**I Przedmiot zamówienia obejmuje:**

1. Dostarczenie systemu do zarządzania urządzeniami końcowymi (tj. stacjami roboczymi, serwerami, urządzeniami mobilnymi) zwanego dalej „Systemem” zgodnie z opisem przedmiotu zamówienia oraz udzielenie lub zapewnienie udzielenia licencji niezbędnych do prawidłowego działania Systemu w ilości pozwalającej na zarządzanie co najmniej 70 tyś urządzeń końcowych (tj. stacji roboczych, serwerów, urządzeń mobilnych), w tym pozwalać na zainstalowanie i skonfigurowanie co najmniej 11 niezależnych instancji Systemu w odrębnych lokalizacjach.
2. Opracowanie projektu wdrożeniowego obejmującego instalację i konfigurację Systemu oraz integrację z systemami obecnie funkcjonującymi w 11 lokalizacjach zlokalizowanych w jednostkach na obszarze 11 apelacji ,
3. Uruchomienie i dokonanie konfiguracji Systemu dla 11 niezależnych instancji Systemu w oparciu o założenia projektu wdrożeniowego
4. Przeprowadzenie instruktażu stanowiskowego dla minimum 15 pracowników wskazanych przez Zamawiającego z zakresu funkcjonowania dostarczonego Systemu i administrowania nim, w podziale na 3 odrębne grupy. Instruktaż obejmuje 16 godzin szkoleniowych dla każdej grupy
5. Udzielenie 36-miesięcznej gwarancji, w ramach której zostanie zapewniona opieka serwisowa dla dostarczonego i uruchomionego Systemu,
6. Wykonanie dokumentacji powykonawczej,
7. Zapewnienie 1000 roboczogodzin asysty technicznej eksperta.

**II Wymagania funkcjonalne systemu**

1. Dostarczone licencje na system muszą być bezterminowe.
2. Dostarczone licencje na system muszą zostać dostarczone wraz z 36 miesięcznym wsparciem świadczonym w języku polskim, liczonym od daty zakończenia wdrożenia.
3. System musi posiadać w pełni polski interfejs językowy.
4. Dostęp do systemu musi być zapewniony za pośrednictwem konsoli webowej bez konieczności instalacji dodatkowych komponentów.
5. System musi realizować bezpośrednio zarządzanie wszystkimi modułami Systemu z poziomu tej samej konsoli zarządzającej.
6. System musi posiadać architekturę trójwarstwową składającą się z bazy Danych, serwera aplikacji oraz agenta.
7. System musi obsługiwać bazy danych co najmniej PostgreSQL, MS SQL Server jako instancje do przechowywania danych
8. System musi umożliwiać instalację agentów na systemie operacyjnym Windows 2008 i nowszym, Windows 7 i nowszym, Mac OS 10.7 i nowszym, Linux (co najmniej RedHat)
9. System musi posiadać wbudowane funkcjonalności wykonywania backupu konfiguracji Systemu i jego przywracania w tym co najmniej bazy danych, odtworzenia bazy danych etc,
10. System musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen (Active Directory).
11. System musi pozwalać na instalacje nieograniczonej ilości elementów Systemu (np. serwerów zarządzających, serwerów dystrybucyjnych itp.) w ramach pojedynczej instancji Systemu.
12. System musi posiadać wbudowaną funkcjonalność umożliwiającą konfigurację mechanizmów wysokiej dostępności (tzw. failover)
13. System musi pozwalać na pracę co najmniej 1 tyś operatorów jednocześnie niezależnie od ilości instancji (tj. kont o użytkownikach o podwyższonych uprawnieniach w Systemie np. operator, administrator itp.),
14. System musi posiadać możliwość włączenia opcji uwierzytelniania dwuskładnikowego.
15. System musi umożliwiać obsługę wielu jednoczesnych sesji operatorów konsoli (np. licencja pływająca) umożliwiającą jednoczesną pracę wielu operatorów na wybranych instancjach zainstalowanych konsol zarządzających.
16. System musi posiadać możliwość integracji z kontami Active Directory jak i możliwość dodania nowego użytkownika systemu z uwierzytelnianiem lokalnym.
17. System musi posiadać rozbudowany system zarządzania użytkownikami z podziałem na role np. administratora, audytora, gościa, menadżera zasobów, menadżera poprawek, z możliwością dodawania nowych ról z określonymi uprawnieniami.
18. System musi posiadać funkcjonalność zarzadzania urządzeniami końcowymi zarówno w infrastrukturze Jednostek jak i poza nią z zachowaniem takiej samej funkcjonalności niezależnie od aktualnej lokalizacji urządzenia końcowego. (tj. miejsca podłączenia do sieci LAN, WAN, INTERNET etc).
19. System musi rozpoznawać stacje robocze i serwery w ramach Active Directory (posiadać mechanizmy integracji z Active Directory) jak i Workgroup.
20. System musi pozwalać na import komputerów z pliku np. CSV.
21. System musi umożliwiać konfigurację ustawień i polis dostępu do zasobów w tym co najmniej 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.
22. Agent systemu musi realizować wszystkie wymagane funkcjonalności za pomocą aplikacji lub usług wyprodukowanych i podpisanych cyfrowo przez Producenta bez użycia aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
23. System musi posiadać wbudowane narzędzie zdalnego dostępu (sesji) z możliwością uzyskania potwierdzenia dostępu przez użytkownika oraz ma możliwość włączenia opcji nagrywania tych sesji np. z wykorzystaniem technologii ActiveX, HTML 5.
24. System musi umożliwiać prowadzenie konwersacji z użytkownikiem poprzez czat tekstowy oraz komunikację głosową i video.
25. Konfiguracja polityk dostępu do USB powinna umożliwiać blokowanie co najmniej poniższych typów urządzeń, a także mieć możliwość wykluczania z listy zablokowanych konkretnych urządzeń o danym identyfikatorze urządzenia lub danego dostawcy tj:
    1. Mysz,
    2. Stacja dysków (takie jak napędy USB, zewnętrzne dyski twarde które są szyfrowane przy pomocy BitLocker),
    3. CD ROM,
    4. Urządzenia przenośne (takie jak telefony komórkowe, kamery cyfrowe i przenośne odtwarzacze multimedialne),
    5. Bluetooth,
    6. Obraz (takie jak kamery USB i skanery), drukarka,
    7. Modem,
    8. Urządzenia USB Apple (takie jak iPad, iPhone i iPod, łączące się z programem iTunes)
26. System musi posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.
27. System musi posiadać możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika w tym umożliwiać instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.
28. System musi posiadać funkcjonalność umożliwiającą tworzenie list aplikacji, które będą mogły być instalowane przez samego użytkownika z poziomu stacji roboczej korzystając z centralnego repozytorium aplikacji.
29. System musi posiadać możliwość blokowania plików wykonywalnych co najmniej EXE, MSI, BAT poprzez reguły oparte co najmniej na ścieżce aplikacji lub wartości hash,
30. System musi umożliwiać uruchamianie zdalnego menedżera systemu dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, pozwalającego na:
31. podgląd i zamykanie uruchomionych procesów na stacji roboczej,
32. podgląd, uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej,
33. uruchamianie zdalnego wiersza poleceń,
34. podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej,
35. przegląd logów systemowych stacji roboczej,
36. podgląd menedżera urządzeń,
37. podgląd udziałów sieciowych
38. System musi posiadać funkcjonalność umożliwiającą rozpoznawania komponentów sprzętowych oraz oprogramowania zainstalowanego na stacjach roboczych i serwerach.
39. System musi posiadać wbudowane funkcje zarządzania i wdrażania poprawek systemowych i ServicePack na stacjach roboczych oraz serwerach, w szczególności musi rozpoznawać sekwencje instalacji.
40. System musi posiadać wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia co najmniej w oparciu o brakujące poprawki systemowe.
41. System musi posiadać możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.
42. Funkcje wdrażania poprawek powinny obejmować co najmniej oprogramowanie:
    1. systemy operacyjne Windows 7 i nowsze wersje,
    2. systemy operacyjne Windows Server 2008 i nowsze wersje,
    3. aplikacje: Microsoft Office, Google Chrome, Opera, Skype, Mozilla Firefox, Adobe Reader, Adobe Acrobat, Adobe Shockwave Player, Adobe Flash Player, Java
43. System musi umożliwiać wykrywanie zakazanego oprogramowania (np. nie znajdującego się na liście dozwolonego oprogramowania) i uruchamiać działania naprawcze, w tym automatyczne odinstalowanie niepożądanej aplikacji.
44. System musi posiadać możliwość włączenia metryk wykorzystania wskazanej aplikacji co najmniej w zakresie liczenia czasu korzystania z aplikacji.
45. System musi umożliwiać dodawanie i rozliczanie licencji odnalezionych na urządzeniach administrowanych przez system.
46. System musi posiadać zintegrowany moduł do wdrażania systemów operacyjnych, który umożliwia przechwytywanie obrazów systemu operacyjnego a następnie pozwala wdrożyć go na komputerach przenośnych, stacjach roboczych i serwerach.
47. System umożliwia tworzenie tzw. wzorców (ang. Template) dystrybucji obrazów, które pozwalają na dystrybucję przygotowanego obrazu zgodnie z określonymi zasadami takimi jak:
    1. Zadania po dystrybucji obrazu /Restart, Zamknięcie systemu/
    2. Zarządzanie tzw. SID (en.: Security Identifier)
    3. Możliwość nadania nazwy komputera
    4. Dodanie komputera do domeny AD
    5. Instalacja dodatkowego oprogramowania
48. System musi posiadać możliwość tworzenia zadań dystrybucji pozwalających na automatyzacje procesu dystrybucji obrazów systemów.
49. System musi posiadać możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalający na dystrybucję obrazu z możliwością wyboru systemów z dostępnej listy komputerów.
50. System musi umożliwiać dystrybucję zadań oraz plików np. z dedykowanego dla każdej lokalizacji repozytorium plików.
51. System musi obsługiwać następujące metody dystrybucji obrazów:
52. Multicast,
53. Unicast
54. oraz pozwalać na tworzenie harmonogramu tejże dystrybucji.
55. System musi posiadać możliwość przechowywania informacji o sterownikach, a także zapewnia ich dystrybucje w obrazach
56. System posiada możliwość tworzenia bootowalnych mediów a także ich edycję:
57. PXE
58. ISO
59. USB
60. System posiada repozytorium możliwych do zainstalowania aplikacji po procesie dystrybucji obrazu a także posiada możliwość edycji tychże aplikacji.
61. System musi posiadać funkcjonalność zarządzania urządzeniami 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, Windows 10.
62. System musi posiadać funkcjonalność rozpoznawania i dodawania urządzeń poprzez mechanizmy:
    1. Over-the-Air (OTA), ręczne dodawanie urządzeń,
    2. zbiorcze dodawanie urządzeń z pliku CSV,
    3. uwierzytelnione np. dodawanie z jednorazowym kodem i/lub poświadczeniami użytkownika AD.
63. System musi posiadać funkcjonalność wyświetla informacji o urządzeniu co najmniej:
64. IMEI,
65. IMSI,
66. numer telefonu,
67. zainstalowane aplikacje itp.
68. Wersje systemu operacyjnego,
69. Producent /Model
70. Adres mac bluetooth
71. Adres mac wifi
72. Zajęte i wolne miejsce na urządzeniu
73. W przypadku androida czy urządzenie jest zrotowane
74. Czy szyfrowanie jest włączone
75. Certyfikaty zainstalowane na urządzeniu
76. System musi posiadać funkcjonalność zarządzania bezpieczeństwem obejmujący co najmniej:
77. kod dostępu tj. wymuszenie kodu w celu blokowania nieautoryzowanego dostępu,
78. zdalna blokada tj. w celu uniknięcia niepowołanego użycia utraconego urządzenia,
79. pełne czyszczenie tj. usunięcie wszystkich danych z telefonu w celu wycieku danych po kradzieży,
80. organizacyjne czyszczenie tj. usunięcie tylko danych organizacyjnych i pozostawienie danych prywatnych
81. szyfrowanie pamięci,
82. zablokowanie rootowania urządzenia
83. Przywracanie ustawień fabrycznych
84. Zmiana ustawień powiadomień na zablokowanym ekranie
85. Instalacja aplikacji spoza sklepu
86. włączanie trybu developerskiego
87. dodawanie użytkowników
88. System musi pozwalać na nakładanie restrykcji co najmniej w zakresie:
89. szyfrowanie pamięci wewnętrznej urządzenia,
90. ograniczanie użytkowania kamery, mikrofonu, robienia zrzutów ekranu
91. ograniczanie użytkowania określonych aplikacji,
92. wymuszenie określonej konfiguracji ustawień polis dostępu do zasobów organizacyjnych np. mail, Wi-Fi, VPN
93. uwierzytelnianie przy użyciu identyfikatora FaceID
94. zabronić urządzeniom firmowym wykonywania konfiguracji zbliżeniowych
95. Ograniczenie używania bluetooth i NFC
96. Ograniczenie wykorzystania kart SD
97. Ograniczenie opcji wbudowanej przeglądarki internetowej
98. Blokada trybu samolotowego
99. Blokada wifi i USB tethering
100. Blokada wyłączenia usług lokalizacji
101. System musi umożliwiać dystrybucję certyfikatów CA na urządzenia z systemem iOS oraz Android, przy użyciu profilu certyfikatu.
102. System musi obsługiwać protokół Simple Certificate Enrollment Protocol (SCEP) do integracji z urzędem certyfikacji za pomocą SCEP w celu automatyzacji dystrybucji certyfikatów klienta na urządzenia z systemem iOS.
103. System musi pozwalać na integrację z urzędem certyfikacji za pomocą SCEP, aby zautomatyzować dystrybucję certyfikatów klienta na urządzenia z systemem Windows.
104. System musi pozwalać na import certyfikatów SSL z rozszerzeniami takimi jak .jks i .keystore
105. System musi pozwalać na obsługę trybu Kiosk dla urządzeń z systemem Android oraz IOS.
106. System musi pozwalać na konfiguracje konta Android for Work w szczególności na konfiguracje uprawnień i konfiguracje aplikacji oraz konteneryzację urządzeń z Androidem w wersji 5.0 lub nowszej.
107. System musi pozwalać na konfigurację systemu Android for Work bez pakietu G Suite.
108. System musi posiadać moduł zarządzania aplikacjami pozwalający na zarządzanie i dystrybucja własnych aplikacji w trybie cichym
109. System musi umożliwiać integracja z programem Apple VPP,
110. System musi pozwalać na śledzenie i zabezpieczenie utraconych urządzeń przy użyciu trybu utraconego dla urządzeń z systemem Android oraz IOS.
111. System musi pozwalać na automatyzację przypisywania użytkowników urządzeniom z funkcją DEP (eng. Device Enrollment Program).
112. System musi pozwalać na wyświetlanie niestandardowych wiadomości i zapewnianie funkcji połączeń na ekranie blokady zagubionego urządzenia itp. na urządzeniach z systemem Android oraz iOS.
113. System musi pozwalać na obsługę Trybu kiosku dla urządzeń, które nie obsługują Android for Work.
114. System musi pozwalać na wprowadzenie nazwy punktu dostępowego (APN) dla urządzeń Samsung, aby skonfigurować komunikację opartą na komórkowej transmisji danych na zarządzanych urządzeniach.
115. System musi pozwalać na obsługę automatycznego usuwania aplikacji / profili powiązanych po usunięciu urządzenia z grupy konfiguracji urządzeń
116. System musi pozwalać na nawiązanie sesji zdalnej na urządzenia Android oraz IOS.
117. System musi pozwalać na wyszukiwanie urządzeń co najmniej za pomocą:
118. numeru telefonu urządzenia.
119. Nazwa użytkownika
120. Nazwa urządzenia
121. Wersja systemu operacyjnego
122. Model urządzenia
123. Wersja agenta
124. IMEI
125. Nr seryjny
126. Adres MAC wifi
127. Adres MAC bluetooth
128. System musi pozwalać na zarządzanie treścią, aby zdalnie dystrybuować dokumenty do zarządzanych urządzeń.
129. System musi pozwalać na rejestrację urządzeń co najmniej za pomocą:
130. Android Zero Touch,
131. NFC
132. Knox Mobile Enrollment
133. Apple Configurator
134. Azure Enrollment
135. System musi pozwalać na integrację z Microsoft Business Store.
136. System musi pozwalać na integrację z wieloma kontami DEP.
137. System musi pozwalać na obsługę wstępnie zdefiniowanych podstawowych ustawień aplikacji Windows przy użyciu Konfiguracji aplikacji.
138. System musi pozwalać na zarządzanie aktualizacjami systemu operacyjnego w celu zautomatyzowania i zaplanowania aktualizacji systemu operacyjnego na urządzeniach z systemem iOS i Android
139. System musi umożliwiać skonfigurowanie adresu URL strony głównej przeglądarki dla urządzeń z systemem Windows.
140. System musi pozwalać na instalację własnych aplikacji wykorzystywanych w organizacji
141. System musi posiadać opcję zarządzania systemami Windows 10 poprzez Modern Management.
142. System musi pozwalać zablokować urządzenia z systemem Windows 10 w jednej aplikacji, używając trybu Kiosk.
143. System musi pozwalać wyświetlać listy restrykcji użytkownikom urządzenia.
144. System musi umożliwić przeglądanie / pobieranie listy Urządzeń Mobilnych kwalifikujących się do programu Apple Free Repair.
145. System musi umożliwiać konfigurację ustawień prywatności urządzenia,.
146. System musi umożliwiać tworzenie grup urządzeń celem wdrażania polis, restrykcji i dystrybucji aplikacji do wszystkich urządzeń w grupie w tym grup urządzeń BYOD (Bring Your Own Device)
147. System musi pozwalać na wdrażanie ustawień konfiguracji Exchange Online/Office365
148. System musi posiadać funkcję Conditional Exchange Access – monitorowanie urządzeń mających dostęp do serwera Exchange
149. System musi posiadać funkcję Geofencing – tj. możliwość ograniczenia korzystania z urządzeń mobilnych do wybranych regionów geograficznych
150. System musi pozwalać na obsługę Google Play Protect dla urządzeń z systemem Android.
151. System musi posiadać interfejs API pozwalający na budowanie integracji z innymi systemami, w tym z systemami helpdesk klasy ITSM w zakresie co najmniej:
152. pobierania informacji o zinwentaryzowanym sprzęcie i aplikacjach
153. wymuszania wdrażania konfiguracji Systemu na podstawie zarejestrowanych zgłoszeń (tzw. ticketów) z systemów HelpDesk
154. System musi umożliwiać planowanie raportów i automatyczne przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres mailowy
155. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o kryteria dostępne z Systemu.
156. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.
157. System musi umożliwiać generowanie raportów na podstawie informacji o aktualności systemów operacyjnych co najmniej w zakresie:
     1. brakujących poprawek,
     2. zainstalowanych poprawek,
     3. komputery z/bez określonych poprawek
158. System musi umożliwiać generowanie raportów na podstawie informacji o aktualności oprogramowania co najmniej w zakresie:
159. Oprogramowanie według producenta,
160. daty zainstalowanego oprogramowania,
161. wykorzystanie oprogramowania przez komputer,
162. kucze produktu oprogramowania,
163. komputery z/bez określonego oprogramowania,
164. oprogramowanie specyficzne dla użytkownika
165. System musi umożliwiać generowanie raportów dotyczących licencji co najmniej w zakresie:
166. całkowita ilość licencji
167. wykorzystana/pozostała ilość licencji lub przekroczenie ilości licencji
168. Lista licencji do odnowienia
169. Lista licencji z informacją o dacie zakupu, dacie wygaśnięcia, producencie,
170. Ostatnio zainstalowane oprogramowanie
171. Niedozwolone oprogramowanie
172. Klucze produktu oprogramowania
173. Komputery z/bez określonego oprogramowania
174. System musi umożliwiać generowanie raportów dotyczących inwentaryzacji sprzętu co najmniej w zakresie:
175. komputery wg systemu operacyjnego
176. komputery wg producenta
177. komputery wg pamięci
178. komputery wg wykorzystania dysku
179. komputery wg typu urządzenia
180. mapowane dyski logiczne
181. modyfikacje komponentów sprzętowych (pamięci, dyski etc.)
182. konfiguracji sprzętowej
     * + płyta główna w zakresie model, producent, nr. seryjny,
       + CPU w zakresie nazwy, modelu, producenta, częstotliwości,
       + HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
       + RAM w zakresie wielkości pamięci,
       + karty sieciowej w zakresie model, adres IP, adres MAC,
       + karty graficznej w zakresie model.
183. System musi umożliwiać generowanie raportów na podstawie informacji dotyczących wykorzystania portów USB
184. System musi umożliwiać generowanie raportów na podstawie informacji dotyczących usług bezpieczeństwa co najmniej w zakresie:
185. Antivirus
186. Bitlocker
187. Firewall
188. System musi umożliwiać generowanie raportów na podstawie skanowania plików multimedialnych.
189. System musi posiadać możliwość logowania zdarzeń z operacji wykonywanych w Systemie, z możliwością ich eksportu/wysyłania do systemów klasy SIEM.

**III Wymagania w zakresie gwarancji**

1. W ramach udzielonej gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego awarii, oprogramowanie to musi zapewnić Odbiorcy brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie awarii.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu przez Odbiorcę.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe awarii Systemu w następujący sposób:
   1. **awaria krytyczna**, tj. niedostępność Systemu dla wszystkich użytkowników: czas reakcji do 4 godzin od chwili Zgłoszenia Serwisowego awarii przez Odbiorcę, czas naprawy (przywrócenia funkcjonalności systemu) do 48 godzin od chwili zgłoszenia awarii przez Odbiorcę;
   2. **awaria niekrytyczna** tj. niepowodująca niedostępności Systemu: czas reakcji do 8 godzin od chwili Zgłoszenia Serwisowego awarii przez Odbiorcę, czas naprawy (przywrócenia funkcjonalności Systemu) do 72 godzin od chwili Zgłoszenia Serwisowego awarii przez Odbiorcę.
   3. Wszelkie awarie będą zgłaszane przez Odbiorcę za pomocą udostępnionego przez Wykonawcę oprogramowania, o którym mowa w punkcie 1 powyżej.
   4. W przypadku potrzeby wydania poprawki do Systemu przez producenta, na wniosek Wykonawcy złożony w formie elektronicznej Odbiorca może zawiesić czas usunięcia awarii niekrytycznych, maksymalnie na 40 dni kalendarzowych.
4. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:
5. aktualizację i konfigurację Systemu przez Wykonawcę,
6. rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu.
7. W ramach udzielonej gwarancji Odbiorcy przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez producenta Systemu bez ponoszenia dodatkowych kosztów finansowych przez Odbiorcę. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Odbiorcy.

**IV Wymagania w zakresie dokumentacji**

1. Wykonawca w uzgodnieniu z Zamawiającym opracuje i dostarczy następującą Dokumentację Projektową:
   1. Projekt Wdrożenia Systemu, który musi zawierać, w szczególności: opis funkcjonalny Systemu, wykaz wymaganych elementów Systemu, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy, harmonogram wdrożenia,
   2. Dokumentację Testów Akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia,
2. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w szczególności:
   1. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
   2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
   3. instrukcje zarządzania systemem,
   4. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Odbiorcy.
3. Dokumentacja projektowa i powykonawcza powinna być dostarczona w wersji elektronicznej i być napisana w języku polskim. Procedury i instrukcje producenta rozwiązania mogą być dostarczone w języku angielskim lub polskim.

**V Wymagania w zakresie transferu wiedzy**

1. W ramach wdrożenia Wykonawca umożliwi Odbiorcy w siedzibie i w środowisku Odbiorcy transfer wiedzy dla co najmniej 15 osób wskazanych przez Odbiorcę polegający na możliwości uczestniczenia ww. osób przy wdrażaniu, konfiguracji i administracji Systemem. W szczególności transfer wiedzy polegać będzie na:
   1. zapewnieniu możliwości udziału osób wskazanych przez Odbiorcę przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
   2. udzielaniu odpowiedzi na pytania zadawane przez osoby wskazane przez Odbiorcę w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego Systemu w środowisku produkcyjnym Odbiorcy, w tym omówieniu wraz z przeprowadzeniem praktycznych scenariuszy możliwości Systemu w zakresie wykrywania, przeciwdziałania   
      i usuwania złośliwego oprogramowania,
   3. Zapewnieniu transferu wiedzy w zakresie konfiguracji Systemu i administracji Systemem, który musi być prowadzony na bieżąco w trakcie wdrożenia, lecz przed zakończeniem wdrożenia. Transfer wiedzy przeprowadzony zostanie w języku polskim.

**VI Wymagania w zakresie wdrożenia**

1. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień dostawy Systemu.
2. Czynności związane z instalacją w infrastrukturze Jednostek oraz uruchomieniem i konfiguracją systemu muszą być przeprowadzone przez personel Wykonawcy we współpracy z personelem IT wskazanym przez Zamawiającego.
3. W ramach wdrożenia Wykonawca przygotuje scenariusz wdrożenia systemu dla 11 niezależnych instancji systemu zgodnie z wymaganiami Zamawiającego,
4. Uruchomienie i dokonanie konfiguracji Systemu w każdej z instancji w oparciu o założenia projektu wdrożeniowego obejmujące,
5. instalację elementów Systemu
6. konfigurację ról i kont użytkowników
7. przygotowanie agenta i jego instalacja na wskazanych przez Zamawiającego co najmniej 20 stacjach końcowych
8. przygotowanie i dystrybucja co najmniej jednej przykładowej konfiguracji na wybranych urządzeniach
9. przygotowanie i dystrybucja co najmniej jednej przykładowej paczki aktualizacji oprogramowania na wybranych urządzeniach
10. W ramach wdrożenia Systemu muszą zostać przygotowane tzw. paczki cichej instalacji dla systemów Windows 7, Windows 10, jak również systemów serwerowych Windows Server 2008, Windows serwer 2016. Paczka instalacyjna musi zawierać mechanizm automatycznej konfiguracji rozwiązania tj. podłączenia agenta do modułu zarządzania oraz instrukcję ich przygotowania i instalacji. Wymagane są także paczki instalacyjne dla systemów MacOS 10.7 oraz Linux (co najmniej RedHat).
11. Lokalizacje realizacji przedmiotu Umowy wskaże Zamawiający. Na wniosek Wykonawcy Jednostka może wyrazić zgodę w formie pisemnej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Jednostkę.
12. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Jednostki.
13. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie podpisany bez zastrzeżeń przez osoby wskazane przez Zamawiającego Protokół odbioru Systemu zawierający w szczególności:
    1. odbiór Systemu realizującego funkcjonalność na podstawie przeprowadzonych testów akceptacyjnych,
    2. odbiór dokumentacji powykonawczej,
    3. odbiór realizacji transferu wiedzy.

**VII Wymagania w zakresie asysty technicznej eksperta**

1. Świadczenie usługi asysty technicznej jest uprawnieniem jednostek realizowanym w ramach prawa opcji. Niewykorzystanie w całości lub w jakiejkolwiek części przewidzianych w umowie roboczogodzin, nie rodzi po stronie Wykonawcy żadnych roszczeń z tego tytułu w stosunku do Zamawiającego lub Jednostek.
2. W roboczogodzinę asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie tzn. nie ma znaczenia ile osób będzie świadczyło asystę techniczną eksperta w danej roboczogodzinie/roboczogodzinach. Rozliczenie roboczogodzin asysty technicznej eksperta odbywać się będzie za faktycznie wykorzystane roboczogodziny na podstawie Protokołów Odbioru Asysty Technicznej eksperta. Do godzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych w ramach realizacji Zgłoszeń Serwisowych awarii Systemu.
3. Asysta techniczna eksperta będzie dotyczyła oferowanego przez Wykonawcę Systemu i będzie polegała w szczególności na:
   1. bieżącym utrzymaniu i zarządzeniu Systemem,
   2. instalacji poprawek i nowych wersji oprogramowania dla Systemu, udostępnianych przez producenta wdrożonego Systemu,
   3. konsultacji w zakresie szczegółowej analizy zdarzeń generowanych przez System z wyłączeniem awarii,
4. Osoby uprawnione w umowie przez Odbiorcę będą przekazywać Wykonawcy zlecenia asysty technicznej, w których każdorazowo określony zostanie przedmiot zlecenia, oczekiwany termin realizacji zlecenia oraz miejsce realizacji zlecenia.
5. Wykonawca w terminie wyznaczonym przez Odbiorcę, od otrzymania zlecenia, przekaże Odbiorcy propozycję sposobu wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, tj. proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
6. Odbiorca może zaakceptować propozycję sposobu wykonania zlecenia albo odrzucić ją, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, dodatkowych wyjaśnień, informacji do przedstawionej propozycji sposobu wykonania zlecenia.
7. Jednostka zastrzega sobie prawo do zakwestionowania zaproponowanego przez Wykonawcę terminu realizacji oraz wyceny zleconych prac. W takiej sytuacji, Strony w drodze uzgodnień doprowadzą do akceptowalnej wyceny zleconych prac oraz terminu ich realizacji, co zostanie potwierdzone pisemnie, poprzez aktualizację zlecenia asysty technicznej.
8. Jednostka zastrzega sobie prawo do ostatecznego odrzucenia propozycji Wykonawcy i rezygnacji z realizacji zleconych prac, bez ponoszenia kosztów opisu sposobu wykonania zlecenia i przygotowania wyceny przez Wykonawcę.
9. W przypadku akceptacji propozycji sposobu wykonania zlecenia, Odbiorca przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
10. Rozliczenie asysty technicznej odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Jednostkę, Protokołów Odbioru Asysty Technicznej eksperta.
11. Odbiorca może wyrazić zgodę na wykonanie zlecenia zdalnie, w takim przypadku Wykonawca zobowiązany jest do przestrzegania wszystkich wymagań Jednostki. Jednostka zastrzega sobie prawo do odmowy, przerwania świadczenia usługi zdalnego dostępu w dowolnym momencie bez wcześniejszego informowania Wykonawcy.

**Zamawiający dopuszcza posiadanie przez Systemem funkcjonalności, które nie są wymagane przez Zamawiającego, lecz mogą stanowić dodatkową funkcjonalność rozwiązania ocenianą przez Zamawiającego dla każdej z poniższych funkcjonalności opcjonalnych niezależnie:**

* + - 1. Aplikacja Mobilna pozwalająca na zdalne administrowanie Systemem dostępna na systemach iOS oraz Android
      2. Centralne raportowanie (zbiorcze tworzenie raportów) z wszystkich instancji Systemu w zakresie zgromadzonych danych
      3. Wbudowane narzędzie do migracji profili użytkowników pomiędzy urządzeniami końcowymi (stacjami roboczymi; urządzeniami mobilnymi)

**VIII Lokalizacje fizyczne Zamawiającego w których będzie realizowana umowa:**

1. ……………………………………………….
2. ……………………………………………….
3. ……………………………………………….
4. ……………………………………………….
5. ……………………………………………….
6. ……………………………………………….
7. ……………………………………………….
8. ……………………………………………….
9. ……………………………………………….
10. ……………………………………………….
11. ……………………………………………….