BDG-V.2610.33.2019.PS

Załącznik nr 1 do SIWZ

(po zawarciu umowy Załącznik nr 3 do umowy)

Szczegółowy Opis Przedmiotu Zamówienia

I. Przedmiot Zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie Systemu do zarządzania stacjami roboczymi i urządzeniami przenośnymi wraz ze wsparciem technicznym przez okres 12 miesięcy dla Ministerstwa Rozwoju.

Przedmiot zamówienia realizowany będzie w szczególności poprzez:
1. Dostawa licencji oprogramowania Systemu wraz z 12 miesięcznym wsparciem technicznym.
2. Wdrożenie Systemu, instalacja, konfiguracja i uruchomienie produkcyjne w środowisku Zamawiającego,
3. Przeprowadzenie instruktażu z zakresu administracji, obsługi i utrzymania dostarczonego Systemu.

II. Wymagania minimalne dla Systemu

1. Dostarczone licencje oprogramowania Systemu muszą umożliwiać bezterminowe korzystanie z Systemu.
2. Dostarczone licencje oprogramowania Systemu muszą być przeznaczone do użytku w jednostkach rządowych na terenie Rzeczypospolitej Polskiej.
3. Wraz z licencją oprogramowania Systemu musi być zapewnione wsparcie techniczne przez okres 12 miesięcy z możliwością odnowienia na dowolny okres po jego wygaśnięciu.
4. Wsparcie powinno umożliwiać nieodpłatne pobieranie najnowszej wersji oprogramowania w trakcie jego obowiązywania.
5. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu.
6. Dostarczone licencje oprogramowania Systemu musi zapewniać zarządzanie 1200 urządzeniami możliwość równoczesnych sesji dla 5 administratorów.
7. System musi umożliwiać jego instalację na systemie operacyjnym Windows (wersja co najmniej 2012 Server).
8. Interfejs Systemu oraz konfiguracji musi być w całości dostępny z poziomu przeglądarki internetowej (Mozilla 65 lub nowszej, Chrome 70 lub nowszej) bez potrzeby instalacji tzw. grubego klienta.
9. Architektura Systemu musi być agentowa.
10. Architektura Systemu musi dawać możliwość instalacji serwerów dystrybucyjnych w lokalizacjach zdalnych, umożliwiając zarządzanie urządzeniami końcowymi bez konieczności łączenia się z serwerem głównym i nadmiernego obciążania łącza.
11. System powinien wspierać co najmniej bazy danych: PostgreSQL oraz MSSQL.
12. System musi mieć możliwość zarządzania stacjami roboczymi z zainstalowanym systemem operacyjnym: Windows co najmniej w wersjach: 7, 8, 10, Server 2008, 2012, 2016.
13. System musi mieć możliwość zarządzania systemami operacyjnymi:
    - Linux co najmniej w wersjach: Ubuntu 10.04, Red Hat Enterprise Linux 6, CentOS, Fedora 19, Mandriva 2010, Debian 7, Linux Mint 13, OpenSuSE 11, SuSE Enterprise Linux 11,
    - Mac OS w wersjach: 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12, 10.13
14. System musi rozpoznawać stacje robocze w ramach sieci Active Directory oraz Workgroup.
15. System musi umożliwiać instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.
16. System musi posiadać możliwość tworzenia list aplikacji, które będą mogły być otwierane i instalowane przez samego użytkownika z poziomu stacji roboczej, tzw. Portal samoobsługowy.

17. System musi mieć wbudowane funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach, w szczególności musi rozpoznawać sekwencje instalacji.
    Funkcje wdrażania łat powinny obejmować co najmniej oprogramowanie:
    - Systemy operacyjne 7, 8, 10, Server 2008, 2012, 2016.
    - Microsoft Office
    - Google Chrome
    - Opera
    - Skype
    - Mozilla Firefox
    - Adobe Reader
    - Adobe Acrobat
    - Adobe Shockwave Player
    - Adobe Flash Player
    - Java
    - WinRar
18. System musi mieć możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.
19. System musi mieć wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.
20. Architektura Systemu musi umożliwiać zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego jak i za pośrednictwem serwerów sond.
21. System musi mieć wbudowane narzędzia zarządzania zasobami IT, w szczególności musi rozpoznawać komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.
22. System musi posiadać wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz mieć możliwość włączenia opcji nagrywania tych sesji.
23. System musi 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.
24. Konfiguracja polityk dostępu do USB musi umożliwiać blokowanie co najmniej poniższych typów urządzeń, a także mieć 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 oraz dyski wirtualne),
    - 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).
25. System musi posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.
26. System musi mieć rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami.
27. System musi mieć możliwość dodania nowego użytkownika systemu z uwierzytelnianiem lokalnym lub Active Directory.
28. System musi mieć 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 kodu z aplikacji Google Authenticator.
29. System musi dawać możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.
30. System musi umożliwiać dodawanie i rozliczanie licencji aplikacji.

31. System musi umożliwiać wykrywanie zakazanego oprogramowania i uruchamiać działania naprawcze, w tym automatyczne odinstalowanie niepożądanej aplikacji.
32. System musi posiadać możliwość włączenia pomiaru wykorzystania wskazanej aplikacji.
33. System musi mieć możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na ścieżce aplikacji lub wartości hash.
34. System powinien mieć możliwość uruchamiania 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.
35. System powinien umożliwiać generowanie następujących raportów:
    - Raporty Active Directory:
        - aktualnie zalogowani użytkownicy,
        - często zalogowani użytkownicy, rzadko logujący się użytkownicy
        - nieaktywni użytkownicy,
        - historia logowania użytkownika,
        - historia logowania użytkowników na poszczególnych komputerach.
    - Wykorzystania aplikacji w skali całej organizacji.
    - Raporty dotyczące poprawek:
        - Narażone systemy,
        - Narażone poprawki,
        - Obsługiwane poprawki,
        - Brakujące poprawki czekające na zatwierdzenie,
        - Systemy wymagające ponownego uruchomienia
    - Raporty inwentaryzacji
        - Raporty dotyczące sprzętu:
            - Komputery wg systemu operacyjnego,
            - Komputery wg producenta,
            - Komputery wg pamięci,
            - Komputery wg wykorzystania dysku,
            - Komputery wg wieku,
            - Komputery wg typu urządzenia,
            - Zmapowane dyski logiczne
        - Raporty dotyczące oprogramowania
            - Oprogramowanie według producenta
            - Ostatnio zainstalowane oprogramowanie
            - Niedozwolone oprogramowanie
            - Wykorzystanie oprogramowania przez komputer
            - Klucze produktu oprogramowania
            - Komputery z/bez określonego oprogramowania
            - Podsumowanie zasad pomiaru użytkowania oprogramowania
            - Oprogramowanie specyficzne dla użytkownika
        - Raporty dotyczące licencji
            - Zgodność licencji
            - Licencje do odnowienia
        - Raporty dotyczące systemu
            - Użytkownicy grupy systemu
            - Komputery wg usług
            - Udostępnij szczegóły
        - Raporty dotyczące gwarancji
            - Gwarancja niedługo wygaśnie
            - Gwarancja wygasła
            - Niezidentyfikowane komputery
        - Raporty bezpieczeństwa
            - Szczegóły Antivirus
            - Szczegóły Bitlocker
            - Szczegóły Firewall

- Raporty skanowania plików multimedialnych
  - Szczegóły pliku wg kategorii
  - Szczegóły pliku wg rozszerzenia
- Raporty dotyczące USB
  - Raport wykorzystania USB

36. System musi umożliwiać planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres mailowy.
37. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu.
38. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.
39. System musi umożliwiać korzystanie z szablonów definiujących adres IP, nazwę, członkostwo w domenie, ustawienia zgodnie z konfiguracją dla nowych instalacji.
40. System musi umożliwiać kopiowanie plików do folderów, kopiowanie wielu plików i kopiowanie folderów.
41. System musi umożliwiać zarządzanie flotą urządzeń mobilnych typu smartfony i tablety z zainstalowanymi systemami operacyjnymi: Android 4.0 i wyższe, iOS 6 i wyższe.
42. System musi posiadać moduł rozpoznawania i dodawania urządzeń:
    - Wdrożenie Over-the-Air(OTA),
    - Ręczne dodawanie urządzeń,
    - Zbiorcze dodawanie urządzeń z pliku CSV,
    - Uwierzytelnione dodawanie z jednorazowym kodem i/lub poświadczeniami użytkownika AD.
43. System musi posiadać moduł zarządzania profilami:
    - Konfiguracja polis/profili - konfiguracja ustawień polis dostępu do zasobów organizacyjnych,
    - Restrykcje – szyfrowanie urządzenia, ograniczanie użytkowania kamery, youtube, przeglądarki internetowe, itp.,
    - Organizacyjny dostęp - zapewnia dostęp do organizacyjnych zasobów jak mail, Wi-Fi, VPN,
    - Grupy 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 w grupie.
44. System musi posiadać moduł zarządzania zasobami:
    - Pełna informacja o urządzeniu: szczegóły, certyfikaty, zainstalowane aplikacje,
    - Wbudowane, predefiniowane raporty.
45. System musi posiadać moduł zarządzania aplikacjami:
    - Zarządzanie i dystrybucja własnych aplikacji i AppStore,
    - Integracja z programem Apple VPP,
    - Publikacja aplikacji w katalogu aplikacji dla użytkowników na potrzeby samodzielnej instalacji.
46. System musi posiadać moduł zarządzania bezpieczeństwem:
    - Kod dostępu: Wymuszenie kodu w celu blokowania nieautoryzowanego dostępu,
    - Zdalna blokada: W celu uniknięcia niepowołanego użycia utraconego urządzenia
    - Pełne czyszczenie: Usunięcie wszystkich danych z telefonu w celu uniknięcia wycieku danych po kradzieży
    - Organizacyjne czyszczenie: Usunięcie tylko danych organizacyjnych i pozostawienie danych prywatnych - funkcjonalność absolutnie kluczowa w przypadku zarządzania urządzeniami BYOD (Bring Your Own Device) w ramach organizacyjnej floty smartphonów.
47. System musi realizować funkcjonalności:
    - pozwalanie na dystrybucję certyfikatów CA na urządzenia z systemem iOS, przy użyciu profilu certyfikatu,
    - aktualizacja urządzenia z systemem Windows 10, nawet bez instalowania aplikacji MDM w urządzeniach,
    - obsługa trybu Kiosk dla urządzeń z systemem Core Android, z systemem iOS 5.0 lub nowszym,
    - wyszukiwanie aplikacji w kiosku według nazwy aplikacji lub identyfikatora wiązki,
    - konfiguracja konta Android for Work, które zapewnia zaawansowane funkcje zarządzania aplikacjami i funkcje konfiguracyjne,

- konteneryzacja urządzeń z Androidem w wersji 5.0 lub nowszej, używając Androida for Work,
- konfiguracja uprawnień i konfiguracje aplikacji za pomocą Android for Work.
- cicha instalacja aplikacji Sklepu Play przy użyciu Android for Work,
- rejestracja urządzeń mobilnych z systemem Windows 10 z kompilacją Redstone,
- reset urządzenia nawet po wygaśnięciu poświadczeń AD,
- śledzenie i zabezpieczenie utraconych urządzeń przy użyciu trybu utraconego,
- obsługiwanie protokołu Simple Certificate Enrollment Protocol (SCEP) do integracji z urzędem certyfikacji za pomocą SCEP w celu automatyzacji dystrybucji certyfikatów klienta na urządzenia z systemem iOS,
- dystrybucja certyfikatów CA na urządzenia z systemem Android przy użyciu profilu certyfikatu,
- pozwalanie na automatyzację przypisywania użytkowników urządzeniom z funkcją DEP,
- pozwalanie na korzystanie z certyfikatu Enterprise CA,
- pozwalanie na przesyłanie zbiorcze szczegółów APN, co ułatwia dystrybucję zasad APN,
- Pozwalanie na wyświetlanie niestandardowych wiadomości i zapewnianie funkcji połączeń na ekranie blokady zagubionego urządzenia itp. na urządzeniach z Androidem,
- powiadamianie Administratorów pocztą, gdy zarządzanie urządzeniem zostało odwołane przez użytkowników,
- obsługa Trybu kiosku dla urządzeń, które nie obsługują Android for Work.
- obsługa zmiany nazwy urządzenia podczas przekazywania urządzenia.
- łatwe wdrażanie ustawień konfiguracji Online Exchange dla wszystkich użytkowników organizacji w korzystających z konteneryzacji.
- wprowadzenie nazwy punktu dostępowego (APN) dla urządzeń Samsung, aby skonfigurować komunikację opartą na komórkowej transmisji danych na zarządzanych urządzeniach.
- konfiguracja systemu Android for Work bez pakietu G Suite.
- integracja z urzędem certyfikacji za pomocą SCEP, aby zautomatyzować dystrybucję certyfikatów klienta na urządzenia z systemem Windows.
- obsługa zdalnego ponownego uruchamianie urządzeń z systemem Windows 10.
- obsługa i bezproblemowa migracja licencji aplikacji na iOS, gdy typ instalacji aplikacji zmienia się, aby nie wymagać identyfikatora Apple ID.
- obsługa automatycznego usuwania aplikacji/profili po usunięciu urządzenia z grupy
- nawiązanie sesji zdalnej na urządzenia Android.
- obsługa historii lokalizacji. Dzięki temu administratorzy mogą wyświetlać i przechowywać lokalizacje obsługiwane przez urządzenie w określonym przedziale czasu.
- wyszukiwanie urządzeń za pomocą numeru telefonu urządzenia.
- import certyfikatów SSL z rozszerzeniami takimi jak .jks i .keystore.
- dystrybucja certyfikatów CA na urządzenia Windows oraz polityka certyfikatów.
- filtr zawartości WWW musi być obsługiwany dla wszystkich dostępnych przeglądarek na urządzeniach z systemem iOS,
- wsparcie dla zarządzania komputerami przenośnymi z systemem Windows 10, komputerami stacjonarnymi i tabletami Surface Pro.
- wsparcie automatycznej instalacji aplikacji Android z obsługą kiosku, jeśli aplikacje nie są obecne na urządzeniu.
- zarządzanie aplikacją Apple Classroom, na urządzenia z systemem iOS 11 i nowszym.
- obsługa zdalną na urządzeniach z systemem iOS,
- zarządzanie treścią, aby zdalnie dystrybuować dokumenty do zarządzanych urządzeń OTA,
- rejestracja Android Zero Touch, aby zdalnie zarejestrować flotę urządzeń, przy aktywacji urządzenia bez interwencji użytkownika,
- obsługa Windows 10 Admin Subsrollment, aby bezproblemowo zarejestrować wiele laptopów, komputerów stacjonarnych i powierzchniowych Windows 10 bez interwencji użytkownika,
- automatyczna instalacja aplikacji, która ma być obsługiwana w trybie Kiosk na urządzeniach z systemem iOS,
- obsługa integracji z Business Store.
- integracja z wieloma kontami DEP.
- obsługa wstępnego definiowania podstawowych ustawień aplikacji Windows przy użyciu konfiguracji aplikacji,

- obsługa urządzenia grupującego różne platformy w jedną grupę, co ułatwia powiązanie polityk.
- możliwość jednym kliknięciem: dystrybuować aplikacje, profile i dokumenty do grup / urządzeń.
- skonfigurowanie zasad dotyczących kodów dostępu dla techników logujących się do serwera MDM.
- udostępnianie aplikacji Home and Photo Booth, pod Kioskiem na urządzeniach z iOS
- tworzenie ról ze wstępnie zdefiniowanymi uprawnieniami do zarządzania niektórymi zarządzanymi grupami urządzeń.
- zarządzanie aktualizacjami systemu operacyjnego w celu zautomatyzowania i zaplanowania aktualizacji systemu operacyjnego na urządzeniach z systemem iOS i Android
- obsługa integracji z produktem Business Store.
- rejestrowanie urządzenia za pomocą konta Azure w MDM Cloud.
- przeglądanie/pobieranie listy urządzeń kwalifikujących się do programu Apple Free Repair.
- skonfigurowanie adresu URL strony głównej przeglądarki dla urządzeń z systemem Windows.
- przesyłanie wewnętrzne aplikacje korporacyjne o rozmiarze do 1,5 GB
- tworzenie ról umożliwiając technikom zdalne sterowanie urządzeniami przenośnymi.
- Administratorzy mogą wybrać strefę czasową do ustawienia na zarządzanych urządzeniach mobilnych,
- obsługa Google Play Protect dla urządzeń z systemem Android,
- nowoczesne zarządzanie urządzeniami Mac i Apple TV. pozwala instalować aplikacje Mac Store w trybie cichym na MacBookach, blokowanie Apple TV w trybie Kiosk i uruchamianie na żądanie polecenia bezpieczeństwa, takie jak zdalna blokada i zdalne czyszczenie,
- konfigurowanie zasad i rozpowszechnianie aplikacji na Chromebookach Google, używając MDM. Aplikacja pozwala zablokować urządzenia z systemem Windows 10 w jednej aplikacji, używając trybu Kiosk,
- daje możliwość zbiorczo zarejestrować wiele urządzeń z systemem Windows 10, a także ułatwić proces aktywacji urządzenia, korzystając z rejestracji Windows Azure/AutoPilot.
- pozwala wyświetlić listę użytkowników w MDM i powiązane z nimi urządzenia w widoku dedykowanym.
- w ramach zasad ograniczeń zabezpieczeń pozwala wymuszać na użytkownikach uwierzytelnianie przy użyciu identyfikatora FaceID, aby umożliwić programowi Safari i innym aplikacjom automatyczne uzupełnianie haseł i danych karty kredytowej,
- system w ramach zasad ograniczeń zabezpieczeń pozwala zabronić urządzeniom firmowym wykonywania konfiguracji zbliżeniowych dla innych urządzeń, co uniemożliwia takie ustawienia, jak kopiowanie Wi-Fi na niezatwierdzone urządzenia,
- system pozwala poznać szczegóły dotyczące sesji użytkownika oraz zakończenia aktualnie aktywnych sesji,
- system powinien pozwalać na obsługę także VPN dla urządzeń z systemem Android.
- wyświetlanie podstawowych informacji, takich jak IMEI, IMSI, numer telefonu itp., dla laptopów Windows i Surface Pros.
- umożliwienie wyboru pomiędzy domyślnym programem uruchamiającym urządzenia a programem uruchamiającym MDM dla Kiosku na urządzeniach z Androidem.
- umożliwienie skonfigurowania ustawień bezpieczeństwa serwera w celu zapewnienia bezpiecznego zarządzania urządzeniami.
- obsługa uwierzytelniania dwuskładnikowego dla logowania administratora.
- zdalne ponowne uruchamianie urządzeń za pomocą jednego kliknięcia.
- wyświetlanie warunków użytkowania odnoszące się do organizacji,.
- konfiguracja ustawień prywatności urządzenia, określenie rodzaju danych, które można gromadzić, poleceń do wykonania na urządzeniu itp.
- obsługa wielu metod tymczasowego wyłączania Kiosku na urządzeniach z Androidem.

48. System musi posiadać zintegrowany moduł do wdrażania systemów operacyjnych, który umożliwia przechwytywanie obrazu systemu operacyjnego a następnie pozwala wdrożyć go na komputerach przenośnych i stacjonarnych.
49. System musi umożliwiać tworzenie tzw. wzorców (ang. Template) dystrybucji obrazów, które pozwalają na dystrybucję przygotowanego obrazu zgodnie z określonymi zasadami takimi jak:

- Zadania po dystrybucji obrazu/Restart, Zamknięcie systemu,
- Zarządzanie tzw. SID,
- Możliwość nadania nazwy komputera,
- Dodanie komputera do domeny Windows,
- Instalacja dodatkowego oprogramowania

50. System musi posiadać możliwość tworzenia zadań dystrybucji pozwalających na automatyzacje procesu dystrybucji obrazów systemów oraz musi posiadać możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalających na dystrybucję obrazu przy użyciu kodu, lub wybieranych systemów z dostępnej listy komputerów.
51. Import komputerów powinien być możliwy z pliku np. CSV.
52. System musi wspierać następujące metody dystrybucji obrazów:
    - Multicast, Unicast oraz powinna pozwalać na tworzenie harmonogramu tejże dystrybucji.
53. System musi posiadać możliwość przechowywania wcześniej zapisanych obrazów w swoim repozytorium System musi posiadać możliwość przechowywania informacji o sterownikach, a także zapewniać ich dystrybucje w obrazach, System musi posiadać możliwość tworzenia boot'owalnych mediów a także ich edycję:
    - PXE
    - ISO
    - USB
54. System musi posiadać repozytorium możliwych do zainstalowania aplikacji po procesie dystrybucji obrazu a także musi posiadać możliwość edycji tychże aplikacji.
55. System musi posiadać możliwość generowania logów a także wyświetlać listę statusów i wykonanych akcji.

III. Wdrożenie Systemu

W ramach wdrożenia Systemu Wykonawca zrealizuje:

1. Instalację i konfigurację dostarczonych licencji oprogramowania Systemu w środowisku Zamawiającego zgodnie z zaleceniami producenta oprogramowania i najlepszymi praktykami.
2. Uruchomienie Systemu.
3. Sprawdzenie poprawności funkcjonowania Systemu, a w szczególności:
    a) konsoli zarządzającej,
    b) automatycznej inwentaryzacji zasobów sprzętowych i oprogramowania,
    c) zdalnego dostępu,
    d) aktywności użytkowników,
    e) statystyk z użytkowania aplikacji,
    f) przypisywania licencji
    g) przygotowanie raportu zabronionych aplikacji,
    h) weryfikacji separacji dostępu do obiektów dla poszczególnych administratorów/operatorów,
    i) przeprowadzenie backupu i odtwarzania systemu,
    j) przeprowadzenie testów penetracyjnych obejmujących skanowanie portów, badanie podatności systemu operacyjnego oraz aplikacji na znane luki w bezpieczeństwie, weryfikację poprawności działania firewalla, ocenę poprawności reakcji systemu zabezpieczeń na wykonywane ataki DDOS, w tym co najmniej:
        - flooding,
        - smurfing,
        - IP fragmentation,
        - syn flood,
        - nuking.
4. Opracowanie dokumentacji powykonawczej obejmującej co najmniej:
    a) schematy funkcjonalne rozwiązania,
    b) opis architektury logicznej,
    c) opis komponentów aplikacyjnych,
    d) opis wykonanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów systemu,
    e) listingi krytycznych plików konfiguracyjnych,
    f) skryptów instalacyjnych,

g) konfigurację firewalli,
h) procedury eksploatacji, w tym instalacji, reinstalacji, aktualizacji systemu, konfiguracji systemu dla nowych jednostek,
i) procedury backupu i odtwarzania (w tym disaster recovery),
j) zalecenia bezpieczeństwa w zakresie bezpiecznej eksploatacji systemu, kontroli i monitorowania dostępu, w tym prób naruszenia zasad bezpieczeństwa.

IV. Instruktaż

Wykonawca po wykonaniu wdrożenia dostarczonego Systemu przeprowadzi zaawansowany instruktaż dla minimum 5 administratorów wskazanych przez Zamawiającego.

1. Zakres tematyczny instruktażu powinien obejmować w szczególności:
   - niezbędne funkcjonalności zapewniające sprawne zarządzanie środowiskiem skonfigurowanym do obsługi wielu jednostek,
   - tworzenie własnych raportów,
   - dostęp do bazy danych systemu, w tym budowania zaawansowanych zapytań bezpośrednio do bazy systemu,
   - sposób analizy logów, debbugowanie systemu,
   - procedury bezpieczeństwa i zasady bezpiecznej eksploatacji.
2. Instruktaż musi zostać przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż (15)* dni od daty zawarcia umowy), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa. Przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/program instruktażu.
3. Zamawiający będzie miał prawo do weryfikacji zakresu tematycznego/programu instruktaży i zgłoszenia ew. dodatkowego zakresu tematycznego.
4. Zapewnienie aby instruktaż przeprowadzony został przez wykwalifikowaną kadrę szkoleniową posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia.

VII Wsparcie techniczne

W ramach realizacji przedmiotu zamówienia, Wykonawca dla dostarczonego Systemu będzie świadczył usługi wsparcia technicznego na rzecz Zamawiającego, w szczególności:

1. zapewnienie ciągłości działania systemu,
2. wsparcie w zakresie wykrywania przyczyn awarii i niestabilnej pracy,
3. obsługi błędów wszystkich elementów wdrożonego systemu,
4. aktualizacji oprogramowania dostarczonego w ramach Umowy do najnowszej dostępnej i stabilnej wersji,
5. optymalizacji systemu,
6. przeprowadzania nieograniczonych konsultacji technicznych,
7. wszelkie zmiany w systemie skutkujące niedostępnością lub wpływające na jego stabilność lub wydajność wymagają uprzedniej zgody Zamawiającego.
8. Zgłoszenia w ramach wsparcia technicznego dokonywane będą przez Zamawiającego telefonicznie lub za pośrednictwem poczty e-mail, z terminem realizacji do …….. dni roboczych dla błędów oraz z terminem realizacji …….. dni roboczych dla awarii/wad, gdzie błąd to sytuacja polegająca na nieprawidłowym, funkcjonowaniu systemu, w tym niezgodnie z dokumentacją, skutkująca:
   - niedostępnością systemu,
   - niespójnością danych,
   - zawieszaniem się systemu,
   - niedostępnością funkcjonalności określonych w dokumentacji;

*) *Termin realizacji zostanie zmodyfikowany w zależności od terminu wskazanego przez Wykonawcę w ofercie*