Tryb COPE łączy pewne elementy modeli BYOD oraz COBO. Urządzenie jest w pełni zarządzane przez firmę, ale dozwolone jest również korzystanie z prywatnych kont Google. Część firmowa znajduje się w odrębnym kontenerze Profilu do Pracy. Twoja organizacja sprawuje jednak kontrolę nad całością urządzenia i może stosować polityki zarówno dotyczące części prywatnej, jak i służbowej.

Dla modelu COPE konieczne będzie odpowiednie skonfigurowanie opcji bezpieczeństwa polityki oraz profilu do pracy. Konfiguracja Profilu do Pracy może być podobna do użytej w modelu BYOD. W celu zapewnienia kontroli nad urządzeniem wdrożone muszą zostać również odpowiednie restrykcje bezpieczeństwa. Bardzo ważne jest również aby poinformować użytkowników o zasadach używania urządzeń do celów prywatnych np. sytuacjach, w których urządzenie może zostać zdalnie wyczyszczone.

Opcje bezpieczeństwa

Przykładem wspomnianej wyżej sytuacji może być rootowanie urządzenia. Taka operacja wpływa na bezpieczeństwo danych, zatem zalecamy zaznaczenie opcji **Czyszczenie urządzenia po wykryciu rootowania** (zakładka Polityka czyszczenia danych). Upewnij się jednak, że użytkownicy wiedzą, że w takiej sytuacji urządzenie zostanie całkowicie wyczyszczone.

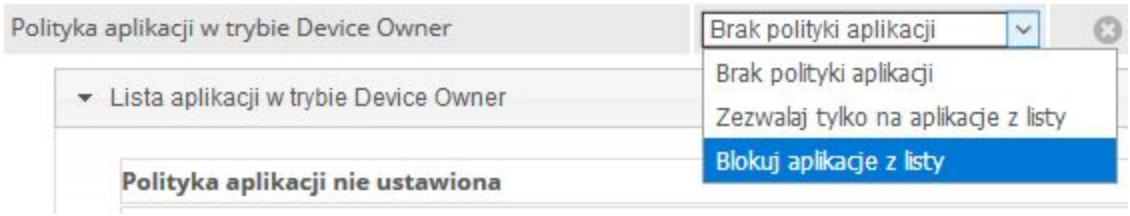
Polityka sieci nie musi być tak restrykcyjna jak w przypadku modelu COBO. Pracownicy będą zapewne korzystać również z domowych sieci WiFi, zatem powinni mieć możliwość ręcznej konfiguracji sieci bezprzewodowej. Możesz jednak rozważyć zablokowanie transferu danych w roamingu (**Blokada danych pakietowych w roamingu**) aby uniknąć generowania dodatkowych kosztów. Z tego samego powodu możesz **zablokować udostępnianie internetu przez WiFi oraz USB.**

W ramach **Polityki sprzętowej** zwróć uwagę na opcje które mogą wpływać na ryzyko złamania zabezpieczeń. Z pewnością należy wybrać **Blokadę przywracania ustawień fabrycznych**, aby użytkownicy nie mogli ręcznie zresetować konfiguracji urządzenia. Wydzielony Profil do Pracy jest niezbędnym elementem funkcjonowania w trybie COPE zatem opcja **Wyłącz możliwość usunięcia profilu służbowego** powinna również być zaznaczona.

Sugerujemy również zaznaczenie opcji **Blokada trybu awaryjnego** oraz **Blokada opcji programisty**. W tych trybach użytkownicy mają dostęp do funkcji, które powinny pozostać jedynie w gestii działu IT.

Polityka aplikacji

Google Play Protect jest użytecznym narzędziem, które skanuje urządzenie chroniąc je przed oprogramowaniem typu malware. Ponieważ użytkownicy mogą instalować na swoich urządzeniach różne aplikacje, ta opcja powinna być uruchomiona aby uniemożliwić działanie podejrzanych aplikacji lub stron WWW. Zalecamy zatem zaznaczenie opcji **Wymuś użycie Google Play Protect** w sekcji **Ograniczenia aplikacji**.
Kolejną opcją, która pozwala na większą kontrolę nad aplikacjami jest tzw. czarna lista. W zakładce **Polityka aplikacji** > **Polityka aplikacji w trybie Device Owner** możesz dodać do listy niechciane aplikacje i z menu powyżej wybrać opcję **Blokuj aplikacje z listy**.



Profil do Pracy Android

W modelu COPE istotne jest aby rozdzielić część prywatną od służbowej, jednakże polityka nie musi być bardzo restrykcyjna, ponieważ obie części znajdują się pod kontrolą organizacji. Sugerujemy poniższe ustawienia:

Ograniczenia profilu służbowego

Wyłącz możliwość modyfikowania kont - w obrębie Profilu do Pracy dostępne powinno być jedynie konto służbowe. Prywatne konto powinno być dostępne poza nim, dzięki czemu unikniemy na przykład użycia niewłaściwego konta pocztowego.

Wyłącz możliwość kopiowania-wklejania w profilu - użytkownik nie będzie mógł przenosić żadnych informacji poza Profil do Pracy za pomocą metody kopiuj-wklej.

Wyłącz możliwość kontrolowania aplikacji - użytkownik nie będzie mógł usuwać, wyłączyć ani modyfikować danych aplikacji.

Uprawnienia aplikacji

Globalny dostęp aplikacji: Zablokuj - użytkownik nie będzie mógł zmieniać uprawnień aplikacji.

W sekcji **Elementy profilu do pracy** wybierz aplikacje, które powinny zostać zainstalowane w kontenerze.

Należy również dodać **Kod blokady profilu służbowego**, w ten sam sposób jak w trybie BYOD. Proces ten opisany jest tutaj, w sekcji *Ustawienia kodu blokady profilu służbowego*.

Po skonfigurowaniu polityki kliknij **Zapisz**.

Polityka jest teraz gotowa do zastosowania na urządzeniach. Administrator będzie posiadał pełną kontrolę nad urządzeniem, natomiast użytkownik będzie mógł dostosować część prywatną do swoich potrzeb. Profil do Pracy będzie wydzielony, a dane firmowe chronione.

Ta konfiguracja jest oczywiście naszą sugestią, jednak powinna określić perspektywę, jak powinien funkcjonować model COPE.