



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



DRUK WZP-01.BU

Znak sprawy WOIT.042.03.2023

załącznik nr 1

OPIS PRZEDMIOTU I WARUNKÓW WYKONANIA ZAMÓWIENIA

(zamówienie o wartości mniejszej niż 130 000 zł)

1. Nazwa (i miejsce) zamówienia :

Zakup oprogramowania do zarządzania i zabezpieczania urządzeń mobilnych (Systemu Mobile Device Management) dla Gminy Miasto Zgierz w ramach projektu grantowego „Cyfrowa Gmina”, finansowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT – EU, działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia o numerze POPC.05.01.00-00-0001/21-00”.

Zamawiający:

Gmina Miasto Zgierz
plac Jana Pawła II 16,
95-100 Zgierz
NIP: 732 20 37 248
REGON: 472057721
woj. łódzkie

2. Opis przedmiotu zamówienia :

Kod i nazwa CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego

Przedmiotem zamówienia jest zakup oprogramowania do zarządzania i zabezpieczania urządzeń mobilnych (Systemu Mobile Device Management) dla Gminy Miasto Zgierz.

Wdrożenie oprogramowania ma pozwolić na dokładną konfigurację polityk bezpieczeństwa na urządzeniach mobilnych, pozwalać na wymuszanie zastosowania bezpiecznych haseł, geolokalizację urządzeń,

Lider projektu



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



szyfrowanie oraz zdalne usuwanie danych zgromadzonych na urządzeniach mobilnych typu: smartfon, laptop i tablet.

Oprogramowanie musi stanowić jeden system, w ramach którego możliwa jest kontrola wszystkiego, czego potrzebujemy przy zabezpieczeniu urządzeń mobilnych do pracy zdalnej. Powinno pozwalać na tworzenie profili, zarządzanie ograniczeniami, ustawianie zasad dotyczących PIN i haseł oraz posiadać wiele innych użytecznych funkcji, o których w dalszej części. Umożliwiać wykonywanie działań na jednym urządzeniu mobilnym, ale również pozwalać na operacje masowe na grupach urządzeń o zróżnicowanych systemach operacyjnych. Dodatkowo ma pozwolić na wymuszenie odpowiedniej blokady urządzenia, umożliwić wprowadzenie ograniczenia związanego z korzystaniem z dostępnych sieci Wi-Fi, restrykcji dotyczących dostępności i korzystania z aplikacji, przeglądarek internetowych, aż po możliwość zdalnego wyczyszczenia bądź zablokowania urządzenia w przypadku kradzieży lub zgubienia.

Oprogramowanie musi posiadać co najmniej następujące funkcjonalności:

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Wspierane platformy systemowe	Oprogramowanie (System) musi wspierać następujące platformy dostępne na rynku: iOS, iPadOS, Android, MacOS, Windows.
2.	Wymagania ogólne dla systemu MDM (Mobile Device Management)	1. System powinien mieć możliwość integracji z usługą katalogową Microsoft Active Directory, Open LADP oraz Microsoft Azure Active Directory w zakresie pobierania użytkowników i grup do systemu MDM 2. System musi mieć możliwość obsługi interfejsu w języku polskim oraz angielskim 3. System musi posiadać możliwość obsługi platformy MacOS w zakresie: a) Wyłączenia usług iCloud (Mail, Calendar, Reminder, Address Book, Notes,) b) Wyłączenia udostępniania plików przez iTunes c) Wyłączenia parowania z Apple TV d) Blokadę wykorzystania danych lokalizacyjnych przez wyszukiwarkę 4. System musi pozwalać na blokowanie zainstalowanych oraz niezainstalowanych aplikacji

		5. System musi pozwalać na zabezpieczenie aplikacji hasłem 6. System musi pozwalać na zarządzanie kontem Factory Reset Protection (FRP) 7. System musi mieć możliwość zarządzania aktualizacjami OTA 8. System musi udostępniać możliwość blokowania i odinstalowywania aplikacji 9. System musi obsługiwać generowanie raportów zgodnie z harmonogramem 10. System musi mieć możliwość zarządzania alertami dotyczącymi urządzeń 11. System musi pozwalać na wymuszanie ściągania lokalizacji, oraz ściąganie lokalizacji zgodnie z interwałem czasowym 12. System musi pozwalać na ograniczenie funkcjonalności bazując na określonym okresie czasowym 13. System musi mieć możliwość ustawienia powiadomień na zablokowanym ekranie 14. Systemu musi pozwalać na ograniczenie funkcjonalności bazując na położeniu geograficznym 15. System musi pozwalać na połączenie za pomocą zdalnego pulpitu z urządzeniami końcowymi 16. System musi umożliwiać grupowanie urządzeń 17. System musi pozwalać na monitoring takich danych jak: a) Użycie danych pakietowych b) Treść SMS c) Użycie aplikacji d) Rozmowy głosowe 18. System musi informować administratora o sytuacjach awaryjnych takich jak: a) Zmiana karty SIM b) Zrootowanie urządzenia c) Brak kontaktu z urządzeniem przez określony czas 19. System musi pozwalać na tworzenie białej i czarnej listy aplikacji 20. System musi pozwolić na zdalną instalację aplikacji własnych oraz z oficjalnych sklepów dostępnych na urządzeniach 21. System musi umożliwiać tworzenie sklepu firmowego
--	--	---

		22. System musi pozwalać na tworzenie własnego korporacyjnego sklepu play (android) 23. System musi posiadać możliwość wysyłania wiadomości SMS oraz Push 24. System musi pozwalać na obsługę konfiguracji typu kiosk 25. System musi umożliwiać konfigurację własnego pulpitu na urządzeniach końcowych 26. System musi pozwalać na wymuszenie ustawienia blokady ekranu, w zakresie: a) Wymuszenie rodzaju blokady b) Wymuszenie ilości minimalnych znaków c) Ustawienie historii haseł d) Wymuszenie złożoności hasła 27. System musi pozwolić na zdalną konfigurację poczty Exchange na urządzeniach końcowych 28. System musi pozwolić na tworzenie wielu użytkowników z różnymi dostęпами oraz uprawnieniami 29. System powinien umożliwiać wdrożenie urządzeń metodami: a. Google zero touch b. Apple Business Manager/Device Enrollment Program c. Samsung Knox Mobile Enrollment d. Właściciel urządzenia (Android Enterprise Device Owner) / Profil Praca (Android Enterprise Work Profile) 30. System musi obsługiwać konteneryzację 31. System musi posiadać możliwość zarządzania dostępem aplikacji w kontenerze 32. System musi posiadać możliwość zarządzania urządzeniem w całości z podziałem na strefę konteryzowaną (COPE) 33. System musi mieć możliwość zarządzania certyfikatami 34. System powinien umożliwiać dostęp do API 35. System musi mieć możliwość integracji z innymi systemami zewnętrznymi 36. System musi mieć możliwość obsługiwanie mechanizmów proxy.
--	--	--

		37. System musi umożliwiać możliwość logowania do konsoli www z autoryzacją opartą o protokół SAML. 38. System musi umożliwiać aktualizowanie systemu operacyjnego Android w trybie bez dostępu do sieci Internet dla urządzeń Zebra, Panasonic, M3, Custom, Xplore. 39. System musi umożliwiać konfigurację aplikacji obsługujących Zarządzane Konfiguracje Google (Google Managed Configuration) dla urządzeń z systemem Android bez pośrednictwa serwerów Google. 40. System musi umożliwiać funkcjonalność zdalnego pulpitu (przejęcie kontroli ekranu oraz klawiatury telefonu) przynajmniej dla platformy Android 41. System musi umożliwiać zarządzanie plikami na urządzeniu mobilnym przynajmniej dla platformy Android 42. System musi umożliwiać działanie w środowisku w pełni zamkniętym (bez dostępu do sieci internet, w szczególności do usługodawców typu Google, Amazon itp) 43. System musi umożliwiać odświeżenie informacji o kartach eSIM dla urządzeń co najmniej z systemem iOS, iPadOS
3.	Obsługiwane polityki bezpieczeństwa	System musi pozwalać na obsługę szerokiej gamy polityk jak: 1. Blokada interfejsu Wi-Fi 2. Blokada interfejsu bluetooth 3. Blokada danych pakietowych 4. Blokada danych pakietowych w roamingu 5. Blokada udostępniania interfejsu przez WiFi, USB 6. Blokada VPN przez sieć komórkową 7. Blokada GPS 8. Włączenie i podtrzymanie działania lokalizacji 9. Blokada Aparatu 10. Blokada opcji programisty 11. Blokada nieznanego źródła 12. Blokada debugowania USB 13. Blokada nagrywania głosu w aplikacjach 14. Blokada NFC 15. Blokada karty pamięci 16. Blokada trybu samolotowego 17. Blokada trybu awaryjnego 18. Blokada instalacji aplikacji

		19. Blokada ustawień telefonu 20. Blokada przeglądarki www 21. Blokada tworzenia konta email
4.	Gwarancja/Wsparcie techniczne	Min. 1 rok wsparcia świadczonego przez producenta rozwiązania, obejmującego dostęp do aktualizacji, nowych wersji oprogramowania i pomocy technicznej. Licencja bezterminowa (wieczysta) na używanie oprogramowania. Licencja powinna pozwalać na obsługę co najmniej 150 urządzeń mobilnych (bez dodatkowych opłat). Zamawiający nie dopuszcza licencji subskrypcyjnych.
5.	Konfiguracja/Instalacja	Oprogramowanie musi zostać zainstalowane i skonfigurowane przez Wykonawcę na wskazanym serwerze Zamawiającego (spełniającym wymogi techniczne stawiane przez oprogramowanie) z konfiguracją pozwalającą na jego uruchomienie i optymalne działanie.

3. Opis warunków wykonania zamówienia - warunki szczególne:

- a) Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
- b) O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).
- c) Nie podlegają wykluczeniu z powodu powiązania osobowego lub kapitałowego. W celu uniknięcia konfliktu interesów zamówienia publiczne, z wyjątkiem zamówień sektorowych, udzielane przez beneficjenta niebędącego podmiotem zobowiązanym do stosowania ustawy Prawo zamówień publicznych zgodnie z art.3 ustawy, nie mogą być udzielane podmiotom powiązanym z nim osobowo lub kapitałowo. A nadto, Zamawiający wykluczy Wykonawcę w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.

4. Opis warunków wykonania zamówienia - warunki ogólne

- 1) Zamawiający odrzuci ofertę, w przypadku gdy:
 - a) Wykonawca złoży więcej, niż jedną ofertę,
 - b) oferta nie jest zgodna z dokumentacją postępowania, w szczególności z opisem przedmiotu warunków wykonania zamówienia,
 - c) oferta jest nieważna na podstawie odrębnych przepisów.

- 2) Zamawiający poprawi w ofercie oczywiste omyłki pisarskie i rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek. Oczywistą omyłką pisarską jest łatwy do zauważenia błąd, a "oczywistość" omyłki, rozumianej jako określona niedokładność nasuwa się bez potrzeby przeprowadzania dodatkowych badań, czy też ustaleń. Może to być błąd pisarski, logiczny, przypadkowe przeoczenie lub inna niedokładność, która nasuwa się sama, a przez dokonanie poprawki tej omyłki, właściwy sens oświadczenia pozostaje bez zmian. Oczywistą omyłką rachunkową jest widoczny, niezamierzony błąd rachunkowy, popełniony przez Wykonawcę, który polega na uzyskaniu nieprawidłowego wyniku przeprowadzonego działania arytmetycznego.
- 3) Zamawiający przewiduje możliwość wyjaśniania treści oferty, jak również uzupełniania dokumentów potwierdzających warunki udziału w postępowaniu lub wymagania dotyczące oferowanego przedmiotu zamówienia.
5. Termin realizacji zamówienia: 31 lipca 2023 r.
6. Kryterium oceny ofert.
- Cena netto © - waga 100%.
- Maksymalnie do uzyskania jest 100 pkt. Wykonawca, który zaoferował najniższą cenę netto otrzymuje 100 pkt. Dla pozostałych wykonawców punktacja za to kryterium obliczana będzie wg wzoru:

$$C = \frac{\text{Najniższa cena netto}}{\text{Cena netto w rozpatrywanej ofercie}} \times 100 \text{ pkt.}$$

Zgierz, 13 czerwca 2023 r.

Paweł Stankowski
.....
Sporządził

Robert Chocholski
.....
Naczelnik Wydziału