



Bezpieczeństwo urządzeń mobilnych

Zapewnienie właściwych zabezpieczeń urządzeń mobilnych używanych przez pracowników to połączenie możliwości technicznych z odpowiednimi procedurami, które może zwiększyć bezpieczeństwo Twojej organizacji.



Wprowadź polityki i procedury bezpieczeństwa

- 1 POLITYKA BYOD (BRING YOUR OWN DEVICE)**
regulacje dotyczące korzystania z prywatnych urządzeń do celów służbowych.
- 2 POLITYKA MDM (MOBILE DEVICE MANAGEMENT)**
oprogramowanie do zarządzania i zabezpieczania służbowych urządzeń mobilnych pracowników.
- 3 PLAN REAGOWANIA NA INCYDENTY**
procedury zgłaszania utraty lub kradzieży urządzenia.
- 4 ODDZIELNE KONTA**
używanie osobnych kont do celów prywatnych i służbowych.



Zarządzaj urządzeniami pracowników

- 1** Zadbaj o rejestrację i właściwą konfigurację wszystkich urządzeń używanych do celów służbowych.
- 2** Udzielaj uprawnień zgodnie z zakresem obowiązków pracowników.
- 3** Ustaw możliwość zdalnego usunięcia danych z urządzeń.
- 4** Sporządź listę zatwierdzonych aplikacji.
- 5** Zezwalaj na instalację aplikacji wyłącznie z zaufanych źródeł i regularnie je aktualizuj.
- 6** Sporządź politykę bezpiecznych haseł i włącz weryfikację dwuetapową.
- 7** Wymuś zabezpieczenie urządzeń mobilnych za pomocą silnych haseł i PIN-ów lub biometrii.