					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P11S					Tytuł dokumentu: **Polityka zarządzania kontami użytkowników i uprawnieniami**							
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 5.3, 8	Role, odpowiedzialności oraz planowanie operacyjne i nadzór w zakresie zarządzania dostępem użytkowników
ISO/IEC 27002:2022	Środek kontrolny 8	Środki kontrolne dotyczące nadawania, przeglądu i usuwania uprawnień uprzywilejowanych
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Tworzenie kont, monitorowanie, zasada najmniejszych uprawnień oraz rozdzielenie obowiązków
Dyrektywa NIS2	Artykuł 21(2)(d)	Zarządzanie dostępem użytkowników dla podmiotów kluczowych i ważnych
Rozporządzenie DORA	Artykuł 9(2)(b)	Kontrola dostępu uprzywilejowanego w podmiotach finansowych
COBIT 2019	DSS05.03, DSS05.04	Nadawanie dostępu, odbieranie uprawnień oraz okresowy przegląd dostępu użytkowników
RODO	Artykuł 32	Odpowiednie mechanizmy kontroli dostępu w celu ochrony danych osobowych

1. Cel

1.1 Niniejsza polityka ustanawia zasady zarządzania kontami użytkowników i uprawnieniami dostępu w sposób bezpieczny, spójny i zapewniający rozliczalność audytową. Zapewnia, że dostęp do systemów i danych mają wyłącznie użytkownicy upoważnieni oraz że zakres dostępu jest adekwatny do ich roli i odpowiedzialności.

1.2 Skuteczne zarządzanie kontami i uprawnieniami ma zasadnicze znaczenie dla zapobiegania nieuprawnionemu dostępowi, ograniczania zagrożeń wewnętrznych oraz zapewnienia zgodności z ISO/IEC 27001, RODO i innymi wymaganiami regulacyjnymi.

1.3 Niniejsza polityka umożliwia organizacji przypisanie właściciela i odpowiedzialności za korzystanie z kont, monitorowanie i audytowanie podwyższania uprawnień oraz bezpieczne wyłączanie lub cofanie uprawnień dostępu, gdy nie są już potrzebne.

1.4 Polityka chroni również działalność organizacji przed błędami operacyjnymi lub niewłaściwym użyciem wynikającym z nadmiernego lub niemonitorowanego dostępu oraz pomaga ograniczać ryzyko przypadkowych wycieków danych, niewłaściwego użycia uprawnień lub braku zgodności z wymaganiami regulacyjnymi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników, stażystów, kontraktorów oraz użytkowników stron trzecich posiadających dostęp do systemów IT organizacji,

2.1.2 wszystkich systemów, urządzeń, usług i platform zarządzanych przez organizację lub w jej imieniu, w tym platform chmurowych, infrastruktury lokalnej oraz narzędzi stron trzecich.

2.2 Obejmuje wszystkie rodzaje kont użytkowników, w tym:

2.2.1 imienne konta użytkowników, np. konta poczty elektronicznej i konta systemowe,

2.2.2 konta administratorów oraz konta systemowe,

2.2.3 tymczasowe poświadczenia dostępu, konta gościnne lub konta stron trzecich,

2.2.4 konta serwisowe używane przez aplikacje lub systemy automatyzacji.

2.3 Polityka ma zastosowanie do całego cyklu życia konta — od utworzenia i zatwierdzenia po modyfikację, monitorowanie i dezaktywację. Obejmuje to początkowe nadawanie dostępu podczas wdrożenia, przeglądy dostępu przy zmianach ról oraz cofanie uprawnień dostępu podczas zakończenia współpracy.

3. Cele

3.1 Przypisanie wszystkim użytkownikom systemów unikalnych, możliwych do prześledzenia identyfikatorów użytkownika, zapewniających rozliczalność i eliminujących stosowanie współdzielonych poświadczeń.

3.2 Egzekwowanie zasady najmniejszych uprawnień, tak aby użytkownikom nadawano wyłącznie minimalny poziom dostępu niezbędny do wykonywania obowiązków.

3.3 Zapobieganie nieuprawnionemu dostępowi do systemów wrażliwych lub danych poprzez jasno udokumentowane procesy zatwierdzania i przeglądu.

3.4 Zapewnienie terminowej dezaktywacji kont użytkowników, gdy nie są już wymagane, np. w przypadku rozwiązania stosunku pracy, zakończenia kontraktu lub zmiany roli.

3.5 Utrzymywanie bezpiecznego środowiska zapewniającego gotowość do audytu poprzez dokumentowanie wszystkich zmian na kontach, zatwierdzeń i okresowych przeglądów.

3.6 Zapewnienie, że podwyższanie uprawnień podlega ścisłej kontroli, niezależnemu zatwierdzeniu i rejestrowaniu oraz że podwyższony dostęp jest niezwłocznie cofany, gdy nie jest już potrzebny.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 PonosI ogólną odpowiedzialność za egzekwowanie postanowień niniejszej polityki.

4.1.2 Zapewnia, że praktyki zarządzania kontami są zgodne z wymaganiami certyfikacyjnymi ISO/IEC 27001 oraz odpowiednimi obowiązkami prawnymi, takimi jak RODO.

4.1.3 Musi być niezwłocznie informowany o każdym nieuprawnionym dostępie, incydencie bezpieczeństwa lub naruszeniu polityki związanym z kontami użytkowników.

4.1.4 Nadzoruje przeglądy polityki, audyty oraz działania związane z egzekwowaniem jej postanowień.

4.2 Kierownik IT lub zewnętrzny dostawca usług IT

4.2.1 Odpowiada za techniczne wdrożenie mechanizmów kontroli kont i uprawnień we wszystkich systemach wykorzystywanych przez organizację.

4.2.2 Musi tworzyć, modyfikować i dezaktywować konta użytkowników wyłącznie na podstawie udokumentowanych zatwierdzeń.

4.2.3 Musi egzekwować złożoność haseł, blokadę ekranu po okresie bezczynności, uwierzytelnianie wieloskładnikowe, jeśli jest dostępne, oraz rejestrowanie zdarzeń systemowych.

4.2.4 Musi utrzymywać bezpieczne zapisy wszystkich zatwierdzeń dostępu, właścicieli kont, przypadków podwyższania uprawnień oraz cofnięcia uprawnień dostępu.

4.2.5 Jest zobowiązany monitorować nieuprawnione lub osierocone konta oraz zgłaszać rozbieżności do GM.

[... 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 GM i Kierownika IT w celu zapewnienia zgodności z:

9.1.1 aktualnymi środkami kontrolnymi i wytycznymi ISO/IEC 27001:2022,

9.1.2 zmianami regulacyjnymi, np. RODO, DORA, NIS2,

9.1.3 zmianami w systemach, usługach lub strukturze biznesowej.

9.2 Przeglądy muszą być również przeprowadzane po:

9.2.1 istotnych incydentach bezpieczeństwa lub ustaleniach audytowych,

9.2.2 znaczących zmianach w systemach IT lub architekturze kont,

9.2.3 wdrożeniu nowych platform wymagających integracji mechanizmów kontroli dostępu.

9.3 Wszystkie zmiany muszą zostać zatwierdzone przez GM i w sposób jasny zakomunikowane personelowi, którego dotyczą.

10. Powiązane polityki i odniesienia

10.1 P2S – Polityka ról i odpowiedzialności w ramach nadzoru organizacyjnego: określa rozliczalność i uprawnienia decyzyjne w zakresie zatwierdzania dostępu oraz nadzoru.

10.2 P4S – Polityka kontroli dostępu: reguluje stosowanie mechanizmów kontroli dostępu w całym środowisku systemowym oraz metody uwierzytelniania.

10.3 P7S – Polityka wdrażania i zakończenia współpracy: zapewnia, że tworzenie i usuwanie kont jest uwzględnione w zmianach kadrowych zarządzanych przez HR.

10.4 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: szkoli użytkowników w zakresie bezpiecznych praktyk dotyczących kont i oczekiwanego sposobu ich używania.

10.5 P30S – Polityka reagowania na incydenty: definiuje działania, które należy podjąć, jeżeli niewłaściwe użycie konta prowadzi do naruszenia bezpieczeństwa lub nieuprawnionego ujawnienia informacji.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 5.3: wymaga, aby role i odpowiedzialności w zakresie bezpieczeństwa informacji były jednoznacznie przypisane i egzekwowane.

11.1.2 Klauzula 8.1: planowanie operacyjne i nadzór muszą obejmować zarządzanie dostępem użytkowników.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.2: określa techniczne i proceduralne środki kontrolne dotyczące nadawania, przeglądu i usuwania uprawnień uprzywilejowanych.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: wymaga tworzenia kont, monitorowania i cofania uprawnień dostępu w oparciu o zdefiniowane role i procesy.

11.3.2 AC-5: dotyczy rozdzielenia obowiązków w celu zapobiegania konfliktom interesów lub nadużyciom uprawnień.

11.3.3 AC-6: nakazuje stosowanie zasady najmniejszych uprawnień do wszystkich praw dostępu.

11.4 RODO

11.4.1 Artykuł 32: wymaga stosowania odpowiednich mechanizmów kontroli dostępu w celu ochrony danych osobowych przed nieuprawnionym dostępem lub modyfikacją.

11.5 Dyrektywa NIS2

11.5.1 Artykuł 21(2)(d): nakłada wymóg zarządzania dostępem użytkowników jako elementu podstawowych środków bezpieczeństwa dla podmiotów kluczowych i ważnych.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 9(2)(b): wymaga, aby podmioty finansowe wdrożyły mechanizmy kontroli dostępu ograniczające i monitorujące uprawnienia uprzywilejowane.

11.7 COBIT 2019

11.7.1 DSS05.03: określa nadawanie dostępu i odbieranie uprawnień użytkowników jako część nadzoru nad IT.

11.7.2 DSS05.04: wskazuje na potrzebę bieżącego przeglądu dostępu użytkowników i jego dostosowania do ról organizacyjnych.