wysoką dostępności aplikacji – HA (Fail Over Service);
7.2.8. system powinien integrować się z Active Directory lub LDAP oraz wspierać logowanie centralne (Single Sign On) oraz autentykację SAML bez konieczności instalowania dodatkowych aplikacji;
7.2.9. system powinien umożliwiać import dowolnych atrybutów UDF z Active Directory;
7.2.10. system powinien pozwalać wyświetlić listę użytkowników nieobecnych, usuniętych z Active Directory i pozwala na ich ręczne bądź automatyczne usuwanie z systemu zgodnie z zadanym harmonogramem;
7.2.11. system powinien posiadać wbudowane mechanizmy wykonywania kopii zapasowych bazy danych wraz z załącznikami, ich odtwarzania oraz możliwość skonfigurowania harmonogramu wykonywania kopii zapasowych z retencją danych.
7.2.12. System powinien posiadać funkcję wysyłania powiadomień w przypadku niewykonania się kopii zapasowej do ustalonych wcześniej użytkowników / administratorów systemu;
7.2.13. interfejs systemu oraz konfiguracji jest w całości dostępny z poziomu przeglądarki internetowej bez potrzeby instalacji tzw. grubego klienta;
7.2.14. system powinien posiadać dodatkowo płatną wersję wielojęzykową pozwalającą na wyświetlanie interfejsu w co najmniej 30 popularnych językach, w tym w języku polskim;
7.2.15. interfejs użytkownika pozwala na wprowadzenia zmian w słownikach atrybutów konfiguracji oraz słowników interfejsu graficznego użytkownika;

7.2.16. system powinien pozwalać na dowolne dostosowanie („customizację") strony logowania użytkownika, poprzez edycję plików HTML i CSS;

7.2.17. system powinien posiadać wbudowaną funkcjonalność „Chat" osób zgłaszających z technikami – w ramach tej funkcjonalności system powinien umożliwiać obsługę następujących scenariuszy:
- po upływie określonego czasu od niepodjętej przez technika konwersacji wiadomość zostaje automatycznie skonwertowana na zgłoszenie do systemu;
- technicy posiadają możliwość zakończenia konwersacji na poziomie chatu i skonwertowania konwersacji do nowego zgłoszenia w systemie;
- zgłaszający posiada możliwość nawiązania chatu w nawiązaniu do zarejestrowanego przez zgłaszającego zgłoszenia – opcja chatu pozwala na wykluczanie techników, którym wiadomości chat nie będą przesyłane;
- system, w ramach widoku zgłoszenia pozwala sprawdzić okres przypisania zgłoszenia do: poszczególnej grupy techników, technika, statusu na zgłoszeniu;

7.2.18. system powinien posiadać możliwość przełączenia widoku rozwiązań do widoku tablicy Kanban;

7.2.19. system powinien posiadać funkcjonalność, która wskazuje serwisantów aktualnie zalogowanych do systemu;

7.2.20. system powinien posiadać pływające menu szybkich działań, widoczne niezależnie od położenia ekranu;

7.2.21. system powinien posiadać możliwość customizacji portalu w tym, rozmieszczenie poszczególnych elementów portalu metodą drag&drop, zagnieżdżanie stron HTML, zagnieżdżanie filmów;

7.2.22. system powinien posiadać możliwość personalizacji użytkowników na zasadzie dodatkowych opisów oraz wgrania grafik, zdjęć prezentujących danego użytkownika;

7.2.23. system powinien posiadać możliwość przekazywania wiadomości od serwisanta, bezpośrednio na skrzynkę pocztową zgłaszającego;

7.2.24. system powinien posiadać moduł umożliwiający globalne definiowanie szablonów e-maili wykorzystywanych przez system do powiadamiania użytkowników o różnych zdarzeniach w systemie. Definiowanie szablonów odbywa się z poziomu interfejsu webowego aplikacji i umożliwia zdefiniowanie treści powiadomienia, reguły wywołującej przesłanie powiadomienia oraz odbiorcy;

7.2.25. system powinien posiadać mechanizm oznaczania, którego z modułów systemu powiadomienie dotyczy;

7.2.26. system powinien posiadać kalendarz przeznaczony dla serwisantów, pozwalający na rejestrowanie nieobecności i wyznaczanie zastępstw. System powinien pozwalać na automatyczne przekierowanie zgłoszeń do wskazanego technika zapasowego (bazując na dacie zarejestrowania zgłoszenia bądź dacie rozwiązania zgłoszenia) lub wyłączenie umowy SLA dla zgłoszenia;

7.2.27. system powinien posiadać moduł zarządzania procesami, który umożliwia tworzenie harmonogramów dla zgłoszeń okresowych, a w ramach realizacji takiego zgłoszenia automatyczne przydzielanie zadań do serwisantów;

7.2.28. system powinien posiadać możliwość wstawianie plików graficznych oraz materiałów video w treści rozwiązania zgłoszenia;

7.2.29. system powinien posiadać funkcjonalność prezentowania w postaci graficznej istotnych wskaźników wydajności pozwalające na monitorowanie statusu

poszczególnych procesów, moduł wskaźników pozwala ustalić okres odświeżania danych na tablicy wskaźników;

7.2.30. system powinien posiadać interfejs programowania aplikacji API;

7.2.31. system powinien umożliwiać tworzenie i jednoczesną pracę (konta nazwane) 12 techników;

7.2.32. system powinien pozwalać na reprezentację użytkowników z wykorzystaniem imienia i nazwiska użytkownika, a także dowolnie rozbudowanymi atrybutami. Każdy z nowo utworzonych atrybutów może być wypełniony automatycznie z danych Active Directory;

7.2.33. system powinien posiadać możliwość odwzorowania struktury organizacji w tym:
- konfiguracji regionu, w którym są świadczone usługi;
- konfiguracji lokalizacji, według której dalej mogą być skonfigurowane dedykowane:
  - godziny pracy dla organizacji;
  - niestandardowe godziny pracy dla każdej lokalizacji;
  - dni wolne;
  - jednostki organizacyjne;
  - role organizacyjne uwzględniane w procesie akceptacji zgłoszeń;
  - reguły automatyzujące przebieg zgłoszeń;
  - reguły auto przypisywania techników według lokalizacji zgłaszających;
  - grupy techników;
  - konta techników;
  - konta zgłaszających;

7.2.34. konfiguracji jednostek organizacyjnych\działów, według których dalej mogą być skonfigurowane:
- role organizacyjne uwzględniane w procesie akceptacji zgłoszeń według struktury działowej;
- grupy techników;
- grupy zgłaszających (użytkowników systemu);

7.2.35. System powinien posiadać wbudowaną funkcjonalność ankietowania użytkowników pozwalającą na:
- konfigurację wyglądu i treści wiadomości z prośbą o ocenę/wypełnienie ankiety;
- konfigurację komunikatu z podziękowaniem za wypełnienie ankiety;
- konfigurację momentu wysłania ankiety (po każdym zamkniętym zgłoszeniu/ po określonej ilości zamkniętych zgłoszeń/ po określonej ilości zamkniętych zgłoszeń od danego użytkownika);
- konfigurację wyjątków wedle których ankiety nie będą rozsyłane (gdy zgłaszającym był technik/ wedle wskazanych kryteriów);
- konfigurację ankiety z uwzględnieniem pytań otwartych, zamkniętych, poziomów zadowolenia;
- podgląd wyników ankiet tylko przez uprawnionych użytkowników;

7.2.36. system powinien posiadać możliwość rejestracji czasu pracy, przez uruchomienie zegara liczącego, czas spędzony nad zgłoszeniem przez technika a system w postaci graficznej prezentuje uruchomiony zegar w widoku zgłoszeń, jak i samym zgłoszeniu;

7.2.37. system powinien pozwalać na analizę czasów: przypisania zgłoszenia do danego technika, przypisania zgłoszenia do danej grupy suportu, przypisania zgłoszenia do danego statusu;

7.2.38. system powinien pozwalać na wprowadzanie dodatkowych atrybutów czasu pracy, możliwych do późniejszego raportowania;
7.2.39. system powinien pozwalać na wprowadzenie dedykowanych typów czasu pracy;
7.2.40. system powinien umożliwiać zdefiniowanie na formularzach, pól niezbędnych do wypełnienia w trakcie rejestracji i zamknięcia zgłoszenia;
7.2.41. architektura systemu pozwala spełniać wskazania RODO / GDPR poprzez możliwość oznaczania danych jako danych zawierających dane osobowe oraz automatycznej anonimizacji danych przy usunięciu użytkownika z aplikacji;
7.2.42. system powinien pozwalać na konfigurację progów i czasu trwania blokady konta użytkownika w przypadku przekroczenia wskazanej ilości nieudanych prób logowania;
7.2.43. system pozwalana konfigurację automatycznego odblokowania konta użytkownika po upłynięciu wyznaczonego czasu;
7.2.44. system powinien pozwalać na ręczne odblokowanie użytkownika z poziomu aplikacji;
7.2.45. system powinien pozwalać na konfigurację komunikatu w momencie uruchomienia blokady konta;
7.2.46. system powinien pozwalać na powiadomienie technika poprzez wiadomość mail i komunikat w portalu o uruchomieniu blokady dla wskazanego użytkownika;
7.2.47. system powinien pozwalać na konfigurację wykorzystywanego protokołu HTTP / HTTPS z poziomu aplikacji;
7.2.48. system powinien pozwalać na konfigurację czasu trwania sesji bez potrzeby ponownego zalogowania użytkownika;
7.2.49. system powinien pozwalać na konfigurację domyślnych nagłówków zabezpieczeń, aby pomóc w ochronie aplikacji przed atakami typu XSS, Reflected XSS, Clickjack itp.;
7.2.50. system powinien pozwalać na blokadę wyświetlania domeny użytkownika podczas próby logowania, celem utrudnienia rozpoznania nazwy domeny użytkownika przez osoby nieuprawnione;
7.2.51. system powinien umożliwiać tagowanie zgłoszeń;
7.2.52. system powinien posiadać mechanizm zatrzymywania ładowania zeskanowanych XML za pośrednictwem niewymagającego logowania adresu URL;
7.2.53. system oferuje funkcjonalność pozwalającą na projektowanie tzw.: cyklu życia zgłoszenia uwzględniając:
- projektowanie stanów w jakim zgłoszenie się aktualnie znajduje uwzględniając stan przed, podczas i po przejściu i ich graficzne odzwierciedlenie;
- system powinien pozwalać na modyfikację już istniejących incydentów;
- system powinien pozwalać na dodawanie tzw. przejść między poszczególnymi statusami;
- system powinien pozwalać finalnie publikować zmodyfikowane szablony wniosków lub incydentów;
- system powinien pozwalać na umieszczanie reprezentacji graficznej zasobów będących elementem wyboru w szablonach wniosków;

7.2.54. system oferuje możliwość tworzenia dodatkowych instancji, które:
- są logicznie od siebie odseparowane;
- w swej odrębności rozwiązanie oferuje wszystkie podstawowe możliwości konfiguracyjne i funkcjonalne o których mówi niniejszy dokument;
- w swej odrębności rozwiązanie pozwala na osobną konfigurację katalogu usług uwzględniając podstawowe funkcjonalności o których mówi niniejszy dokument

- posiada customizowalny portal samoobsługowy;
- posiada możliwość przypisywania odpowiednich grup wsparcia i użytkowników korzystających z wybranej dodatkowej instancji;

7.2.55. system powinien posiadać moduł AI który można szkolić w celu automatyzacji zadań pomocy technicznej;

7.2.56. system powinien posiadać możliwość skonfigurowania funkcji Auto Update;

7.2.57. system powinien posiadać natywną integrację z systemami Microsoft 365, Atlassian Jira, Microsoft Teams, Microsoft Outlook, Microsoft Calendar;

7.2.58. system wyświetla opis z wiadomości email zawierających zaproszenie do kalendarza w formacie iCalendar;

7.2.59. system powinien posiadać limit obrazków w treści wiadomości e-mail wynoszący 3MB lub pozwolić na skonfigurowanie takiego limitu;

7.2.60. system powinien posiadać możliwość dwuskładnikowego uwierzytelniania dla dostępu do panelu administracyjnego.

7.3. Wymagania dotyczące modułu helpdesk – system powinien:

7.3.1. posiadać wsparcie metodologii ITSM w zakresie zarządzania incydentem, zarządzanie wnioskami o usługę, zarządzanie zasobami potwierdzone certyfikatami organizacji Pink Elephant;

7.3.2. posiadać moduł zarządzania procesami w pełni konfigurowalny z poziomu interfejsu webowego oprogramowania;

7.3.3. posiadać mechanizm oznaczania pierwszej reakcji na zgłoszenie jako rozwiązania zgłoszenia – first call resolution;

7.3.4. pozwalać na dowolną rozbudowę pól wykorzystywanych do opisania czasu pracy poświęconego na rozwiązanie zgłoszenia;

7.3.5. umożliwiać rejestrację zgłoszenia wieloma kanałami, w szczególności przez stronę WWW, telefon i email;

7.3.6. umożliwiać przekazywanie wiadomości od serwisanta, bezpośrednio na skrzynkę pocztową zgłaszającego;

7.3.7. umożliwiać w trakcie rejestracji zgłoszenia przez użytkownika na stronie www, załączenie dowolnej ilości dowolnego formatu załączników. System powinien pozwalać na wymuszenie na użytkowniku końcowym konieczność dodania załącznika do zgłoszenia;

7.3.8. pozwalać na udostępnianie do wglądu (sharing) zgłoszenia pomiędzy serwisantów oraz zgłaszających. Zgłoszenie może być udostępnione dla poszczególnych użytkowników lub w grupy w obrębie działów i lokalizacji użytkowników;

7.3.9. pozwalać wstrzymać zegar SLA (timer) zgłoszenia wraz z ustawieniem automatycznego jego otwarcia i wysłania powiadomienia do serwisanta;

7.3.10. pozwalać użytkownikom na przeglądanie na stronie www statusu własnych zgłoszeń, dodawania komentarzy, podgląd i edycję danych użytkownika, przeglądania bazy wiedzy znanych problemów i ich rozwiązań oraz ocenianie wpisów w bazie wiedzy;

7.3.11. pozwalać na definiowanie dodatkowych pól w formularzu incydentu;

7.3.12. pozwalać na konfigurację dedykowanych do wybranych typów zgłoszeń incydentów przycisków, wyzwalających uruchomienie:

- dedykowanego pliku HTML, powiązanego z wykonywalnym skryptem lub klasą na systemie helpdeskowym;
- dedykowanego pliku HTML, powiązanego z wykonywalnym skryptem lub klasą na systemie zintegrowanym z helpdeskowym;

- wykonywalnego skryptu lub klasy na systemie helpdeskowym;
- wykonywalnego skryptu lub klasy na systemie zintegrowanym z helpdeskowym;
- wykonywalnego skryptu lub klasy na systemie zintegrowanym z helpdeskowym w oparciu o ustalony harmonogram;

7.3.13. pozwalać na konfigurację globalnych reguł biznesowych, wywołujących wykonywalny skrypt lub klasę na systemie helpdeskowym, lub na systemie zintegrowanym z systemem helpdeskowym;

7.3.14. pozwalać na wymuszenie podawania komentarzy przy zmianie statusów zgłoszenia;

7.3.15. pozwalać na budowanie zależności między zarejestrowanymi zgłoszeniami incydentów. Zależności pozwalają na uzależnienie zamykania zgłoszenia od zamknięcia zgłoszenia zależnego poprzedzającego dane zgłoszenie;

7.3.16. pozwalać na konfigurację funkcjonalności informującej zgłaszających o czasie na rozwiązanie zgłoszenia;

7.3.17. posiadać centralne repozytorium incydentów, umożliwiające filtrowanie i sortowanie zapisanych zgłoszeń według co najmniej następujących kryteriów: status zgłoszenia, kategoria, użytkownik, czas rozwiązania, czas przyjęcia, przydzielona grupa wsparcia;

7.3.18. posiadać centralne repozytorium incydentów, umożliwiające definiowanie własnych filtrów umożliwiających sortowania zapisanych zgłoszeń;

7.3.19. umożliwiać dla każdego zgłoszenia określenie takich atrybutów, jak: dane osoby zgłaszającej oraz priorytet realizacji;

7.3.20. umożliwiać przeszukiwanie zgłoszeń według co najmniej następujących atrybutów: nr zgłoszenia, użytkownik, tytuł, opis;

7.3.21. posiadać interfejs zarejestrowanych zgłoszeń, w tym widok prezentujący listę zarejestrowanych zgłoszeń incydentów i zadań;

7.3.22. interfejs systemu pozwala na stworzenie dedykowanego widoku dla każdego z techników oraz na ukrywanie dodatkowego okna z listą zadań do wykonania;

7.3.23. dla każdego z widoku zgłoszeń i zadań, system powinien pozwalać na wybór prezentowanych danych według wszystkich atrybutów dostępnych w zgłoszeniach i zadaniach;

7.3.24. dla każdego z widoku zgłoszeń i zadań rozwiązanie pozwala na filtrowanie widoku prezentowanych zgłoszeń;

7.3.25. pozwalać na rejestrację zgłoszeń pochodzących z zewnętrznych narzędzi monitorujących, jednocześnie umożliwiając ich klasyfikację i na tej podstawie automatyczne przekazywanie do grup wsparcia;

7.3.26. pozwalać na przesyłanie i prezentowanie na stronie www powiadomień dla użytkowników i / lub serwisantów, przesyłanie powiadomień do pojedynczych użytkowników lub grup użytkowników / serwisantów;

7.3.27. w ramach obsługi zgłoszeń umożliwiać komunikację z użytkownikiem poprzez pocztę elektroniczną i rejestrację wiadomości do właściwych wątków zgłoszeń;

7.3.28. pozwalać zgłaszającym na edycję zgłoszenia po jego zarejestrowaniu, możliwość edycji zgłoszeń po zarejestrowaniu jest ustawiana po stronie administracyjnej;

7.3.29. pozwalać na klasyfikację zgłoszeń, w co najmniej 3 poziomowej strukturze drzewiastej, przy czym struktura klasyfikacji może być dowolnie edytowalna przez uprawnionych administratorów z poziomu interfejsu webowego systemu;

7.3.30. umożliwiać automatyczne wyliczenie i przydzielenie priorytetu do zgłoszenia;

7.3.31. pozwalać na automatyczną eskalację zgłoszeń do grup wsparcia, na podstawie co najmniej następujących atrybutów: użytkownik, priorytet, poziom, tytuł zgłoszenia, słowo kluczowe w tytule i treści zgłoszenia;
7.3.32. umożliwiać przekierowanie zgłoszeń do innych serwisantów lub grup wsparcia celem dalszej obsługi;
7.3.33. umożliwiać tworzenie szablonów zgłoszeń z predefiniowanymi atrybutami i regułami przekazywania tychże zgłoszeń do zespołów wsparcia;
7.3.34. umożliwiać tworzenie harmonogramów dla zgłoszeń okresowych, a w ramach realizacji takiego zgłoszenia automatyczne przydzielanie zadań do serwisantów;
7.3.35. umożliwiać zdefiniowania reguł biznesowych, z ich rozróżnieniem względem lokalizacji;
7.3.36. umożliwiać zdefiniowanie umów SLA w oparciu o priorytet;
7.3.37. umożliwiać rejestrację historii incydentów, zablokowaną do edycji dla użytkownika oprogramowania;
7.3.38. umożliwiać rejestrowanie aktywności i zleceń pracy związanych z poszczególnymi incydentami.
7.3.39. umożliwiać definiowanie i filtrowanie szablonów zgłoszeń dedykowanych dla określonych grup użytkowników;
7.3.40. umożliwiać przesyłanie do użytkowników powiadomień o następujących zdarzeniach zarejestrowanych przez system: przyjęcie zgłoszenia, aktualizacja zgłoszenia, rozwiązanie zgłoszenia, zamknięcie zgłoszenia;
7.3.41. umożliwiać automatyczne zamykanie rozwiązanych zgłoszeń po określonym czasie;
7.3.42. umożliwiać przekazywanie do akceptacji osób trzecich działań podejmowanych w ramach rozwiązania zgłoszenia, np. akceptacja realizacji zlecenia na usługę serwisową;
7.3.43. pozwalać na automatyczne przypisywanie osób wymaganych do akceptacji zgłoszenia w oparciu o sposób wypełnienia zgłoszenia, akceptacje mogą być oparte o dowolne atrybuty zgłaszającego oraz dane osoby zgłaszającej;
7.3.44. umożliwiać przeglądanie bazy wiedzy z poziomu incydentu i podłączanie rozwiązania z bazy rozwiązań do rozwiązania w zgłoszeniu;
7.3.45. automatycznie podpowiadać serwisantom możliwe do zastosowania rozwiązania dla zgłoszeń, zapisuje również rozwiązania, które zostały zastosowane w zgłoszeniu, ale zostały odrzucone przez zgłaszającego;
7.3.46. umożliwiać implementację warunków umów SLA i na tej podstawie obliczania czasu rozwiązania incydentu. Atrybuty umowy SLA, na postawie których system wylicza czas rozwiązania incydentu muszą zawierać co najmniej taki parametr jak nazwa użytkownika, oddział, komputer, priorytet, poziom;
7.3.47. posiadać moduł zarządzania bazą wiedzy, który umożliwia rejestrację rozwiązań zawierających co najmniej następujące atrybuty: temat i opis rozwiązania, powiązane słowa kluczowe, klasyfikacja rozwiązania – umożliwia on:
- klasyfikację rozwiązań w strukturze drzewiastej katalogu, dowolnie definiowanego przez użytkownika;
- przeszukiwanie danych po dowolnych atrybutach rozwiązania.
- udostępnianie rozwiązań osobno dla użytkowników i osobno dla serwisantów;
- rejestrację rozwiązań z poziomu incydentu;
- przeglądanie rozwiązań bez konieczności logowania się użytkownika do systemu;
- dokonanie akceptacji dodawanego do bazy wiedzy rozwiązania przez administratora bazy wiedzy;

- zamieszczanie i wyświetlanie w treści rozwiązania plików graficznych oraz dołączania dowolnej ilość załączników;
- przesłanie rozwiązania do użytkownika za pomocą poczty elektronicznej bez konieczności powiązania tego działania z procesem zarządzania incydentem;
- automatyczne podpowiadanie serwisantom możliwych do zastosowania rozwiązania dla zgłoszeń, zapisuje również rozwiązania które zostały zastosowane w zgłoszeniu ale zostały odrzucone przez zgłaszającego;
- automatyczne podpowiadanie możliwych do wykorzystania rozwiązania dla aktualnie rejestrowanych zgłoszeń - sugestie rozwiązań są przedstawiane zgłaszającym podczas rejestrowania zgłoszenia w postaci listy rozwijalnej rozwijanej pod tematem zgłoszenia oraz okienka typu „pop-up" kliknięciu w przycisk rejestracji zgłoszenia;
- ukrycie bazy wiedzy lub jej części przed zgłaszającymi;
- moduł bazy wiedzy powinien posiadać API;

7.3.48. umożliwiać tworzenie raportów zarejestrowanych incydentów, problemów i zmian filtrowanych według kategorii, departamentu, statusu zgłoszenia, użytkownika;

7.3.49. umożliwiać tworzenie raportów umożliwia utworzenie raportów przedstawiających rozkład incydentów w czasie według dowolnego atrybutu, próbkowane co jeden dzień roboczy;

7.3.50. umożliwiać tworzenie raportów czasu pracy użytkowników w ramach rozwiązywania zgłoszeń;

7.3.51. posiadać wbudowaną funkcjonalność exportu utworzonych raportów do plików formatu HTML, PDF, XLS, XLSX, CSV, DOC, DOCX, XML;

7.3.52. umożliwiać automatyczne tworzenie raportów, zdefiniowanych według cyklicznego harmonogramu, a następnie przesyłanie tychże raportów za pomocą poczty elektronicznej do dowolnego użytkownika;

7.3.53. umożliwiać dostęp do modułu raportowego tylko wybranym technikom;

7.3.54. posiadać funkcjonalność wykonywania zapytań SQL do bazy danych systemu, funkcjonalność ta jest realizowana poprzez interfejs webowy oprogramowania;

7.3.55. umożliwiać tworzenie dynamicznych wskaźników prezentowanych na tablicy wskaźników;

7.3.56. umożliwiać tworzenie dowolnie customizowanych tablic wskaźników w oparciu o raporty generowane z systemu oraz raporty zewnętrzne możliwe do przedstawienia w tablicy;

7.3.57. umożliwiać edycję tablic wskaźników w oparciu o mechanizm przeciągania i upuszczania poszczególnych obiektów na tablicy wskaźników;

7.3.58. umożliwiać przyłączenie do niego zewnętrznych systemów raportujących, takich jak Crystal Reports, Jasper Reports lub równoważnych;

7.3.59. posiadać portal ESM, który pozwala na:

- tworzenie osobnych instancji dla poszczególnych biznesów;
- wdrożenie specyficznych dla biznesu przebiegów procesu dla każdej instancji;
- używanie predefiniowanych formularzy zgłoszeń w zależności od typu instancji;
- tworzenie scentralizowanego portalu ESM, który zapewnia pracownikom dostęp do określonych lub wszystkich instancji.

7.4. Wymagania dotyczące modułu zarządzania zasobami

7.4.1. system powinien umożliwiać cykliczne automatyczne skanowanie i inwentaryzacje min 750 zasobów takich jak stacje robocze czy urządzenia sieciowe.

7.4.2. system powinien posiadać moduł wykrywania środowiska, który umożliwia zbieranie danych o konfiguracji sprzętu:
- skanowanie urządzeń na podstawie integracji z systemem do zarządzania stacjami roboczymi i urządzeniami mobilnymi dostarczanego w niniejszym zapytaniu;
- skanowanie urządzeń z wykorzystaniem Telnet / SSH;
- skanowanie urządzeń z wykorzystaniem poświadczeń VMware;
- skanowanie urządzeń z wykorzystaniem SNMP V1, V2, V3;
- poświadczenia SNMPv3 wspierają SHA256 oraz SHA512;

7.4.3. skanowanie z wykorzystaniem agenta umożliwia zbieranie danych conajmniej o:
- ilość i rodzaj procesorów;
- ilość i rodzaj kości pamięci RAM;
- ilość dostępnej pamięci wirtualnej oraz fizycznej;
- numer seryjny komputera (ServcieTag);
- zainstalowane karty sieciowe z adresami IP oraz MAC;
- zainstalowane dyski twarde z numerem seryjnym oraz pojemnością;
- zainstalowane drukarki;
- zainstalowany system operacyjny, oprogramowanie oraz poprawki;
- konta użytkowników;

7.4.4. system powinien pozwalać na przypisywanie zasobu do użytkownika, działu, lokalizacji;

7.4.5. system powinien posiadać możliwość wprowadzania zasobów skanowanych po kodzie kreskowym;

7.4.6. system powinien posiadać mechanizm generowania kodów kreskowych dla zasobów. Moduł pozwala na zdefiniowanie formatu kodu kreskowego i jego wydruk według zdefiniowanego formatu wydruku;

7.4.7. system powinien umożliwiać przeprowadzenie wykrywania zmian w konfiguracji i generowania raportów porównawczych zmian w elementach konfiguracji;

7.4.8. system powinien umożliwiać przeprowadzenie automatycznych, zdefiniowanych według cyklicznego harmonogramu audytów konfiguracji komputerów i serwerów, pod kątem zmian w konfiguracji i zainstalowanym oprogramowaniu;

7.4.9. system powinien umożliwiać przeprowadzenie skanowania komputerów i zasilenie danych do bazy dla komputerów niepodłączonych do sieci komputerowej. Możliwe jest zastosowanie dedykowanego skryptu VBS, którego plik wynikowy następnie zostanie zaimportowany do bazy;

7.4.10. system powinien pozwalać na zarządzanie licencjami oprogramowania poprzez ich rejestrowanie w systemie. Licencja posiada informacje co najmniej o typie licencji, dozwolonej ilości instalacji, kluczu licencji;

7.4.11. system powinien pozwalać na wizualną prezentację ilości licencji;

7.4.12. system powinien integrować się z Microsoft 365 w celu zarządzania licencjami;

7.4.13. system powinien posiadać mechanizm wypożyczania sprzętu użytkownikom, który pozwala na:
- określenie zasobów możliwych do wypożyczenia;
- określenie maksymalnego czasu trwania wypożyczenia;
- określenie przyczyny wypożyczenia;
- weryfikowanie listy wypożyczonego sprzętu;
- powiadamianie użytkowników o konieczności zwrócenia wypożyczonego sprzętu;

7.4.14. system powinien posiadać moduł uzupełniania zasobów, który pozwala na utrzymywanie stanów minimalnych określonych typów zasobów;

- system powinien pozwalać na grupowanie zasobów w sposób statyczny lub dynamiczny z wykorzystaniem kryteriów takich jak: typ zasobu, model, producent, status zasobu, region, lokalizacja, dział. Użytkownik, domena, ilość pamięci RAM, typ procesora, taktowanie procesora, typ monitora, typ myszki, typ klawiatury, adres IP;
- system powinien pozwalać na określenie statusu zasobu oraz dodawanie własnych statusów, takich jak: na stanie, w użyciu, zużyte, zutylizowane.

7.5. Wymagania dotyczące modułu zarządzania umowami

7.5.1. system powinien posiadać możliwość zarządzania umowami serwisowymi:

- posiadać możliwość tworzenia umów, przegląd, edycje oraz usuwanie;
- umożliwiać rejestrację warunków umów gwarancyjnych i serwisowych, w tym w szczególności dane teleadresowe gwaranta, czas obowiązywania umowy, jej koszt, warunki na jakich umowa jest świadczona;
- posiadać funkcjonalność pozwalającą przesyłać powiadomienia o wygaśnięciu okresu obowiązywania umowy serwisowej i gwarancyjnej;
- posiadać możliwość dołączenia załączników;
- posiadać możliwość tworzenia tzw. umów podrzędnych do głównej umowy;
- pozwalać na tworzenie dodatkowych pól niezbędnych i wymaganych przez organizacje;
- pozwalać na powiązanie umowy z zasobami.

7.6. Wymagania dotyczące modułu zarządzania zakupami

7.6.1. moduł zarządzania zakupami umożliwia przeprowadzenie procesu zakupowego składającego się z co najmniej następujących kroków:

- utworzenie zamówienie – rejestracja numeru zamówienia, powiązanie z dostawcą, określenie terminu realizacji zamówienia.
- dodanie pozycji do zamówienia – rejestracja produktów, ich ilości oraz ceny jednostkowej produktu;
- przedstawienie zamówienia do akceptacji – moduł zarządzania zakupami umożliwia przeprowadzenie weryfikacji i akceptacji zamówienia przez osoby trzecie, z tymże użytkownik rejestrujący zamówienie nie może być jednocześnie osobą trzecią weryfikującą i akceptującą realizację zamówienia;
- powiązanie zamówienia z elementami konfiguracji w bazie zasobów;
- moduł zarządzania zakupami umożliwia przesłanie powiadomienia do osób trzecich o przekroczonym terminie realizacji zamówienia;

7.6.2. moduł zarządzania zakupami umożliwia przydzielenie zamówienia do wybranego centrum kosztów (Cost Center) oraz konta księgi głównej w księgowości;

8. Wymagania dotyczące sprzętu:

8.1. Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej:

8.1.1. nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych;

8.1.2. nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta;

8.1.3. elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta;

8.1.4. w okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia;

8.1.5. urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta;
8.1.6. urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta;
8.1.7. do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej;
8.1.8. gwarancja i serwis na urządzenia musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku gdy Oferent nie posiada takiej autoryzacji;
8.1.9. urządzenia na etapie dostawy producent a zamawiający nie mogą podlegać modyfikacjom;
8.1.10. zamawiający wymaga możliwości sprawdzenia statusu gwarancji i konfiguracji oferowanego sprzętu na stronie producenta, po podaniu jego numeru seryjnego;
8.1.11. na min. 3 dni przed dostawą sprzętu należy przesłać Zamawiającemu wykaz numerów seryjnych oferowanych urządzeń celem weryfikacji u producenta spełnienia w/w wymagań;
8.1.12. wymagane jest pisemne oświadczenie producenta potwierdzające pochodzenie serwera z oficjalnego kanału dystrybucyjnego;
8.1.13. niżej wymienione parametry stanowią specyfikację minimalną – dopuszczalne jest zastąpienie każdego z elementów nowszym i nie mniej wydajnym odpowiednikiem;
8.1.14. wszystkie urządzenia muszą być wyprodukowane zgodnie z normą ISO-9001, ISO-140001 lub równoważną oraz posiadać deklarację CE lub równoważną, potwierdzającą zgodność z R & TTE 1999/5/EC1, rozporządzeniem Komisji (WE) nr 1275/2008 oraz przepisami dyrektywy ErP 2009/125/WE;
8.1.15. wszystkie urządzenia muszą być objęte gwarancją producenta na okres minimum 36 miesięcy wraz z usługą serwisu gwarancyjnego świadczoną w miejscu instalacji przez inżyniera.

8.2. Serwer w obudowie typu „rack” (1 sztuka):
8.2.1. obudowa rack o wysokości 1U umożliwiająca instalację minimum 8 dysków 2.5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z ramieniem do mocowania kabli;
8.2.2. zatoki dyskowe do zainstalowania dysków SFF typu „Hot-Plug” NVMe U.3/SAS/SATA/SSD 2.5”:
- gotowe do zainstalowania 8 dysków;
- z opcją rozbudowy o dodatkowe 2 dyski montowane z przodu obudowy;
8.2.3. czujnik otwarcia obudowy współpracujący z BIOS / UEFI;
8.2.4. zdejmowany panel przedni z możliwością dodania zamka chroniącego przed nieuprawnionym dostępem do dysków;
8.2.5. umieszczona z przodu chowana karta identyfikacyjna serwera;
8.2.6. dwuprocesorowa płyta główna fabrycznie obsługująca procesory po 160 rdzeni i mocach maksymalnych po 390W, wyposażona w moduł TPM 2.0 lub nowszy;
8.2.7. zainstalowane 2 (dwa) procesory piątej generacji AMD EPYC 9115 2.6GHz 16C;
8.2.8. pamięć operacyjna RAM:
- zainstalowane 1TB pamięci typu DDR5 Registered 5600MT/s w modułach dwubankowych o pojemności 64GB każdy;
- możliwość rozbudowy do 1.5TB bez wymiany zainstalowanych pamięci;

- płyta główna z 24 slotami na pamięć umożliwiająca instalację 6TB pamięci przy zastosowaniu odpowiednich modułów (np. obsługująca 24 moduły po 256GB);
- wsparcie dla technologii zabezpieczania pamięci „Advanced ECC";

8.2.9. serwer musi być wyposażony w 2 aktywne gniazda PCIe Gen5 x16 (bus width) gotowe do obsadzenia kartami;

8.2.10. zainstalowane 2 (dwa) dyski 480GB NVMe M.2 typu „Hot-Plug" skonfigurowane fabrycznie w RAID1 z tyłu serwera;

8.2.11. możliwość rozbudowy o sprzętowy kontroler RAID (na dedykowanym slocie płyty głównej) spełniający wymagania:
- obsługa napędów dyskowych SAS, SATA i NVMe;
- obsługa trybów RAID 0, 1, 5, 6, 10, 50, 60;
- możliwa równoczesna praca w trybach RAID i HBA;
- bateryjne podtrzymanie pamięci cache kontrolera;
- obsługa 16 napędów dyskowych przy 4GB pamięci cache lub
  obsługa 32 napędów dyskowych przy 8GB pamięci cache;

8.2.12. interfejsy sieciowe:
- zainstalowane w dedykowanych slotach, nie zajmujące slotów PCIe opisach wyżej 2 (dwie) dwuportowe karty sieciowe 10Gbps SFP+ wraz z oryginalnymi wkładkami LC SR;
- zainstalowana dwuportowa karta Fibre Channel 32 Gb z wkładkami SW;
- dedykowany port 1Gb RJ45 dla karty zarządzającej;

8.2.13. zintegrowana karta graficzna;

8.2.14. porty:
- VGA na tylnym panelu;
- dedykowany port USB z przodu serwera dla karty/modułu zarządzającego;
- minimum 5 portów USB 3.2 Gen1 – 1 z przodu, 2 z tyłu, 2 wewnątrz;
- możliwość rozbudowy o port szeregowy typu DB9/DE-9 (9-pinowy) wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45, bez konieczności instalowania kart w slotach PCIe;
- możliwość rozbudowy o cyfrowy port wideo z przodu serwera;
- ilość dostępnych złączy nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy, konwerterów IP, kart PCIe, itp.;

8.2.15. możliwość rozbudowy o wewnętrzny napęd DVD-ROM lub DVD-RW;

8.2.16. 2 (dwa) redundatne zasilacze typu „Hot-Plug" o sprawności 96% (tzw. klasa Titanum) i mocy min. 1000W każdy;

8.2.17. redundantny zestaw wentylatorów typu „Hot-Plug" – minimum 7 sztuk;

8.2.18. diody LED z przodu serwera, pozwalające uzyskać informacje o jego stanie;

8.2.19. możliwość rozbudowy o elektroniczny panel diagnostyczny dostępny z przodu serwera, pozwalający uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy oraz o temperaturze;

8.2.20. karta / moduł zarządzający – niezależna od systemu operacyjnego, zintegrowana z płytą główną lub zainstalowana w gnieździe PCI dodatkowa karta posiadająca aktywne funkcjonalności:
- monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe dyski (fizyczne i logiczne);
- wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym;
- 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) oraz poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface);
- wbudowane narzędzia diagnostyczne;
- zdalna konfiguracji serwera (BIOS / UEFI / RAID) i instalacji systemu operacyjnego;
- 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 CD/DVD/ISO/FDD w trybie HTML5;
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie;
- 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;
- możliwość trwałego zablokowania dokonania obniżenia wersji oprogramowania układowego (firmware) serwera;
- wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API;
- możliwość autokonfiguracji sieci karty zarządzającej (DNS / DHCP);

8.2.21. możliwość rozszerzenia o wyposażony w interfejs graficzny centralny system zarządzania serwerami w formie wirtualnej maszyny, dla której Zamawiający udostępni odpowiednie zasoby w swoim środowisku wirtualnym;

8.2.22. wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych:
- Microsoft Windows Server, min. 2019, 2022, 2025;
- VMware ESXi, min. 7, 8;
- Red Hat Enterprise Linux (RHEL), min. 8.6, 9.0;
- SUSE Linux Enterprise Server (SLES), min. 15;
- Ubuntu, min. 20.04 LTS, 22.04 LTS, 24.04 LTS;
- Oracle Linux, min. 9;

8.2.23. serwer musi znajdować się na liście liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2019, 2022, 2025;

8.2.24. dołączona licencja Microsoft Windows Server 2025 w wersji Data Center;

8.2.25. dołączony komplet (2 sztuki) kabli zasilających z wtyczką C13-C14 o długościach co najmniej 2 metry każdy;
8.2.26. reakcja w ramach gwarancji producenta najpóźniej w następnym dniu roboczym (NBD) od zgłoszenia.

9. W ramach konfiguracji i wdrożenia Wykonawca:
   9.1. Dokona synchronizacji użytkowników i komputerów z Active Directory Zamawiającego.
   9.2. Zaimplementuje w ramach wdrażanego systemu dystrybucję agentów dla stacji roboczych użytkowników min 200 sztuk.
   9.3. Uruchomi portal sklep do samodzielnej instalacji oprogramowania przez użytkownika.
   9.4. Skonfiguruje możliwość pomocy zdalnej w ramach LAN/WAN jak również poza siecią Zamawiającego (SGS).
   9.5. Skonfiguruje wykaz systemów informatycznych, wskazanych przez Zamawiającego, jako inwentaryzacja oprogramowania na stacjach użytkowników.
   9.6. Skonfiguruje wykaz grup i poziomów wsparcia, względem lokalizacji i odpowiedzialności za dany system informatyczny (możliwość przynależności jednego Operatora do kilku grup wsparcia).
   9.7. Skonfigurowanie cyklicznych raportów.
   9.8. Wdroży i przetestuje na wybranych stacjach roboczych (10 sztuk) poprawność dystrybucji:
      9.8.1. systemów operacyjnych (po 1 obrazie Windows 11 z dynamicznym przypisywaniem najlepszych sterowników względem przynajmniej 2 modeli komputerów);
      9.8.2. oprogramowania;
      9.8.3. aktualizacji.
   9.9. Wdroży i przetestuje polityki dla szyfrowania lokalnych dysków stacji roboczych.
   9.10. Skonfiguruje polityki automatycznych aktualizacji z uwzględnieniem grup testowych i docelowych.
   9.11. Skonfiguruje raporty z inwentaryzacji systemów.
   9.12. Skonfiguruje usługę typu sklep dla użytkownika.
10. Harmonogram realizacji zamówienia:
   10.1. Dostawa licencji dla wszystkich elementów wdrażanego systemu.
   10.2. Wdrożenie:
      10.2.1. przygotowanie środowiska sprzętowego i systemowego;
      10.2.2. instalacja oprogramowania;
      10.2.3. skonfigurowanie bazy użytkowników oraz integracja z Active Directory;
      10.2.4. testy wdrożeniowe;
      10.2.5. szkolenia specjalistyczne z administracji i użytkowania;
      10.2.6. przygotowanie nowych funkcjonalności;
      10.2.7. testy i wdrożenie globalne;
      10.2.8. Podsumowanie wdrożenia i przekazanie wszystkich dokumentów.
   10.3. Wsparcie serwisowe przez okresie 60 miesięcy od zawarcia umowy.
11. Cechy szkoleń:
   11.1. Szkolenia będą przeprowadzone z podziałem na zarządzanie serwerami i stacjami roboczymi.
   11.2. Szkolenie zawierać będzie część teoretyczną oraz praktyczną.
   11.3. Szkolenie będzie realizowane zdalnie za pośrednictwem platformy Microsoft Teams wystawionej przez Zamawiającego.
   11.4. Szkolenia będą trwały łącznie min. 16 godzin i będą realizowane zdalnie w cyklach ustalonych z Zamawiającym. Czas trwania jednego cyklu to max. po 6 godzin dziennie. Każdy cykl szkolenia zostanie nagrany za pośrednictwem platformy Microsoft Teams.

11.5. Ćwiczenia przeprowadzane będą w środowisku laboratoryjnym, stworzonym dla indywidualnych potrzeb klienta.

12. Gwarancja oraz wsparcie:
    12.1. Zamawiający wymaga świadczenia serwisu gwarancyjnego przez producenta lub autoryzowanego partnera producenta przez okres 60 miesięcy (5 lat);
    12.2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub autoryzowanego partnera producenta w języku polskim w zakresie:
        12.2.1. wsparcia zespołu inżynierów przez zgłoszenie w portalu producenta;
        12.2.2. pomocy w prawidłowej i zgodnej z wymaganiami producenta;
        12.2.3. doradztwa w zakresie konfiguracji oprogramowania;
        12.2.4. zdalnego wsparcia technicznego;
        12.2.5. pomocy w zakładaniu zgłoszeń serwisowych u producenta.
    12.3. Minimum raz w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
13. Postępowania przy zlecaniu usług serwisowych – 70 godzin:
    13.1. Zlecenia do realizacji przez Wykonawcę będą przesyłane w formie mailowej przez Zamawiającego na adres wskazany przez Wykonawcę. W przypadku zleceń na usługi serwisowych Wykonawca przed przystąpieniem do realizacji zlecenia musi uzyskać akceptację Zamawiającego dotyczącą warunków realizacji zlecenia – szacowanej ilości roboczogodzin na poszczególne prace składające się na zlecenie, terminu rozpoczęcia i zakończenia realizacji, miejsca realizacji itp. Na każde spotkanie Wykonawca zobowiązany będzie przygotować podsumowanie działań wykonanych przez niego od ostatniego spotkania. Termin spotkania będzie ustalany w trybie roboczym.
14. Czas reakcji na incydenty i awarie:

    Wykonawca zobowiązuje się w przypadku zgłoszenia awarii lub pojedynczego incydentu związanego z użytkowaniem, eksploatacją i poprawnością pracy systemów objętych usługami utrzymania i wsparcia w przeciągu 24 godzin od otrzymania od Zamawiającego e-maila ze zgłoszeniem podjąć działania zmierzające do analizy przyczyny wystąpienia awarii lub incydentu oraz przystąpić do jego naprawy. W celu potwierdzenia podjęcia działań Wykonawca jest zobowiązany przesłać zwrotny e-mail z potwierdzeniem do Zamawiającego.

    W przypadku gdy naprawa incydentu lub awarii miałaby przedłużyć się ponad 24 godzin od momentu otrzymania od Zamawiającego e-maila ze zgłoszeniem, Wykonawca niezwłocznie prześlę tę informację na wskazany przez Zamawiającego adres e-mail podając w korespondencji przyczyny powstania incydentu lub awarii (jeżeli możliwe były do wykrycia) oraz koniecznie prace do realizacji w kontekście wyeliminowania awarii lub incydentu. Przesłanie Zamawiającemu niniejszej informacji nie zwalnia Wykonawcy z podejmowania dalszych działań w celu niezwłocznego usunięcia incydentu lub awarii.
15. Instalacja, konfiguracja oprogramowania

    Wymagane jest wdrożenie zamówionego oprogramowania na środowisku Zamawiającego dostarczonym w ramach niniejszego postępowania. Instalacja i konfiguracja będzie wykonana w trybie zdalnym za pośrednictwem dostępów VPN oraz komunikacji Microsoft Teams. Zamawiający wymaga, aby w ramach realizacji przedmiotu zamówienia Wykonawca przeprowadził instalację i konfigurację zgodnie z wytycznymi Zamawiającego. Wykonawca zobowiązany jest w celu realizacji tych czynności oddelegować swojego inżyniera do wykonania prac u Zamawiającego, na czas niezbędny do wykonania tych czynności, nie dłuższy niż zaoferowany w ofercie termin realizacji. Uruchomieniu i konfiguracji systemu zgodnie z politykami oraz wskazaną konfiguracją przez Zamawiającego.