					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P11					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	Klauzula 6.1.3, Klauzula 8	-
ISO/IEC 27002:2022	Środki kontrolne 5.15-5	-
RODO	Artykuły 5(1)(f), 32; Motyw 39	-
Dyrektywa NIS2	Artykuły 21(2)(a, d), 21(3)	-
Rozporządzenie DORA	Artykuły 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Cel

1 Niniejsza polityka ustanawia obowiązkowe środki kontrolne dotyczące zarządzania kontami użytkowników i uprawnieniami we wszystkich systemach informatycznych i usługach. Zapewnia, że dostęp do zasobów organizacji jest nadawany na podstawie zweryfikowanej tożsamości, uzasadnionej potrzeby wynikającej z roli oraz zasad najmniejszych uprawnień i rozdzielenia obowiązków.

1.1 Wspiera ona zobowiązanie organizacji do zapewnienia bezpieczeństwa informacji poprzez wdrożenie ustrukturyzowanych, audytowalnych procesów nadawania dostępu, przypisywania uprawnień, monitorowania wykorzystania oraz cofania uprawnień dostępu.

1.2 Polityka ta ma kluczowe znaczenie dla ograniczania ryzyka nieuprawnionego dostępu, niewłaściwego wykorzystania uprawnień, zagrożeń wewnętrznych oraz niezgodności z mającymi zastosowanie ramami regulacyjnymi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich pracowników, kontraktorów, dostawców usług zewnętrznych, konsultantów oraz innych osób, którym przyznano dostęp do zasobów IT, aplikacji lub danych organizacji.

2.2 Obejmuje wszystkie systemy i środowiska, w których stosowane są mechanizmy uwierzytelniania użytkowników i kontroli dostępu, w tym między innymi:

2.2.1 Aplikacje korporacyjne i bazy danych

2.2.2 Platformy chmurowe i środowiska SaaS

2.2.3 Systemy operacyjne i konsole administracyjne

2.2.4 Narzędzia dostępu zdalnego i VPN

2.2.5 Systemy zarządzania tożsamością i dostępem (IAM)

2.3 Polityka obejmuje zarówno standardowe konta użytkowników, jak i konta uprzywilejowane, i zawiera środki kontrolne dotyczące:

2.3.1 Tworzenia, modyfikacji i dezaktywacji kont

2.3.2 Eskalacji uprawnień i delegowania uprawnień

2.3.3 Kontroli i monitorowania sesji

2.3.4 Metod uwierzytelniania i zarządzania poświadczeniami

3. Cele

3.1 Zapewnienie, że wszystkie konta użytkowników są jednoznacznie identyfikowalne, prawidłowo autoryzowane i przypisywane wyłącznie po formalnym potwierdzeniu potrzeby biznesowej.

3.2 Wdrożenie zasady najmniejszych uprawnień oraz zapobieganie zbędnemu lub nadmiernemu dostępowi poprzez egzekwowanie ścisłych środków kontrolnych dotyczących nadawania i wykorzystywania kont uprzywilejowanych.

3.3 Zapewnienie terminowej aktualizacji statusu kont w następstwie zmian zatrudnienia lub roli, w tym natychmiastowej dezaktywacji po zakończeniu współpracy.

3.4 Umożliwienie proaktywnego wykrywania i usuwania uśpionych, niewłaściwie używanych lub nieautoryzowanych kont za pomocą rejestrowania, przeglądów i automatyzacji.

3.5 Utrzymanie zgodności z ISO/IEC 27001:2022 i powiązanymi normami oraz spełnienie obowiązków wynikających z odpowiednich ram prawnych i regulacyjnych, takich jak RODO, NIS2, DORA i COBIT 2019.

4. Role i odpowiedzialności

4.1 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia jej stosowanie w całej organizacji.

4.1.2 Dokonuje przeglądu i zatwierdza wszelkie formalne odstępstwa oraz przypadki dostępu awaryjnego.

4.1.3 Raportuje ustalenia audytowe dotyczące kont i eskaluje ryzyka do kierownictwa wykonawczego.

4.2 Menedżer kontroli dostępu / Administrator IT

4.2.1 Utrzymuje i obsługuje zabezpieczenia techniczne służące do zarządzania cyklem życia kont użytkowników.

4.2.2 Realizuje nadawanie dostępu, odbieranie uprawnień oraz działania związane z zarządzaniem uprawnieniami na podstawie zatwierdzonego wniosku.

4.2.3 Prowadzi autorytatywny rejestr wszystkich kont użytkowników, ich statusu oraz poziomu uprawnień.

4.2.4 Wspiera audyty i przeglądy zgodności, dostarczając logi i raporty aktywności.

[... 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 podlegać przeglądowi co najmniej raz w roku lub w przypadku istotnych zmian dotyczących:

9.1.1 Struktury organizacyjnej lub procesów biznesowych

9.1.2 Systemów IT, platform tożsamości lub metod dostępu

9.1.3 Wymagań regulacyjnych lub umownych związanych z zarządzaniem tożsamością i dostępem

9.2 Dyrektor ds. bezpieczeństwa informacji (CISO), we współpracy z Menedżerem kontroli dostępu, odpowiada za zainicjowanie procesu przeglądu oraz koordynację informacji zwrotnych od interesariuszy.

9.3 Przeglądy doraźne mogą zostać uruchomione w wyniku:

9.3.1 Incydentów bezpieczeństwa związanych z niewłaściwym wykorzystaniem kont

9.3.2 Ustaleń audytowych wskazujących na słabości w zarządzaniu cyklem życia kont

9.3.3 Wdrożenia nowych narzędzi do zarządzania tożsamością lub zarządzania dostępem uprzywilejowanym (PAM)

9.4 Aktualizacje niniejszej polityki muszą być:

9.4.1 Objęte kontrolą wersji i odnotowane w bibliotece dokumentacji SZBI

9.4.2 Zakomunikowane wszystkim właściwym interesariuszom, w tym kierownikom działów, operacjom IT i HR

9.4.3 Wspierane przez zaktualizowane materiały szkoleniowe i instrukcje proceduralne

9.5 Wszystkie zmiany muszą być zatwierdzane przez kierownictwo wykonawcze lub Komitet Sterujący ds. Bezpieczeństwa Informacji oraz rejestrowane do celów audytowych.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest operacyjnie powiązana z następującymi politykami w ramach pakietu SZBI i jest przez nie wspierana:

10.1.1 P4 Polityka kontroli dostępu: ustanawia nadrzędne zasady i mechanizmy kontroli dostępu, w tym środki kontrolne oparte na regułach i rolach.

10.1.2 P7 Polityka wdrożenia i zakończenia współpracy: określa proceduralne kroki inicjowania i kończenia dostępu użytkowników zgodnie z działaniami HR.

10.1.3 P8 Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: wzmacnia odpowiedzialność użytkowników za bezpieczeństwo kont i ochronę poświadczeń.

10.1.4 P13 Polityka klasyfikacji danych i etykietowania: określa poziomy dostępu na podstawie klasyfikacji danych, zapewniając zgodność granic uprawnień z poziomami wrażliwości.

10.1.5 P22 Polityka rejestrowania i monitorowania: zapewnia gromadzenie ścieżek audytu dla wszystkich działań związanych z kontami oraz ich przegląd w celu wykrywania anomalii lub nieuprawnionego użycia.

10.1.6 P30 Polityka reagowania na incydenty: reguluje eskalację, powstrzymanie i działania po incydencie w przypadkach nadużycia uprawnień lub nieuprawnionej aktywności kont.

10.2 Każda z tych polityk działa łącznie w celu egzekwowania spójnych, opartych na ryzyku ram zarządzania tożsamością i dostępem w całej organizacji.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi na świecie normami cyberbezpieczeństwa i ramami regulacyjnymi, które wymagają bezpiecznego zarządzania tożsamością, dostępem i uprawnieniami jako podstawowego elementu bezpieczeństwa informacji w organizacji.

11.2 ISO/IEC 27001:

11.2.1 Klauzula 6.1.3 - wymaga od organizacji określenia, oceny i postępowania z ryzykiem bezpieczeństwa informacji, co sprawia, że zarządzanie dostępem i uprawnieniami stanowi formalny środek kontroli oparty na ryzyku, osadzony w procesie planowania SZBI.

11.2.2 Klauzula 8.1 - Planowanie i nadzór operacyjny: wzmacnia wdrożenie zabezpieczeń technicznych i proceduralnych regulujących dostęp użytkowników oraz dostęp uprzywilejowany.

11.3 ISO/IEC 27002:2022 - Środki kontrolne 5.15 do 5:

11.3.1 Środek kontrolny 5.15 - Zarządzanie dostępem użytkowników: wspiera formalne procesy nadawania dostępu, autoryzacji dostępu oraz okresowego przeglądu praw dostępu.

11.3.2 Środek kontrolny 5.16 - Zarządzanie tożsamością: ustanawia unikalność tożsamości, środki kontroli cyklu życia oraz wymuszanie bezpiecznego uwierzytelniania.

11.3.3 Środek kontrolny 5.17 - zapewnia, że przydzielanie i wykorzystywanie praw dostępu uprzywilejowanego jest ściśle kontrolowane, możliwe do prześledzenia i zgodne z zasadą najmniejszych uprawnień w całym cyklu życia konta użytkownika.

11.3.4 Środek kontrolny 5.18 - Prawa dostępu uprzywilejowanego: w pełni adresowany poprzez przypisywanie uprawnień oparte na rolach, audyt oraz wymagania dotyczące zatwierdzania dostępu podwyższonego.

11.4 Środki kontrolne te wyznaczają kierunek dla ustrukturyzowanego wdrożenia rejestracji kont, wyrejestrowywania kont, rozdzielenia uprawnień oraz stosowania informacji uwierzytelniających. Polityka egzekwuje nadzór nad cyklem życia tożsamości, dostęp just-in-time oraz monitorowanie sesji podwyższonych w celu zapobiegania nieuprawnionemu korzystaniu z systemów.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Polityka kontroli dostępu) i AC-2 (Zarządzanie kontami): odwzorowane poprzez wymagania polityki dotyczące zatwierdzania dostępu, mapowania ról i audytowania kont użytkowników.

11.5.2 AC-5 (Rozdzielenie obowiązków) i AC-6 (Najmniejsze uprawnienia): realizowane poprzez ograniczanie uprawnień, powiązanie z rolami służbowymi oraz podwójne zatwierdzanie zadań wysokiego ryzyka.

11.5.3 IA-2 do IA-5 (Identyfikacja i uwierzytelnianie): egzekwowane poprzez silne mechanizmy uwierzytelniania, zasady cyklu życia poświadczeń oraz wymagania MFA.

11.5.4 AU-2, AU-12 (rejestrowanie audytowe i analiza): realizowane poprzez rejestrowanie sesji oraz monitorowanie działań uprzywilejowanych w środowiskach wrażliwych.

11.6 RODO (2016/679):

11.6.1 Artykuł 32 - Bezpieczeństwo przetwarzania: wymaga kontroli dostępu oraz mechanizmów weryfikacji tożsamości w celu ochrony danych osobowych. Jest realizowany poprzez obowiązek zatwierdzania kont, przeglądów uprawnień i stosowania silnych zabezpieczeń uwierzytelniania.

11.6.2 Artykuł 5(1)(f) - Integralność i poufność: zapewnia, że do danych osobowych mają dostęp wyłącznie upoważnieni użytkownicy pełniący uzasadnione role, co jest wzmacniane przez egzekwowanie zarządzania kontami.

11.6.3 Motyw 39: wskazuje na potrzebę jasnego ograniczania dostępu i rozliczalności — niniejsza polityka wspiera pełną identyfikowalność tożsamości użytkowników i przypisań uprawnień.

11.7 Dyrektywa NIS2 (2022/2555):

11.7.1 Artykuł 21(2)(a, d): wymaga od podmiotów stosowania polityk zarządzania dostępem oraz bezpiecznego postępowania z poświadczeniami i sesjami uprzywilejowanymi, co jest wspierane przez środki kontrolne dotyczące nadawania, monitorowania i odstępstw określone w niniejszej polityce.

11.7.2 Artykuł 21(3): promuje dyscyplinę dostępu i silne zapewnienie tożsamości w sektorach krytycznych, realizowane poprzez stosowanie unikalnych identyfikatorów, RBAC oraz ograniczonego czasowo dostępu podwyższonego.

11.8 Rozporządzenie DORA (2022/2554):

11.8.1 Artykuł 5 - Ład ICT i kontrola: wymaga sformalizowanych procesów zarządzania użytkownikami ICT, co jest objęte udokumentowanymi zasadami nadawania dostępu, dezaktywacji i obsługi odstępstw.

11.8.2 Artykuł 9 - Zarządzanie ryzykiem ICT: nakierowuje organizacje na zabezpieczanie systemów poprzez ograniczenia dostępu i monitorowanie, co jest realizowane przez MFA, rejestrowanie dostępu uprzywilejowanego oraz scentralizowane przeglądy.

11.9 COBIT 2019:

11.9.1 DSS01 - Zarządzane operacje: promuje stosowanie ustandaryzowanych środków kontroli operacyjnej, w tym zarządzania cyklem życia kont użytkowników i dokumentowania dostępu.

11.9.2 DSS05 - Zarządzane usługi bezpieczeństwa: odzwierciedla bezpieczną administrację uprawnieniami użytkowników i systemów, wspierając ograniczanie ryzyka poprzez najmniejsze uprawnienia i walidację ścieżki audytu.

11.9.3 APO13 - Zarządzane bezpieczeństwo: wymaga nadzoru nad dostępem w odniesieniu do aktywów cyfrowych, co jest realizowane poprzez sformalizowane praktyki autoryzacji kont i ról oraz obowiązkowe okresowe przeglądy.