**Nr sprawy: O.252.10.2025**

**Załącznik nr 1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dotyczy: postępowania realizowanego w trybie podstawowym wariant I np. Dostawa systemu do zarządzania urządzeniami mobilnymi wraz z wdrożeniem, zagwarantowaniem wsparcia technicznego producenta Systemu i przeprowadzeniem warsztatów powdrożeniowych.**

1. **Przedmiot zamówienia**
	1. Dostawa, uruchomienie i wdrożenie systemu do zarządzania urządzeniami mobilnymi MDM (Mobile Device Management), zwanego dalej Systemem MDM, w infrastrukturze Zamawiającego **dla minimum 280 urządzeń**;
	2. Dostarczenie wszystkich niezbędnych licencji na oprogramowanie (również firm trzecich – jeśli są niezbędne do prawidłowego funkcjonowania systemu MDM) wymaganych do uruchomienia i wdrożenia Systemu MDM zgodnie z wymogami Zamawiającego;
	3. Przygotowanie dokumentacji powykonawczej wdrożonego Systemu MDM;
	4. Przeprowadzenie warsztatów powdrożeniowych dla nie więcej niż 5 osób wskazanych przez Zamawiającego w zakresie obsługi, konfiguracji oraz administrowania Systemem MDM;
	5. Dostarczenie bezterminowych licencji na dołączenie co najmniej 280 urządzeń mobilnych do Systemu MDM. Licencje nie mogą być przypisane do konkretnego urządzenia mobilnego lub użytkownika;
	6. Licencje muszą być nowe, nie używane;
	7. Świadczenie usługi serwisu gwarancyjnego wraz ze wsparciem technicznym dla Systemu MDM przez okres 12 miesięcy.
2. **Wdrożenie systemu musi objąć co najmniej:**
	1. Dostarczenie wstępnego projektu dla Zamawiającego (na 5 dni roboczych przed przystąpieniem do instalacji i konfiguracji) – obejmującego co najmniej:
		* Ilość i parametry wirtualnych maszyn potrzebnych dla sprawnego działania systemu dla wskazanej ilości zarządzanych urządzeń;
		* Wszystkie niezbędne informacje odnośnie wymagań sieciowych dla Systemu. Opis konfiguracji sieciowej opartej na ruchu przychodzącym/wychodzącym na poszczególnych portach;
	2. Instalację i konfigurację systemu we wskazanym środowisku;
	3. Integrację produktu ze środowiskiem LDAP/Active Directory Zamawiającego;
	4. Stworzenie pierwszego sklepu dla urządzeń Android, iOS/iPadOS(obejmującego zamknięty katalog aplikacji: Microsoft Word, Microsoft Excel, Microsoft Powerpoint, Outlook, Microsoft Teams, Zoom);
	5. Integrację produktu z systemem Apple Business Manager oraz Android Enterprise.
3. **Zakres warsztatów powinien objąć co najmniej:**
	1. Omówienie funkcji wdrażanego Systemu;
	2. Tworzenie własnych sklepów z aplikacjami dla systemów Android, IOS/ipadOS/Windows;
	3. Tworzenie polityk dla urządzeń Android/IOS/ipadOS;
	4. Zdalne wsparcie dla użytkowników Android;
	5. Czas trwania warsztatów: co najmniej 30 godzin, podzielonych na min. 4 spotkania;
	6. Zajęcia muszą być przeprowadzone w języku polskim;
	7. Warsztaty muszą się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00;
	8. Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim;
	9. Uczestnicy dostaną imienne certyfikaty potwierdzające uczestnictwo w warsztatach.
4. **Wymagania odnośnie architektury**
	1. System powinien zostać dostarczony w formie maszyny wirtualnej, dla środowiska on-premise, zgodnej ze środowiskiem wirtualizacyjnym Zamawiającego - VMware vSphere (lub zainstalowany na stworzonych w tym celu maszynach wirtualnych Zamawiającego (zgodnie z projektem stworzonym w punkcie 2.1);
	2. Zamawiający wyklucza dostarczenie Systemu MDM w formie usługi chmurowej oraz osobnego urządzenia;
	3. Konsola Systemu MDM musi być dostępna z poziomu przeglądarki;
	4. Konsola Systemu MDM musi być dostępna w języku polskim;
	5. Konsola Systemu MDM musi być dostępna w jasny i ciemnym motywie kolorystycznym;
	6. Konsola Systemu MDM musi oferować możliwość wymuszenia pojedynczej sesji logowania na koncie administratora;
	7. Konsola Systemu MDM musi rejestrować udane i nieudane próby logowania na koncie administratora;
	8. Rozwiązanie MDM musi oferować obsługę zmiennych globalnych służących do parametryzacji i personalizacji konfiguracji zarządzanej kierowanej w urządzeń;
	9. Rozwiązanie MDM musi oferować obsługę zmiennych globalnych na poziomie użytkownika, urządzenia, kart SIM oraz certyfikatów;
	10. Rozwiązanie MDM musi oferować wbudowane centrum certyfikacji;
	11. Rozwiązanie MDM musi oferować wbudowany VPN;
	12. Rozwiązanie MDM musi oferować wsparcie dla protokołu SCEP;
	13. Rozwiązanie MDM musi oferować wsparcie dla Android Enterprise;
	14. Rozwiązanie MDM musi oferować wsparcie dla Apple Business Manager;
	15. Rozwiązanie MDM musi oferować wsparcie dla Apps and Books (dawniej Apple VPP);
	16. Rozwiązanie MDM musi oferować wsparcie dla Knox Mobile Enrollment;
	17. Rozwiązanie MDM musi oferować wsparcie dla Android zero-touch Enrollment;
	18. Rozwiązanie MDM musi oferować narzędzie do backupu serwera;
	19. Rozwiązanie MDM musi oferować wsparcie dla Active Directory;
	20. Rozwiązanie MDM musi oferować wsparcie dla LDAP;
	21. Rozwiązanie MDM musi ofertować automatyczny onboarding i offboarding użytkowników;
	22. Rozwiązanie MDM musi oferować wsparcie dla Azure Active Directory;
	23. Rozwiązanie MDM musi oferować logowanie jednokrotne (SSO) przy pomocy Azure Active Directory;
	24. Rozwiązanie MDM musi oferować automatyczną synchronizację użytkowników z usług katalogowych AD/LDAP/AAD;
	25. Rozwiązanie MDM musi oferować wsparcie dla Microsoft Exchange;
	26. Rozwiązanie MDM musi oferować wsparcie dla protokołów ActiveSync, POP, IMAP;
	27. Rozwiązanie MDM musi oferować mechanizm zabezpieczający dostęp do poczty elektronicznej weryfikowany na podstawie dotykowego składnika np. certyfikat użytkownika;
	28. Rozwiązanie MDM musi oferować dodawanie aplikacji z pliku (aplikacje typu in-house);
	29. Rozwiązanie MDM musi oferować import aplikacji ze sklepu z aplikacjami Google Play;
	30. Rozwiązanie MDM musi oferować import aplikacji ze sklepu z aplikacjami iTunes;
	31. Rozwiązanie MDM musi oferować dodawanie aplikacji z zewnętrznego zasobu;
	32. Rozwiązanie MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji Android;
	33. Rozwiązanie MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji iOS;
	34. Rozwiązanie MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji typu in-house;
	35. Rozwiązanie MDM musi oferować konfiguracje ACL dla konsoli;
	36. Rozwiązanie MDM musi oferować możliwość zmiany motywów konsoli (główny kolor, logo, favicon);
	37. Rozwiązanie MDM musi oferować uwierzytelnianie dwuskładnikowe dla użytkowników konsoli;
	38. Rozwiązanie MDM musi oferować wbudowany audyt integralności danych i bezpieczeństwa serwera;
	39. Rozwiązanie MDM musi obsługiwać wysyłanie niestandardowych profili konfiguracyjnych do urządzeń iOS;
	40. Rozwiązanie MDM musi obsługiwać wysyłanie niestandardowych poleceń do urządzeń iOS;
	41. Rozwiązanie MDM musi gromadzić logi audytowe aplikacji;
	42. Rozwiązanie MDM musi gromadzić informacje na temat wykonanych akcji wewnątrz Systemu;
	43. Rozwiązanie MDM musi gromadzić logi sieciowe aplikacji;
	44. Rozwiązanie MDM musi oferować konfigurowalną lokalizacje Google Play i App Store;
	45. Rozwiązanie MDM musi oferować możliwość włączenia dostępu do całej treści zarządzanego sklepu Google Play bez konieczności logowania oraz nałożenie białej lub czarnej listy aplikacji;
	46. Rozwiązanie MDM musi oferować możliwość przejęcia kontroli zdalnej nad urządzeniem;
	47. Rozwiązanie MDM musi umożliwiać wykorzystanie klawiatury komputera do wpisywania tekstu na urządzeniu, podczas przejmowania kontroli zdalnej nad urządzeniem;
	48. Rozwiązanie MDM musi oferować automatyczne i manualne aktualizacje serwera;
	49. Rozwiązanie MDM musi oferować możliwość przypisywania konfiguracji w sposób dynamiczny np. Na podstawie parametrów urządzenia.
5. **Wymagania techniczne dotyczące obsługiwanych przez rozwiązanie MDM urządzeń:**
	1. Urządzenia przenośne pracujące pod kontrolą Systemu operacyjnego Apple iOS 13 lub wyższe, iPadOS, macOS;
	2. Urządzenia przenośne pracujące pod kontrolą Systemu operacyjnego Google Android 8.0 lub wyższe;
	3. Urządzenia z systemem Windows od wersji 10/11 Pro;
	4. MacOS 11 lub wyższe.
6. **Rozwiązanie MDM musi oferować pobieranie informacji o zarządzanych urządzeniach co najmniej w zakresie:**
	1. Udostępnianie informacji o producencie urządzenia;
	2. Udostępnianie informacji o modelu urządzenia;
	3. Informacja o systemie operacyjnym urządzenia;
	4. Informacja o stanie baterii urządzenia;
	5. Informacja o pamięci wewnętrznej urządzenia;
	6. Informacja o pamięci RAM urządzenia;
	7. Informacja o procesorze urządzenia;
	8. Informacja o operatorze używanych kart SIM urządzenia;
	9. Informacja o języku urządzenia;
	10. Informacja o szyfrowaniu danych na urządzeniu;
	11. Informacja o IP sieci komórkowej urządzenia;
	12. Informacja o IP sieci Wi-Fi urządzenia;
	13. Informacja o adresie MAC sieci Wi-Fi urządzenia;
	14. Informacja o SSID podłączonej sieci Wi-Fi urządzenia;
	15. Informacja o ICCID używanych kart SIM urządzenia;
	16. Informacja o numerze telefonu karty SIM urządzenia;
	17. Informacja o IMEI gniazd kart SIM urządzenia;
	18. Informacja o numerze seryjnym urządzenia;
	19. Informacja o ostatnim kontakcie urządzenia z serwerem;
	20. Informacja o wykorzystaniu karty SD urządzenia;
	21. Informacja o dostępności aktualizacji Systemu operacyjnego urządzenia;
	22. Informacja o aplikacjach na urządzeniu wraz z wersją aplikacji;
	23. Możliwość wykonania raportu wykorzystania pamięci urządzenia;
	24. Możliwość wykonania raportu wykorzystania danych mobilnych na urządzeniu;
	25. Możliwość wykonania raportu wykorzystania danych przez Wi-Fi na urządzeniu;
	26. Możliwość wykonania raportu wykorzystania aplikacji na urządzeniu.
7. **Rozwiązanie MDM musi oferować funkcjonalności związane z konfiguracją urządzeń w zakresie co najmniej:**
	1. Możliwość resetu hasła;
	2. Możliwość zmiany hasła przez administratora;
	3. Możliwość przywrócenia urządzeń do ustawień fabrycznych;
	4. Możliwość usunięcia danych służbowych z urządzeń;
	5. Możliwość zablokowania ekranu urządzenia;
	6. Możliwość wysłania notyfikacji;
	7. Możliwość restartu urządzenia;
	8. Możliwość eksportu SMS;
	9. Możliwość eksportu kontaktów;
	10. Możliwość eksportu dziennika połączeń;
	11. Możliwość eksportu logów audytowych z urządzenia;
	12. Możliwość lokalizacji urządzeń na żądanie;
	13. Możliwość lokalizacji urządzeń w interwałach czasowych;
	14. Możliwość lokalizacji urządzeń w ruchu;
	15. Możliwość zbierania historia lokalizacji urządzeń;
	16. Możliwość filtrowania urządzeń po ich lokalizacji;
	17. Możliwość zablokowania i odblokowania aplikacji
	18. Możliwość uruchomienia aplikacji na urządzeniu;
	19. Możliwość zarządzanej konfiguracji dla aplikacji ze sklepu;
	20. Możliwość zarządzanej konfiguracji dla aplikacji z pliku;
	21. Możliwość wysłania konfiguracji aplikacji na urządzenia;
	22. Możliwość usunięcie aplikacji z urządzenia;
	23. Możliwość backupu SMS i MMS;
	24. Możliwość backupu kontaktów;
	25. Możliwość backupu dziennika połączeń;
	26. Możliwość instalacji aplikacji ze sklepu oraz z pliku;
	27. Możliwość cichej instalacji aplikacji;
	28. Możliwość instalacji skonfigurowanych aplikacji;
	29. Możliwość opóźnienia instalacji aplikacji ze sklepu Play;
	30. Możliwość zarządzania uprawnieniami aplikacji;
	31. Możliwość uruchomienia służbowego sklepu z aplikacjami;
	32. Możliwość włączenia Activation Lock;
	33. Możliwość wyłączenia Activation Lock;
	34. Możliwość dostarczenia konfiguracji ActiveSync;
	35. Możliwość dostarczenia konfiguracji IMAP/POP;
	36. Możliwość konfiguracji Wi-Fi;
	37. Możliwość konfiguracji Enterprise Wi-Fi;
	38. Możliwość konfiguracji SCEP;
	39. Możliwość dostarczenia certyfikatu na urządzenie;
	40. Możliwość konfiguracji VPN w tym VPN per aplikacja;
	41. Możliwość dostarczenia dokumentów służbowych;
	42. Możliwość konfiguracji tapety;
	43. Możliwość dostarczenia konfiguracji APN;
	44. Możliwość użycia biometrii do odblokowania urządzenia;
	45. Możliwość zablokowania Bluetooth;
	46. Możliwość zablokowania połączeń wychodzących;
	47. Możliwość zablokowania SMS;
	48. Możliwość zablokowania transferu plików przez USB;
	49. Możliwość ustawiania metod wprowadzania danych;
	50. Możliwość zarządzania usługami lokalizacji;
	51. Możliwość zablokowania zrzutów ekranu;
	52. Możliwość zablokowania opcji deweloperskich;
	53. Możliwość zablokowania trybu awaryjnego;
	54. Możliwość zablokowania dodawania nowych kont Google;
	55. Możliwość zablokowania Smart Lock;
	56. Możliwość zablokowania OTG przez USB;
	57. Możliwość zablokowania mikrofonu;
	58. Możliwość zablokowania zmian tapety;
	59. Możliwość zablokowania FaceTime;
	60. Możliwość zablokowania AirDrop;
	61. Możliwość zablokowania iMessage;
	62. Możliwość zablokowania usług Apple Music;
	63. Możliwość zablokowania usługi radio;
	64. Możliwość zablokowania Siri;
	65. Możliwość zablokowania iBooks;
	66. Możliwość zablokowania zakupów w aplikacji;
	67. Możliwość zablokowania iCloud backup;
	68. Możliwość zablokowania Keychain w iCloud;
	69. Możliwość zablokowania udostępniania zdjęć z iCloud;
	70. Możliwość zablokowania My Photo Stream;
	71. Możliwość zablokowania modyfikowania kont;
	72. Możliwość zablokowania Handoff
	73. Możliwość zablokowania parowania Apple Watch;
	74. Możliwość zablokowania klawiatury predykcyjnej;
	75. Możliwość zablokowania skrótów klawiszowych;
	76. Możliwość zablokowania autokorekty;
	77. Możliwość zablokowania sprawdzania pisowni;
	78. Możliwość zablokowania AirPrint;
	79. Możliwość zablokowania dyktowania;
	80. Możliwość zablokowania modyfikacji eSIM;
	81. Możliwość zablokowania autouzupełniania haseł;
	82. Możliwość wymuszenia korzystania z Wi-Fi;
	83. Możliwość zablokowania iTunes;
	84. Możliwość zablokowania News;
	85. Możliwość zablokowania Podcasts;
	86. Możliwość zablokowania Game Center;
	87. Możliwość zablokowania Safari;
	88. Możliwość konfiguracji Safari;
	89. Możliwość zablokowania App Store;
	90. Możliwość zablokowania Find My Device;
	91. Możliwość zablokowania Find My Friends;
	92. Możliwość filtrowania treści w Safari;
	93. Możliwość SIM PINNING(ochrona przed użyciem służbowej karty SIM w innym urządzeniu);
	94. Możliwość wykrywania i reagowania na zmiany konfiguracji gateway, proxy, dns;
	95. Możliwość wykrywania i reagowania na włączone opcje developerskie.