					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P04					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**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 5.15, 5.17, 5.18	Zarządzanie dostępem logicznym i fizycznym
ISO/IEC 27002:2022	Środki kontrolne 8.2, 8.3	Kontrola dostępu oparta na rolach (RBAC) i zarządzanie tożsamością
NIST SP 800-53 Rev. 5	AC-1 do AC-20, IA-1 do IA-8	Kontrole kont i dostępu, tożsamość i uwierzytelnianie
RODO	Artykuły 5 ust. 1 lit. f, 32 ust. 1 lit. b; motyw 39	Ochrona danych i minimalizacja dostępu
Dyrektywa NIS2	Artykuł 21 ust. 2 lit. c–e	Kontrola dostępu, uwierzytelnianie użytkowników i ochrona aktywów
Rozporządzenie DORA	Artykuły 6, 9 ust. 2	Dostęp użytkowników do ICT, silne mechanizmy kontrolne, strony trzecie
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Wdrożenie, operacje, monitorowanie i zgodność

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe zasady, odpowiedzialności oraz wymagania dotyczące mechanizmów kontrolnych w zakresie zarządzania dostępem do systemów informatycznych, aplikacji, obiektów fizycznych oraz zasobów danych w całej organizacji.

1.2 Zapewnia ona, że dostęp jest przyznawany na podstawie potrzeb biznesowych, roli służbowej oraz profilu ryzyka, z zastosowaniem takich zasad jak zasada najmniejszych uprawnień, zasada wiedzy koniecznej oraz rozdzielenie obowiązków.

1.3 Polityka wspiera wdrożenie klauzuli 5.15 normy ISO/IEC 27001:2022 oraz powiązanych mechanizmów kontrolnych regulujących dostęp logiczny i fizyczny, uwierzytelnianie użytkowników oraz zarządzanie cyklem życia dostępu.

1.4 Niniejsza polityka stanowi podstawę ochrony zasobów cyfrowych i fizycznych przed nieuprawnionym użyciem, nadużyciem lub naruszeniem bezpieczeństwa.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich użytkowników, systemów i obiektów objętych zakresem SZBI, w tym do:

2.1.1 pracowników, kontraktorów, dostawców oraz personelu tymczasowego

2.1.2 infrastruktury lokalnej, zasobów hostowanych w chmurze oraz środowisk hybrydowych

2.1.3 wszystkich zasobów organizacji — sprzętu, oprogramowania, danych oraz chronionych obszarów fizycznych

2.1.4 dostępu logicznego (np. systemy, sieci, aplikacje, interfejsy API) oraz dostępu fizycznego (np. budynki, centra danych)

2.2 Reguluje ona dostęp w całym cyklu życia tożsamości i interakcji z zasobami — od wdrożenia i nadawania dostępu po zmiany ról i zakończenie współpracy.

2.3 Polityka obejmuje również wykorzystywanie prywatnych urządzeń (BYOD) oraz dostęp zdalny (VPN, zarządzanie urządzeniami mobilnymi), zapewniając spójność mechanizmów kontrolnych niezależnie od lokalizacji i modelu własności urządzenia.

3. Cele

3.1 Wdrożenie bezpiecznych mechanizmów kontroli dostępu opartych na rolach, wspierających integralność operacyjną i zgodność regulacyjną.

3.2 Zapewnienie, że uprawnienia dostępu są właściwie zatwierdzane, monitorowane i terminowo odbierane.

3.3 Zapobieganie nieuprawnionemu dostępowi, eskalacji uprawnień oraz utrzymywaniu nieaktualnych uprawnień dostępu.

3.4 Wspieranie zasad zero trust poprzez domyślną odmowę dostępu, chyba że został on wyraźnie zatwierdzony i uzasadniony.

3.5 Zapewnienie audytorom i interesariuszom możliwości wykazania zgodności poprzez oparte na dowodach i zautomatyzowane przeglądy dostępu oraz egzekwowanie postanowień polityki.

3.6 Włączenie kontroli dostępu do procesów biznesowych, zdarzeń w cyklu życia HR oraz architektury technicznej.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza politykę kontroli dostępu oraz zapewnia odpowiedni budżet i zasoby kadrowe do jej stosowania.

4.1.2 Dokonuje przeglądu ryzyk związanych z kontrolą dostępu podczas przeglądów zarządzania oraz przypisuje rozliczalność na poziomie strategicznym.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO) / Kierownik systemu zarządzania bezpieczeństwem informacji

4.2.1 Odpowiada za ramy kontroli dostępu i zapewnia ich zgodność z ISO/IEC 27001 oraz powiązanymi normami.

4.2.2 Koordynuje stosowanie polityki, testowanie mechanizmów kontrolnych i raportowanie wskaźników kontroli dostępu.

4.2.3 Nadzoruje modelowanie dostępu oparte na ryzyku i monitoruje systemowe luki kontrolne.

[... 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 Wyzwalacze przeglądu i częstotliwość

9.1.1 Niniejsza polityka musi być przeglądana:

9.1.1.1 corocznie lub

9.1.1.2 po istotnej zmianie infrastruktury IT, wymagań regulacyjnych lub profilu ryzyka

9.1.1.3 po incydentach ujawniających słabości kontroli dostępu

9.1.1.4 w przypadku istotnych zmian w technologiach uwierzytelniania lub platformach tożsamościowych

9.2 Uprawnienia do przeglądu i proces

9.2.1 CISO lub wyznaczona osoba kierująca SZBI zarządza cyklem przeglądu, uwzględniając:

9.2.1.1 ustalenia audytu wewnętrznego

9.2.1.2 wyniki i wskaźniki przeglądów dostępu

9.2.1.3 aktualizacje prawne i regulacyjne

9.2.1.4 zmiany platform technologicznych

9.2.2 Wszystkie zmiany muszą zostać zatwierdzone przez kierownictwo wykonawcze i zakomunikowane wszystkim interesariuszom.

9.2.3 Użytkownicy, których dotyczą zmiany, mogą być zobowiązani do ponownego potwierdzenia zapoznania się z polityką po wprowadzeniu istotnych aktualizacji.

9.3 Kontrola wersji i dokumentacja

9.3.1 Wersja główna musi być przechowywana w repozytorium dokumentów SZBI z następującymi metadanymi:

9.3.1.1 numer wersji i rejestr zmian

9.3.1.2 data wejścia w życie i data kolejnego przeglądu

9.3.1.3 właściciel i organ zatwierdzający

9.3.1.4 zapisy dystrybucji i potwierdzeń zapoznania się

9.3.2 Wersje wycofane muszą być archiwizowane i dostępne przez co najmniej 3 lata.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest funkcjonalnie zależna od poniższych dokumentów i musi być interpretowana łącznie z nimi:

10.1.1 P01 – Polityka bezpieczeństwa informacji: określa zobowiązanie organizacji w zakresie bezpieczeństwa oraz wysokopoziomowe oczekiwania dotyczące kontroli dostępu.

10.1.2 P03 – Polityka dopuszczalnego użytkowania: określa zasady korzystania z dostępu oraz rozliczalność użytkowników za odpowiedzialne korzystanie z systemów.

10.1.3 P05 – Polityka zarządzania zmianą: reguluje sposób bezpiecznego wdrażania i testowania zmian konfiguracji dostępu, ról lub struktur grup.

10.1.4 P07 – Polityka wdrażania i zakończenia współpracy: inicjuje nadawanie i cofanie uprawnień dostępu zgodnie ze zdarzeniami w cyklu życia użytkownika.

10.1.5 P11 – Polityka zarządzania kontami użytkowników i uprawnieniami: operacjonalizuje mechanizmy kontrolne na poziomie kont i uzupełnia niniejszą politykę o wytyczne dotyczące technicznego egzekwowania dostępu.

10.2 Łącznie polityki te tworzą spójne i egzekwowalne ramy nadzoru nad dostępem we wszystkich jednostkach biznesowych i technologiach.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001:2022:

11.1.1 Klauzula 5.15 – Kontrola dostępu: niniejsza polityka spełnia wymóg kontrolowania dostępu do informacji i innych powiązanych aktywów na podstawie wymagań biznesowych oraz wymagań bezpieczeństwa informacji.

11.1.2 Klauzula 5.17 – Zarządzanie tożsamością oraz klauzula 5.18 – Informacje uwierzytelniające: są realizowane poprzez systemy provisioningu tożsamości, mechanizmy uwierzytelniania oraz przypisania uprawnień.

11.1.3 Załącznik A, środki kontrolne 8.2 (Polityka kontroli dostępu) i 8.3 (Zarządzanie tożsamością): stanowią podstawę celów kontrolnych niniejszej polityki, w tym dostępu opartego na rolach, integracji z cyklem życia użytkownika oraz ochrony dostępu uprzywilejowanego.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Rodzina AC (AC-1 do AC-20): niniejsza polityka wspiera wymagania NIST dotyczące kontroli dostępu zarówno do systemów fizycznych, jak i logicznych, w tym definiowanie polityki (AC-1), zarządzanie kontami (AC-2) oraz rozdzielenie obowiązków (AC-5).

11.2.2 Rodzina IA (IA-1 do IA-8): zapewnia wytyczne dotyczące uwierzytelniania tożsamości, ochrony poświadczeń oraz MFA.

11.2.3 AU-2, AU-12: wymagania dotyczące rejestrowania i audytu egzekwowane na podstawie niniejszej polityki wspierają rozliczalność użytkowników oraz dochodzenia incydentów.

11.2.4 PE-2 do PE-6: dotyczą ograniczeń dostępu fizycznego, które niniejsza polityka częściowo egzekwuje za pomocą identyfikatorów dostępu i uprawnień wejścia do budynków.

11.3 RODO (2016/679):

11.3.1 Artykuł 5 ust. 1 lit. f: dane osobowe muszą być chronione przed nieuprawnionym dostępem. Niniejsza polityka zapewnia techniczne i proceduralne stosowanie tej zasady.

11.3.2 Artykuł 32 ust. 1 lit. b: wymaga wdrożenia mechanizmów kontroli dostępu, pseudonimizacji i szyfrowania w celu zapobiegania nieuprawnionemu przetwarzaniu danych osobowych.

11.3.3 Motyw 39: nakazuje minimalizację dostępu do danych osobowych, realizowaną tutaj poprzez zasadę najmniejszych uprawnień oraz wymogi uzasadniania dostępu.

11.4 Dyrektywa NIS2 (2022/2555):

11.4.1 Artykuł 21 ust. 2 lit. c–e: niniejsza polityka umożliwia stosowanie środków technicznych i organizacyjnych w zakresie kontroli dostępu, uwierzytelniania użytkowników oraz ochrony aktywów w podmiotach kluczowych i ważnych.

11.5 Rozporządzenie DORA (2022/2554):

11.5.1 Artykuł 6: wymaga polityk zarządzania ryzykiem ICT, które wyraźnie obejmują zarządzanie dostępem użytkowników i mechanizmy kontrolne cyklu życia tożsamości. Niniejsza polityka spełnia ten wymóg dla sektorów finansowych i usług ICT.

11.5.2 Artykuł 9 ust. 2: niniejsza polityka wspiera egzekwowanie silnych mechanizmów kontroli dostępu jako części zarządzania usługami ICT wewnątrz grupy oraz świadczonymi przez strony trzecie.

11.6 COBIT 2019:

11.6.1 APO07 – Zarządzanie zasobami ludzkimi: egzekwuje mechanizmy kontrolne wdrożenia i offboardingu w celu wsparcia nadzoru nad dostępem.

11.6.2 BAI03 – Managed Solutions Identification and Build: uwzględnia wymagania kontroli dostępu w projektowaniu systemów i procesach zmian.

11.6.3 DSS01 – Managed Operations i DSS05 – Zarządzanie usługami bezpieczeństwa: regulują egzekwowanie ograniczeń dostępu logicznego oraz monitorowanie naruszeń.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: wspiera mechanizmy audytu i zapewnienia skuteczności zabezpieczeń służące walidacji skuteczności kontroli dostępu.