					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P34S					Tytuł dokumentu: **Polityka urządzeń mobilnych i BYOD**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 5.1, 5.2, 6.1, 6.2, 8	Ogólne wymagania dotyczące SZBI oraz zabezpieczeń dla urządzeń mobilnych i BYOD
ISO/IEC 27002:2022	Zabezpieczenia 5.10–5.13	Szczegółowe zabezpieczenia dla urządzeń mobilnych, BYOD oraz dostępu zdalnego
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Kontrole federalne dotyczące urządzeń, nośników i konfiguracji
RODO	Artykuł 5(1)(f)	Ochrona danych osobowych oraz mobilnych punktów końcowych
NIS2	Artykuł 21(2)(d)	Ochrona urządzeń krytycznych dla działalności, w tym BYOD
DORA	Artykuły 9, 10	Ryzyko ICT i ciągłość działania w odniesieniu do mobilnych punktów końcowych
COBIT 2019	APO13, DSS01, DSS05	Ład IT, operacje oraz zabezpieczenia usług bezpieczeństwa

1. Cel

1.1. Niniejsza polityka określa obowiązkowe wymagania bezpieczeństwa dotyczące korzystania z urządzeń mobilnych, w tym smartfonów, tabletów i laptopów, podczas uzyskiwania dostępu do informacji, systemów lub usług organizacji.

1.2. Reguluje również wykorzystywanie urządzeń prywatnych (BYOD) w celu zapewnienia ochrony danych klientów i danych biznesowych niezależnie od właściciela urządzenia.

1.3. Polityka ustanawia spójne zabezpieczenia dostępu mobilnego, wspiera realizację celów certyfikacji ISO/IEC 27001 oraz zapobiega utracie danych i incydentom bezpieczeństwa wynikającym z utraty, kradzieży lub niewłaściwego użycia mobilnych punktów końcowych.

1.4. Zapewnia stosowanie zabezpieczeń technicznych i proceduralnych w zakresie korzystania z urządzeń mobilnych w organizacjach SME bez dedykowanych zespołów IT, w tym w środowiskach pracy zdalnej oraz przy korzystaniu z usług chmurowych.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich pracowników, kontraktorów, stażystów i dostawców usług, którzy:

2.1.1. Używają urządzenia mobilnego do uzyskiwania dostępu do danych lub systemów organizacji, ich przetwarzania lub przechowywania

2.1.2. Łączą się z usługami organizacji, w tym z pocztą elektroniczną, folderami współdzielonymi, aplikacjami chmurowymi lub systemami wewnętrznymi, za pośrednictwem firmowej sieci VPN

2.2. Polityka obejmuje:

2.2.1. Wszystkie urządzenia mobilne: smartfony, tablety, laptopy (wydane przez organizację lub prywatne w modelu BYOD)

2.2.2. Wszystkie systemy operacyjne (np. iOS, Android, Windows, macOS)

2.2.3. Wszystkie lokalizacje (biuro, dom, praca zdalna, przestrzenie publiczne)

2.3. Polityka obowiązuje we wszystkich środowiskach pracy i musi być stosowana niezależnie od własności urządzenia.

3. Cele

3.1. Zapobieganie utracie danych: zapewnienie, że korzystanie z urządzeń mobilnych nie naraża danych wrażliwych organizacji ani danych klientów na nieuprawniony dostęp, kradzież lub niewłaściwe użycie.

3.2. Określenie jasnych zasad BYOD: ustanowienie egzekwowalnych warunków korzystania z urządzeń prywatnych do celów służbowych z zapewnieniem zabezpieczeń prawnych i technicznych.

3.3. Wsparcie zgodności regulacyjnej: spełnienie wymagań wynikających z ISO/IEC 27001, RODO, NIS2 oraz innych obowiązków prawnych poprzez egzekwowalne praktyki bezpieczeństwa urządzeń mobilnych.

3.4. Ograniczenie ryzyka operacyjnego: zmniejszenie prawdopodobieństwa zakłóceń operacyjnych spowodowanych niewłaściwym użyciem urządzeń mobilnych, ich naruszeniem lub awarią.

3.5. Utrzymanie zaufania klientów: wykazanie klientom i partnerom, że ich dane pozostają chronione nawet wtedy, gdy dostęp do nich odbywa się z urządzeń mobilnych lub prywatnych.

4. Role i odpowiedzialności

4.1. Dyrektor Generalny (GM):

4.1.1. Odpowiada za niniejszą politykę.

4.1.2. Zatwierdza każde wykorzystanie dostępu mobilnego oraz BYOD do systemów organizacji.

4.1.3. Zapewnia, że porozumienia BYOD są podpisywane, przechowywane i monitorowane.

4.1.4. Weryfikuje, czy zewnętrzni dostawcy usług IT stosują wymagane zabezpieczenia dla urządzeń mobilnych.

4.2. Wyznaczony personel lub wsparcie IT:

4.2.1. Wspiera konfigurację, rejestrację i przygotowanie urządzeń mobilnych wykorzystywanych do pracy.

4.2.2. Wdraża kontrole dostępu dotyczące urządzeń mobilnych, ograniczenia aplikacji oraz zasady monitorowania.

4.2.3. Wspiera reagowanie na incydenty dotyczące urządzeń mobilnych (urządzenia utracone, skradzione lub naruszone).

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1. Coroczny przegląd

9.1.1. Dyrektor Generalny (GM) musi dokonywać przeglądu niniejszej polityki co najmniej raz na 12 miesięcy.

9.1.2. Przegląd musi potwierdzać dalsze dostosowanie do wymagań ISO/IEC 27001, rozwoju technologii mobilnych oraz zmian w działalności biznesowej.

9.1.3. Aktualizacje muszą również uwzględniać ostatnie incydenty, wyniki audytów oraz zmiany regulacyjne (np. RODO, NIS2, DORA).

9.2. Zdarzenia uruchamiające przegląd doraźny

9.2.1. Niniejsza polityka musi zostać niezwłocznie zaktualizowana, jeżeli wystąpi którekolwiek z poniższych zdarzeń:

9.2.1.1. Poważny incydent bezpieczeństwa dotyczący urządzeń mobilnych (np. naruszenie związane z utraconym lub przejętym urządzeniem)

9.2.1.2. Zmiana obsługiwanych platform lub narzędzi do zarządzania urządzeniami mobilnymi

9.2.1.3. Zmiana prawna lub regulacyjna wpływająca na używanie urządzeń prywatnych lub ochronę danych

9.2.1.4. Wprowadzenie nowych aplikacji, usług lub narzędzi stron trzecich używanych na urządzeniach mobilnych

9.3. Dokumentowanie zmian

9.3.1. Wszystkie przeglądy i aktualizacje muszą być dokumentowane, w tym data przeglądu, wprowadzone zmiany oraz zatwierdzenie przez GM

9.3.2. Historia wersji musi być przechowywana do celów audytowych

9.4. Komunikacja i dostęp

9.4.1. GM musi zapewnić, że wszyscy użytkownicy (pracownicy, kontraktorzy, strony trzecie) zostaną poinformowani o zmianach

9.4.2. Zaktualizowane wersje muszą być łatwo dostępne, na przykład w folderach współdzielonych lub na platformach wewnętrznych

10. Polityki powiązane i zależności

10.1. Niniejsza polityka stanowi część ogólnego zestawu polityk bezpieczeństwa informacji dla organizacji SME i musi być stosowana łącznie z następującymi dokumentami:

10.1.1. P4S – Polityka kontroli dostępu: określa wymagania dotyczące zarządzania bezpiecznym dostępem do systemów, w tym dostępu realizowanego z urządzeń mobilnych. Wymusza właściwe praktyki zarządzania hasłami i kontrolę sesji.

10.1.2. P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że użytkownicy są szkoleni w zakresie bezpiecznego korzystania z urządzeń mobilnych, zgłaszania incydentów oraz warunków BYOD.

10.1.3. P17S – Polityka ochrony danych i prywatności: ustanawia zgodne z RODO zasady postępowania z danymi osobowymi i danymi organizacji na platformach mobilnych, szczególnie gdy do pracy wykorzystywane są urządzenia prywatne.

10.1.4. P9S – Polityka pracy zdalnej: zapewnia spójność z wymaganiami dotyczącymi korzystania z urządzeń mobilnych podczas pracy poza siedzibą organizacji lub z domu, w tym w zakresie postępowania z urządzeniami i zabezpieczeń dostępu sieciowego.

10.1.5. P30S – Polityka reagowania na incydenty: określa zasady reagowania na incydenty związane z urządzeniami mobilnymi, w tym urządzeniami naruszonymi lub utraconymi.

10.2. Łącznie polityki te tworzą kompletny zestaw zabezpieczeń dla urządzeń mobilnych w organizacjach SME bez dedykowanego personelu IT, zapewniając egzekwowalność, przejrzystość oraz gotowość do certyfikacji.

11. Normy i ramy odniesienia

11.1. Niniejsza polityka wspiera pełne dostosowanie do następujących norm bezpieczeństwa i zgodności:

11.2. ISO/IEC 27001:

11.2.1. Klauzula 5.1 – Przywództwo i zaangażowanie: zapewnia nadzór kierownictwa i rozliczalność w odniesieniu do dostępu mobilnego i BYOD

11.2.2. Klauzula 6.1 – Działania dotyczące ryzyk i szans: wymaga oceny i postępowania z ryzykami bezpieczeństwa urządzeń mobilnych

11.2.3. Klauzula 8.1 – Planowanie i nadzór operacyjny: wymaga spójnych procedur dostępu mobilnego w celu ochrony danych biznesowych

11.3. ISO/IEC 27002:

11.3.1. Zabezpieczenia 5.10 (korzystanie z urządzeń mobilnych), 5.11 (telepraca), 5.12 (dostęp zdalny) i 5.13 (BYOD): zapewniają wytyczne wdrożeniowe dotyczące zarządzania ryzykiem urządzeń w kontekście małej organizacji

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – kontrola dostępu dla urządzeń mobilnych: wymaga ustawień bezpieczeństwa dla autoryzowanego użycia urządzeń mobilnych

11.4.2. AC-20 – korzystanie z systemów zewnętrznych: reguluje ryzyka związane z BYOD i dostępem zdalnym

11.4.3. CM-6 – ustawienia konfiguracji: wymusza bezpieczne ustawienia domyślne i dostosowane na platformach mobilnych

11.4.4. MP-7 – korzystanie z nośników: odnosi się do właściwego użycia i ograniczeń dotyczących nośników przenośnych oraz dostępu do danych

11.5. RODO (2016/679):

11.5.1. Artykuł 5(1)(f) – integralność i poufność: wymaga ochrony danych poprzez odpowiednie zabezpieczenie danych osobowych, szczególnie na platformach mobilnych

11.5.2. Artykuł 32 – bezpieczeństwo przetwarzania: nakłada obowiązek stosowania odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych, do których uzyskuje się dostęp lub które są przechowywane na urządzeniach mobilnych

11.6. Dyrektywa NIS2 (UE 2022/2555):

11.6.1. Artykuł 21(2)(d) – środki bezpieczeństwa urządzeń: wymaga stosowania zabezpieczeń dla sprzętu i oprogramowania wykorzystywanego do uzyskiwania dostępu do systemów krytycznych dla działalności, w tym urządzeń prywatnych

11.7. Rozporządzenie DORA (UE 2022/2554):

11.7.1. Artykuł 9 – ramy zarządzania ryzykiem ICT: wymaga ochrony mobilnych punktów końcowych wykorzystywanych do krytycznej komunikacji biznesowej i usług chmurowych

11.7.2. Artykuł 10 – ciągłość działania ICT: wymusza utrzymanie bezpiecznego dostępu do systemów biznesowych nawet podczas zakłóceń lub pracy zdalnej

11.8. COBIT 2019:

11.8.1. APO13 – zarządzanie bezpieczeństwem: wymaga, aby organizacja stosowała polityki dotyczące urządzeń mobilnych i BYOD zgodnie z ryzykiem organizacji

11.8.2. DSS01 – zarządzanie operacjami: zapewnia techniczne wdrożenie mechanizmów bezpiecznego dostępu

11.8.3. DSS05 – zarządzanie usługami bezpieczeństwa: reguluje udział stron trzecich w utrzymaniu bezpiecznych środowisk mobilnych oraz koordynację reagowania na incydenty