					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P34					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	5.2, 6.1, 7.5, 8	Określa stosowanie środków bezpieczeństwa i wymagań zgodności
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Zawiera szczegółowe środki bezpieczeństwa dotyczące zarządzania urządzeniami mobilnymi
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Obejmuje kontrolę dostępu, dostęp zdalny, konfigurację oraz wymagania bezpieczeństwa dla urządzeń mobilnych
RODO	5(1)(f), 25, 32	Określa obowiązkowe wymagania w zakresie prywatności, szyfrowania danych i bezpieczeństwa przetwarzania
Dyrektywa NIS2	21(2)(d)	Wymaga technicznych i organizacyjnych środków ochrony dla dostępu mobilnego
Rozporządzenie DORA	9, 10	Określa wymagania dotyczące zarządzania ryzykiem ICT i bezpieczeństwa urządzeń mobilnych
COBIT 2019	APO13.02, DSS01.04, BAI09	Obejmuje planowanie bezpieczeństwa informacji, konfigurację aktywów oraz środki bezpieczeństwa dla środowisk mobilnych

1. Cel

1.1 Niniejsza polityka określa wymagania bezpieczeństwa, zgodności i operacyjne dotyczące korzystania z urządzeń mobilnych oraz prywatnych urządzeń wykorzystywanych do celów służbowych (BYOD) podczas uzyskiwania dostępu do systemów, aplikacji lub danych organizacji.

1.2 Jej celem jest zapewnienie poufności, integralności i dostępności (CIA) informacji organizacji, do których uzyskuje się dostęp lub które są przetwarzane za pośrednictwem mobilnych punktów końcowych, w tym smartfonów, tabletów, laptopów i urządzeń hybrydowych.

1.3 Polityka określa również obowiązek stosowania zabezpieczeń technicznych i proceduralnych wymaganych do ograniczania ryzyk, takich jak wyciek danych, nieuprawniony dostęp, utrata lub kradzież urządzenia oraz naruszenie bezpieczeństwa aplikacji mobilnych.

1.4 Niniejsza polityka wspiera zgodność z wymaganiami regulacyjnymi i umownymi, a jednocześnie umożliwia bezpieczne wykonywanie obowiązków w trybie mobilnym przez pracowników, kontrahentów oraz uprawnione strony trzecie.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do całego personelu, w tym pracowników, kontrahentów, stażystów i dostawców usług zewnętrznych, którzy wykorzystują urządzenia mobilne do uzyskiwania dostępu do danych, systemów, aplikacji lub platform komunikacyjnych organizacji.

2.2 Obejmuje ona wszystkie mobilne urządzenia komputerowe, w tym między innymi:

2.2.1 smartfony i tablety (iOS, Android itp.)

2.2.2 laptopy i ultrabooki (Windows, macOS, Linux)

2.2.3 urządzenia ubieralne oraz inteligentne urządzenia hybrydowe zdolne do synchronizacji danych

2.3 Polityka ma zastosowanie niezależnie od tego, czy urządzenie stanowi własność organizacji, czy jest urządzeniem prywatnym wykorzystywanym na podstawie uzgodnienia BYOD.

2.4 Polityka obejmuje wszystkie kanały dostępu, w tym korporacyjny VPN, pulpity wirtualne, aplikacje chmurowe, pocztę elektroniczną, platformy współpracy (np. SharePoint, Teams) oraz narzędzia synchronizacji plików (np. OneDrive, Dropbox, jeżeli są autoryzowane).

2.5 Obejmuje ona korzystanie z urządzeń w ramach pracy zdalnej, w infrastrukturze lokalnej, podczas podróży służbowych oraz w modelach pracy hybrydowej.

3. Cele

3.1 Ograniczenie ryzyka naruszenia, wycieku lub utraty danych wynikających z niebezpiecznego korzystania z urządzeń mobilnych.

3.2 Zapewnienie spójnego i egzekwowalnego stosowania środków bezpieczeństwa we wszystkich mobilnych punktach końcowych, niezależnie od modelu własności (urządzenia organizacji lub BYOD).

3.3 Zapewnienie, że korzystanie z urządzeń mobilnych jest zgodne z ISO/IEC 27001 oraz innymi mającymi zastosowanie ramami regulacyjnymi dotyczącymi prywatności danych, ochrony danych i cyberbezpieczeństwa.

3.4 Umożliwienie bezpiecznej integracji urządzeń mobilnych z procesami operacyjnymi, komunikacyjnymi i współpracy w organizacji.

3.5 Zapewnienie jasno określonych odpowiedzialności i procesów dotyczących zarządzania urządzeniami mobilnymi (MDM), w tym wdrożenia, zdalnego wymazywania, szyfrowania, uwierzytelniania i monitorowania.

3.6 Ochrona prawa do prywatności osób korzystających z własnych urządzeń przy jednoczesnym zabezpieczeniu informacji wrażliwych organizacji.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO) / Kierownik ds. Bezpieczeństwa IT

4.1.1 Określa politykę oraz standardy techniczne dotyczące korzystania z urządzeń mobilnych i BYOD.

4.1.2 Nadzoruje zgodność, reagowanie na incydenty oraz zarządzanie wyjątkami w zakresie zabezpieczeń urządzeń mobilnych.

4.1.3 Koordynuje działania z zespołami prawnym i zgodności oraz zasobów ludzkich (HR), aby zapewnić, że stosowanie polityki jest zgodne z przepisami i spójne organizacyjnie.

4.2 Administrator IT / Administrator MDM

4.2.1 Zarządza nadawaniem dostępu, wdrażaniem i konfiguracją urządzeń mobilnych za pośrednictwem rozwiązań zarządzania urządzeniami mobilnymi (MDM).

4.2.2 Wymusza zabezpieczenia na poziomie urządzenia (np. szyfrowanie, kody PIN, kontrolę aplikacji).

4.2.3 Wykonuje zdalne wymazywanie, blokowanie urządzeń oraz cofanie dostępu, gdy jest to wymagane.

[... 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 Niniejsza polityka musi być przeglądana co najmniej raz w roku przez Dyrektora ds. Bezpieczeństwa Informacji (CISO) lub wyznaczonego Kierownika ds. Bezpieczeństwa Informacji w celu zapewnienia zgodności z:

9.1.1 zmianami w mobilnych platformach systemów operacyjnych, technologiach MDM lub standardach uwierzytelniania,

9.1.2 zmianami regulacyjnymi lub umownymi wpływającymi na ochronę danych mobilnych (np. RODO, DORA, NIS2),

9.1.3 zmianami w zestawach środków bezpieczeństwa ISO/IEC 27001:2022, ISO/IEC 27002:2022 lub NIST SP 800-53 Rev.5,

9.1.4 informacjami zwrotnymi pochodzącymi z audytów, analiz poincydentalnych lub zgłoszeń pracowników.

9.2 Przeglądy doraźne mogą zostać uruchomione przez:

9.2.1 incydenty bezpieczeństwa dotyczące urządzeń mobilnych lub platform BYOD,

9.2.2 powiadomienie dostawcy o podatnościach wysokiego ryzyka w obsługiwanych platformach,

9.2.3 wdrożenie nowych aplikacji mobilnych lub platform współpracy wykorzystywanych do operacji biznesowych.

9.3 Aktualizacje polityki muszą być:

9.3.1 udokumentowane w historii wersji polityki,

9.3.2 zakomunikowane całemu personelowi oraz kontrahentom objętym zakresem,

9.3.3 ponownie potwierdzone poprzez zaktualizowane potwierdzenie zapoznania się dla wszystkich użytkowników BYOD.

9.4 Wszystkie przeglądy i zmiany muszą być formalnie zatwierdzone przez kierownictwo wykonawcze oraz zarejestrowane w Rejestrze zmian polityki.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka pozostaje współzależna z kilkoma kluczowymi politykami w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) organizacji. Do najważniejszych powiązań należą:

10.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia nadrzędne zasady ładu zarządczego dla wszystkich zabezpieczeń informacji, w tym dotyczących korzystania z urządzeń mobilnych.

10.1.2 P3 – Polityka dopuszczalnego użytkowania: określa dozwolone zachowania i ograniczenia dotyczące korzystania z technologii, które mają bezpośrednie zastosowanie do dostępu mobilnego i BYOD.

10.1.3 P9 – Polityka pracy zdalnej: określa dodatkowe obowiązki w zakresie bezpieczeństwa dla mobilnych środowisk pracy, uzupełniając zabezpieczenia specyficzne dla urządzeń mobilnych określone w niniejszej polityce.

10.1.4 P13 – Polityka klasyfikacji i oznaczania informacji: określa sposób postępowania z danymi na urządzeniach mobilnych w zależności od poziomu klasyfikacji, co wpływa na wymagania dotyczące przechowywania, transferu i wymuszania szyfrowania.

10.1.5 P22 – Polityka logowania i monitorowania: wspiera gromadzenie i przegląd rejestrów dostępu mobilnego w celu wykrywania anomalii lub naruszeń.

10.1.6 P30 – Polityka reagowania na incydenty: określa sposób obsługi i eskalacji incydentów związanych z urządzeniami mobilnymi (np. utrata urządzenia, nieuprawniony dostęp).

10.1.7 P33 – Polityka monitorowania audytu i zgodności: stanowi podstawę okresowych kontroli zgodności bezpieczeństwa mobilnego, w tym przestrzegania polityki BYOD.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo ramami cyberbezpieczeństwa oraz obowiązkami prawnymi, aby zapewnić bezpieczne korzystanie z urządzeń mobilnych i prywatnych urządzeń wykorzystywanych do celów służbowych (BYOD) w środowisku przedsiębiorstwa.

11.2 ISO/IEC 27001:

11.2.1 Klauzula 5.10 – Dopuszczalne użytkowanie informacji i innych aktywów powiązanych: wymaga stosowania zabezpieczeń dla odpowiedzialnego korzystania z aktywów korporacyjnych, w tym urządzeń mobilnych.

11.2.2 Klauzula 5.11 – Zwrot aktywów: określa wymagania związane ze zwrotem aktywów organizacji.

11.2.3 Klauzula 5.12 – Klasyfikacja informacji: wymaga odpowiedniego klasyfikowania informacji.

11.2.4 Klauzula 5.13 – Oznaczanie informacji: wymaga właściwego oznaczania informacji.

11.3 ISO/IEC 27002:2022 – Środki bezpieczeństwa 5.10 do 5.13:

11.3.1 Środki bezpieczeństwa z załącznika A 5.10 do 5.13 określają, w jaki sposób w ramach SZBI należy egzekwować dostęp mobilny, szyfrowanie, monitorowanie i ograniczanie skutków utraty. Środki te zawierają szczegółowe wytyczne wdrożeniowe dotyczące zabezpieczenia mobilnych punktów końcowych, stosowania konteneryzacji, monitorowania integralności urządzeń oraz zapewnienia konfiguracji BYOD uwzględniających prywatność.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – kontrola dostępu dla urządzeń mobilnych: określa bazowe zabezpieczenia, w tym szyfrowanie, uwierzytelnianie i egzekwowanie MDM.

11.4.2 AC-17 – dostęp zdalny: wymaga bezpiecznego uwierzytelniania i zabezpieczeń sesji dla zdalnych użytkowników mobilnych.

11.4.3 CM-7 – zasada minimalnej funkcjonalności: wspiera usuwanie zbędnych aplikacji i funkcji z mobilnych punktów końcowych w celu ograniczenia ryzyka.

11.4.4 MP-5 – ochrona transportu nośników: określa zasady bezpiecznego przesyłania danych z systemów mobilnych do lokalizacji zewnętrznych lub do chmury.

11.4.5 SC-12 – ustanawianie kluczy kryptograficznych: wymaga stosowania bezpiecznych protokołów kryptograficznych dla komunikacji mobilnej i przechowywania danych.

11.5 RODO (2016/679):

11.5.1 Artykuł 5(1)(f) – integralność i poufność: wymaga od organizacji ochrony danych osobowych na urządzeniach mobilnych przed dostępem nieuprawnionym lub niezgodnym z prawem.

11.5.2 Artykuł 25 – uwzględnianie ochrony danych w fazie projektowania i domyślna ochrona danych: wymaga wbudowania prywatności w procesy BYOD i MDM.

11.5.3 Artykuł 32 – bezpieczeństwo przetwarzania: wymaga stosowania zabezpieczeń opartych na ryzyku (np. szyfrowania, uwierzytelniania, kontroli dostępu) dla danych osobowych na platformach mobilnych.

11.6 Dyrektywa UE NIS2 (2022/2555):

11.6.1 Artykuł 21(2)(d): wymaga, aby dostęp mobilny do systemów krytycznych i informacji był chroniony przy użyciu odpowiednich zabezpieczeń technicznych i organizacyjnych, takich jak kontrola punktów końcowych, szyfrowanie i monitorowanie.

11.7 Rozporządzenie DORA (2022/2554):

11.7.1 Artykuł 9 – ramy zarządzania ryzykiem ICT: wymaga od podmiotów sektora finansowego ograniczania ryzyk związanych z dostępem mobilnym i zdalnym jako elementu odporności operacyjnej.

11.7.2 Artykuł 10 – wymagania bezpieczeństwa systemów ICT: wymaga bezpiecznej architektury mobilnej, monitorowania oraz mechanizmów reagowania na cyberzagrożenia pochodzące z urządzeń mobilnych.

11.8 COBIT 2019:

11.8.1 APO13.02 – ustanowienie i utrzymanie planu bezpieczeństwa informacji: wymaga uwzględnienia korzystania z urządzeń mobilnych, w tym BYOD, w strategiach bezpieczeństwa organizacji.

11.8.2 DSS01.04 – zarządzanie konfiguracją i integralnością aktywów: odnosi się do kontroli konfiguracji i bezpiecznego wdrażania urządzeń mobilnych.

11.8.3 BAI09.01 – ustanowienie i utrzymanie zabezpieczeń: wspiera wdrażanie zabezpieczeń technicznych i proceduralnych dla bezpiecznych operacji mobilnych i zdalnych.