					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P04S					Tytuł dokumentu: **Polityka kontroli dostępu**							
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**

Zgodność z normami i regulacjami

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 5	
ISO/IEC 27002:2022	Zabezpieczenia: 5.15, 5.16, 5	
NIST SP 800-53 Rev. 5	AC-1 do AC-5	
RODO	Artykuł 32	
Dyrektywa NIS2	Artykuł 21(2)(b)	
Rozporządzenie DORA	Artykuł 9	
COBIT 2019	Zarządzanie zasobami ludzkimi, DSS	

1. Cel

1.1. Niniejsza polityka określa sposób zarządzania dostępem do systemów, danych i obiektów w organizacji w celu zapewnienia, że dostęp do informacji mają wyłącznie osoby upoważnione, zgodnie z uzasadnioną potrzebą biznesową.

1.2. Ustanawia jednoznaczne zasady nadawania, modyfikowania, monitorowania i odbierania dostępu w celu ograniczenia ryzyka nieuprawnionego dostępu oraz zapewnienia zgodności z mającymi zastosowanie przepisami prawa i normami.

1.3. Polityka wdraża zasadę najmniejszych uprawnień, zgodnie z którą dostęp musi być ograniczony do minimum niezbędnego do wykonywania obowiązków służbowych.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich osób, które korzystają z dostępu do systemów IT, sieci, danych lub obiektów organizacji albo zarządzają takim dostępem, w tym do:

2.1.1. pracowników

2.1.2. wykonawców

2.1.3. pracowników tymczasowych

2.1.4. zewnętrznych dostawców usług IT

2.2. Polityka obejmuje dostęp do:

2.2.1. aplikacji firmowych, zasobów plikowych i baz danych

2.2.2. poczty elektronicznej, sieci VPN i systemów dostępu zdalnego

2.2.3. usług chmurowych wykorzystywanych do celów biznesowych

2.2.4. dostępu fizycznego do stref bezpiecznych, takich jak biura lub serwerownie

2.3. Niniejsza polityka obowiązuje w odniesieniu do wszystkich urządzeń (wydanych przez organizację lub zatwierdzonych w modelu korzystania z prywatnych urządzeń do celów służbowych (BYOD)), platform i lokalizacji.

3. Cele

3.1. Zapewnienie, że uprawnienia dostępu są nadawane wyłącznie po formalnej akceptacji, na podstawie roli oraz uzasadnienia biznesowego.

3.2. Zapobieganie nieuprawnionemu lub nadmiernemu dostępowi do danych wrażliwych, systemów lub infrastruktury.

3.3. Określenie jasnych procedur nadawania dostępu, jego modyfikacji oraz zakończenia dostępu użytkownika.

3.4. Wymaganie regularnych przeglądów dostępu oraz zautomatyzowanego lub ręcznego rejestrowania zdarzeń na potrzeby audytu.

3.5. Wsparcie technicznego egzekwowania ograniczeń dostępu poprzez odpowiednią konfigurację i monitorowanie.

4. Role i obowiązki

4.1. Dyrektor Generalny

4.1.1. Zatwierdza niniejszą politykę i zapewnia dostępność zasobów niezbędnych do wdrożenia skutecznych mechanizmów kontroli dostępu.

4.1.2. Zatwierdza odstępstwa i dokonuje przeglądu rocznych audytów dostępu.

4.2. Kierownik IT / zewnętrzny dostawca usług IT

4.2.1. Odpowiada za nadawanie, modyfikację oraz usuwanie kont użytkowników.

4.2.2. Prowadzi rejestr kontroli dostępu obejmujący wszystkie działania (utworzenie, zmiana, usunięcie).

4.2.3. Wdraża kontrolę dostępu opartą na rolach (RBAC) oraz egzekwuje stosowanie silnych mechanizmów uwierzytelniania (np. uwierzytelniania wieloskładnikowego).

4.2.4. Dokonuje przeglądu dzienników dostępu pod kątem podejrzanej aktywności i zgłasza incydenty Dyrektorowi Generalnemu.

[... 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 polityki

9.1.1. Kierownik IT musi dokonywać przeglądu niniejszej polityki co najmniej raz w roku. Każda zmiana uwarunkowań prawnych, technicznych lub organizacyjnych musi skutkować jej niezwłoczną aktualizacją.

9.2. Przesłanki przeglądu

9.2.1. Przegląd polityki musi zostać również przeprowadzony, jeżeli wystąpi którekolwiek z poniższych zdarzeń:

9.2.2. istotne zmiany systemowe lub migracje do chmury

9.2.3. zmiany ról lub struktury organizacyjnej

9.2.4. incydent bezpieczeństwa obejmujący nieuprawniony dostęp

9.2.5. zmiany regulacyjne (np. aktualizacje RODO, NIS2 lub DORA)

9.3. Dokumentowanie i komunikowanie zmian

9.3.1. Zmiany muszą być rejestrowane wraz z historią wersji, zatwierdzeniem przez Dyrektora Generalnego oraz zakomunikowane całemu personelowi, którego dotyczą.

9.4. Dostępność i szkolenia

9.4.1. Niniejsza polityka musi być udostępniona całemu personelowi, a odpowiednie szkolenia powinny być realizowane w ramach wdrożenia oraz następnie corocznie.

10. Powiązane polityki i zależności

10.1. Niniejszą politykę należy stosować łącznie z poniższymi politykami SME w celu pełnego wdrożenia bezpiecznych praktyk w zakresie dostępu:

10.1.1. P3S – Polityka dopuszczalnego użytkowania: zapewnia, że użytkownicy rozumieją dopuszczalne zachowania związane z przyznanym dostępem.

10.1.2. P5S – Polityka zarządzania zmianą: zapewnia, że uprawnienia dostępu są zgodne z zatwierdzonymi zmianami systemowymi.

10.1.3. P7S – Polityka wdrażania i zakończenia współpracy: określa zdarzenia inicjujące nadawanie i odbieranie uprawnień dostępu.

10.1.4. P17S – Polityka ochrony danych i prywatności: zapewnia, że mechanizmy kontroli dostępu są zgodne z zabezpieczeniami danych osobowych.

10.1.5. P30S – Polityka reagowania na incydenty: określa sposób zarządzania i badania incydentów związanych z dostępem (np. niewłaściwego użycia lub naruszeń).

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 5.15 – wymaga sformalizowanych polityk i procesów kontroli dostępu.

11.2. ISO/IEC 27002

11.2.1. Zabezpieczenia 5.15–5.17 – określają szczegółowe wytyczne dotyczące dostępu opartego na rolach, zarządzania cyklem życia użytkownika oraz obsługi dostępu uprzywilejowanego.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 do AC-5 – wymagają ustrukturyzowanych polityk zarządzania dostępem, w tym autoryzacji kont, przeglądów i monitorowania.

11.4. RODO

11.4.1. Artykuł 32 – wymaga wdrożenia środków technicznych i organizacyjnych (takich jak zarządzanie dostępem) w celu zapewnienia bezpieczeństwa i poufności danych.

11.5. Dyrektywa UE NIS2

11.5.1. Artykuł 21(2)(b) – nakłada obowiązek stosowania operacyjnych mechanizmów kontroli dostępu oraz systemów zarządzania tożsamością w celu zapobiegania nieuprawnionemu dostępowi do systemów.

11.6. Rozporządzenie DORA

11.6.1. Artykuł 9 – podkreśla znaczenie bezpiecznego zarządzania ryzykiem ICT, w tym stosowania skutecznej kontroli dostępu przez podmioty finansowe.

11.7. COBIT 2019

11.7.1. Zarządzanie zasobami ludzkimi – wskazuje na potrzebę zdefiniowania i egzekwowania odpowiedzialności za dostęp.

11.7.2. DSS01 – Zarządzanie operacjami: obejmuje procedury zarządzania dostępem logicznym i utrzymywania bezpiecznych środowisk operacyjnych.