„Zakup smartfonów wraz z systemem zarządzania ”

Zamawiający informuje, iż jeśli w poniższych opisach występują: nazwy lub symbol konkretnego producenta, model, typ produktu, czy nazwy z konkretnego katalogu należy to traktować jedynie jako pomoc (model wzorcowy) w opisie przedmiotu zamówienia. W każdym przypadku Zamawiający dopuszcza produkty równoważne pod względem konstrukcji, materiałów, parametrów, wymagań technicznych oraz funkcjonalnych.

Wyjaśnienia:

Bramka SEG (Secure Email Gateway) – dodatkowa warstwa bezpieczeństwa (model proxy) pomiędzy infrastrukturą firmowej poczty e-mail i urządzeniami użytkowników końcowych. Za pomocą SEG możliwe jest wymuszanie zasady kontroli dostępu do poczty e-mail, takie jak wymaganie szyfrowania urządzenia, blokowanie zagrożonych urządzeń, wdrażanie lub odwołanie certyfikatów, jak również wykrywanie i blokowanie urządzeń niezarządzanych. Model proxy umożliwia także zabezpieczanie załączników poczty e-mail poprzez wymaganie otwierania załączników tylko w zatwierdzonej aplikacji.

MDM (Mobile Device Management) – oprogramowanie służące do zdalnego zarządzania urządzeniami przenośnymi pracowników. Systemy MDM przeznaczone są przede wszystkim do zarządzania urządzeniami przenośnymi obsługiwanymi przez różne systemy operacyjne, operatorów i firmy oraz zabezpieczania tych urządzeń. Ważną cechą tego typu oprogramowania jest również możliwość integrowania urządzeń mobilnych z infrastrukturą sieciową przedsiębiorstwa oraz zdalna konfiguracja.

VPN (Virtual Private Network, Wirtualna Sieć Prywatna) – odseparowana sieć, w ramach której zapewniona jest komunikacja między grupą lokalizacji lub urządzeń. Granice VPN określone są przez politykę bezpieczeństwa i administracyjną, ustaloną przez użytkownika VPN.

1. Wymagania Ogólne.

Przedmiotem dialogu technicznego jest zapoznanie się z funkcjonalnością systemu zarządzania urządzeniami mobilnymi.
Zamawiający w ramach projektu zamierza zakupić 1120 sztuk urządzeń mobilnych typu smartfon wraz z systemem zarządzania MDM.
Świadczenie usługi powinno obejmować sprzedaż i dostarczenie do siedziby Zamawiającego fabrycznie nowych smartfonów wraz z odpowiednim wyposażeniem (baterie, ładowarki, itd) spełniających wymogi opisane poniżej, zapewnienie gwarancji i serwisu na dostarczone urządzenia oraz dostawę, wdrożenie i konfigurację oprogramowania centralnego MDM na serwerze Zamawiającego. Każdy dostarczony smartfon powinien po włączeniu połączyć się z systemem zarządzania.

2. Wymagania dotyczące smartfonu

- 1120 sztuki o równoważnych lub lepszych parametrach niż:

Ekran:	Ekran o przekątnej od 4.5” do 6”, minimalnej rozdzielczości 800x480 pikseli

Obsługa:	Ekran dotykowy w technologii pojemnościowej z rozpoznawaniem wielu punktów dotyku jednocześnie (multitouch)
Procesor:	Procesor minimum czterordzeniowy o częstotliwości taktowania 1.2 Ghz
Pamięć RAM:	minimum 1,5 GB
Pamięć masowa:	Wbudowana pamięć minimum 8 GB
Porty/złącza:	złącze słuchawkowe Mini Jack, złącze kart microSD do 32GB, złącze Micro USB,
Kamera:	Wbudowana tylna i przednia. Przednia minimum 2 Mpix, tylna minimum 5 Mpix z możliwością nagrywania filmów i robieniem zdjęć, wbudowana lampa błyskowa,
Łączność:	LTE, WCDMA 900/2100 MHz + GSM, wbudowana karta Wi-fi, Wbudowany GPS, bluetooth
Bateria:	wyjmowana o pojemności minimum 2200 mAh
System operacyjny	Android w wersji minimum 4.4 spełniający następujące wymagania: system operacyjny dedykowany do pracy w telefonach typu smartfon z graficznym interfejsem użytkownika w języku polskim. Urządzenie musi posiadać licencję na aplikacje Google Play, wykaz urządzeń posiadających licencję znajduję się pod adresem: https://support.google.com/googleplay/android-developer/answer/6154891?hl=pl&rd=1#K
Wyposażenie dodatkowe	Certyfikat odporności IP67. Ładowarka sieciowa, przewód USB, ładowarka samochodowa, karta pamięci minimum 16 GB, słuchawki, Szkło ochronne 9H, Pokrowiec z klapką na magnes

3. Wymagania dotyczące systemu zarządzania

System powinien umożliwiać zarządzanie urządzeniami mobilnymi na każdym etapie ich wykorzystania w środowisku Policji, począwszy od prekonfiguracji, poprzez zdalną instalację i aktualizację aplikacji, cykliczny backup danych, monitorowanie bezpieczeństwa, aż po zdalne czyszczenie pamięci urządzenia. Oprogramowanie powinno cechować się intuicyjnym interfejsem oraz nieskomplikowaną obsługą.
Dostarczony system powinien mieć następujące cechy:

1. Umożliwiać zarządzanie urządzeniami mobilnymi opartymi o system: Android od wersji 4.0 wzwyż, Windows 10 mobile, iOS 4 wzwyż,
2. Interfejs w języku polskim,
3. Możliwość instalacji na serwerze Zamawiającego,
4. Licencja umożliwiająca korzystanie z jednego urządzenia o nieograniczonej liczbie użytkowników tzw. licencja na urządzenie,
5. Licencja nieograniczona czasowo,

6. Gwarancja bezpłatnych poprawek bezpieczeństwa w wymaganym umową okresie,
7. Dostęp dla administratorów do MDM poprzez stronę WWW,
8. Dostęp do informacji o urządzeniu np.: model urządzenia, nazwa urządzenia, IMEI, ID urządzenia, wersja firmware, producent urządzenia, wersja systemu operacyjnego, adres MAC karty WIFI, adres IP WIFI, adres IP GPRS, ustawienia DNS, stan baterii, ilość wolnego miejsca na dysku/karcie SD, poziom zajętości pamięci,
9. Powinien posiadać funkcje: możliwość wprowadzenia daty zakupu urządzenia, daty wygaśnięcia umowy gwarancyjnej, wprowadzenie szczegółów przeprowadzonych napraw i usług serwisowych,
10. Informacje o zainstalowanym oprogramowaniu, lista aplikacji dozwolonych i zabronionych, wyłączenie sklepu z aplikacjami, włączenie możliwości odblokowania funkcji deweloperskich, zdalna instalacja wymaganych aplikacji w trybie „push", instalacja, aktualizacja i usuwanie aplikacji - możliwość wskazania, którą drogą ma się dokonywać – WLAN czy GSM, zdalne usuwanie wybranego oprogramowania, planowany upgrade oprogramowania + możliwość powiadomień na urządzeniu o konieczności podłączenia urządzenia do sieci LAN celem aktualizacji oprogramowania, możliwość prezentacji i instalacji aplikacji wewnętrznego sklepu Zamawiającego,
11. Karty SIM: możliwość wprowadzenia szczegółów dotyczących umów z operatorem, śledzenie limitów wielkości transmisji danych, daty wygaśnięcia umów, adres IP karty SIM, Numer karty SIM,
12. Monitoring parametrów i alertów – log zdarzeń oraz log przeprowadzonych konfiguracji, identyfikowanie błędów w procesie backupu, aktualizacji
13. Zarządzanie konfiguracją – zdalna instalacja aplikacji firmowych, polityki konfiguracji, blokowanie urządzeń (ograniczony zestaw aplikacji i dostępnych ustawień), brak możliwości odinstalowania aplikacji przez użytkownika końcowego, możliwość konfiguracji urządzeń do działania w trybie jednej wybranej aplikacji, ustawianie harmonogramu przeprowadzanych operacji (m. in. zdalnych aktualizacji), możliwość jednoczesnej konfiguracji wybranej grupy urządzeń, konfiguracja ustawień przeglądarki internetowej w tym strony startowej, listy adresów, uniemożliwienie kopiowania informacji na zewnątrz za pomocą nośników zewnętrznych lub po podłączeniu urządzenia do stacji roboczych.
14. Konfiguracja sieci – konfiguracja połączeń sieciowych, wyłączenie udostępniania internetu, wyłączenie interfejsu WIFI, wyłączenie raportowania hotspotów WIFI, wyłączenie ręcznej konfiguracji profili WIFI, Możliwość konfiguracji VPN
15. Reguły dostępu – możliwość zdefiniowania reguł dostępu i uprawnień dla poszczególnych grup użytkowników - grupowanie urządzeń w systemie MDM w ramach określonych grup, ilość nieudanych logowań do urządzenia/konta użytkownika przed wyczyszczeniem urządzenia, okres bezczynności po jakim urządzenie zablokuje się samodzielnie, funkcja realizująca blokadę przechwytywania ekranu, blokowanie kopiuj&wklej,
16. Zdalne wsparcie - Zdalny dostęp do ekranu i klawiatury dotykowej, zdalna pomoc w przypadku problemów z urządzeniem lub pojawieniem się błędów, rejestrowanie zdalnej pomocy
17. Zdalne/automatyczne działanie – Inicjowanie czyszczenia pamięci urządzenia i zewnętrznych kart pamięci w razie wykrycia zagrożenia, wyłączenie soft resetu, wyłączenie hard resetu, możliwość zdalnego usuwania zawartości pamięci flash oraz oprogramowania urządzenia, selektywne usuwanie danych firmowych z urządzenia
18. Zarządzanie magazynem – wymuszenie szyfrowania pamięci flash urządzenia, wymuszenie szyfrowanie pamięci karty microSD, zablokowanie wymiennych nośników,
19. Bezpieczny i kontrolowany dostęp do poczty LOTUS i kalendarza za pośrednictwem bramki SEG. (obsługa poczty email i kalendarza w dedykowanej na urządzenia mobilne aplikacji)
20. Restrykcje: wyłączenie kamery, bluetooth, WIFI, location, NFC, GPS