					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P07					Tytuł dokumentu: **Polityka wdrażania i zakończenia współpracy**							
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 7.2, Klauzula 6	Kompetencje personelu, bezpieczne wdrożenie oraz egzekwowanie obowiązków związanych z zakończeniem współpracy lub zmianą roli.
ISO/IEC 27002:2022	Środki kontrolne 6.2, 6.5, 5	Wdrażanie, dostęp oraz środki kontrolne dotyczące cyklu życia personelu.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Zmiana roli i zakończenie współpracy personelu, zasada najmniejszych uprawnień, rejestrowanie zdarzeń audytowych, zarządzanie dostępem w trakcie i po zmianach personalnych.
RODO	Artykuły 5(1)(f), 25, 32; Motyw 39	Ograniczenie dostępu, poufność, ochrona oraz odpowiednie środki kontrolne dotyczące danych personelu.
Dyrektywa NIS2	Artykuł 21(2)(b, c, d)	Środki bezpieczeństwa dotyczące personelu i operacji; ograniczanie zagrożeń wewnętrznych; procesy cyklu życia.
Rozporządzenie DORA	Artykuły 5, 8, 9	Ład organizacyjny, kontrola wewnętrzna ICT, ryzyko ICT, zarządzanie incydentami w trakcie zmian personalnych.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Zasoby ludzkie, zarządzanie wiedzą, bezpieczeństwo i zgodność w procesach wdrażania i zakończenia współpracy.

1. Cel

1.1 Niniejsza polityka ustanawia ustandaryzowane procedury zarządzania wdrażaniem, transferami wewnętrznymi oraz zakończeniem współpracy dla wszystkich typów użytkowników.

1.2 Zapewnia terminowe i bezpieczne nadawanie oraz odbieranie dostępu fizycznego i logicznego, przy jednoczesnym egzekwowaniu poufności, rozliczalności oraz zwrotu aktywów.

1.3 Polityka ogranicza ryzyka związane z nieuprawnionym dostępem, wyciekiem danych oraz niezwróconymi aktywami poprzez włączenie środków kontrolnych dotyczących wdrażania i zakończenia współpracy do procesów HR, IT i bezpieczeństwa.

1.4 Wspiera środek kontrolny 6.5 załącznika A normy ISO/IEC 27001:2022, zapewniając egzekwowanie obowiązków z zakresu bezpieczeństwa personelu w trakcie i po zakończeniu zatrudnienia lub współpracy.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich pracowników, wykonawców, konsultantów, dostawców oraz innych stron trzecich, którym przyznano dostęp do systemów, sieci, obiektów lub danych organizacji.

2.2 Obejmuje pełny cykl życia następujących procesów:

2.2.1 Wdrożenie (zatrudnienie, zawarcie umowy lub czasowe zaangażowanie)

2.2.2 Transfery wewnętrzne lub zmiany ról

2.2.3 Zakończenie współpracy (rezygnacja, przejście na emeryturę, rozwiązanie umowy, wygaśnięcie kontraktu)

2.3 Polityka obejmuje:

2.3.1 Dostęp logiczny (systemy, aplikacje, chmura, VPN)

2.3.2 Dostęp fizyczny (identyfikatory, klucze, systemy kontroli wejścia do budynków)

2.3.3 Przypisane aktywa (laptopy, telefony, tokeny, dane uwierzytelniające)

2.3.4 Potwierdzenie zapoznania się z politykami i obowiązkami zachowania poufności

2.4 Wszystkie działy (HR, IT, administracja obiektami, bezpieczeństwo i kierownictwo) odpowiadają za realizację swoich ról w procesach wdrażania i zakończenia współpracy.

3. Cele

3.1 Zapewnienie, że wszystkim członkom personelu przyznaje się dostęp wyłącznie po spełnieniu wymagań dotyczących bezpieczeństwa, szkoleń i warunków umownych.

3.2 Odebranie uprawnień dostępowych i odzyskanie aktywów organizacji niezwłocznie po zmianie roli lub zakończeniu współpracy.

3.3 Zachowanie poufności, integralności i dostępności aktywów organizacji w trakcie zmian personalnych.

3.4 Wspieranie wykazania zgodności i obrony prawnej poprzez prowadzenie kompletnych rejestrów zdarzeń związanych z wdrażaniem i zakończeniem współpracy.

3.5 Ograniczenie narażenia na zagrożenia wewnętrzne poprzez weryfikowanie i dokumentowanie wszystkich zdarzeń dostępowych związanych z personelem.

3.6 Dostosowanie cyklu życia personelu w organizacji do opartych na ryzyku praktyk bezpieczeństwa i wymogów regulacyjnych.

4. Role i obowiązki

4.1 Kadra zarządzająca

4.1.1 Zatwierdza niniejszą politykę oraz zapewnia uprawnienia i zasoby niezbędne do realizacji procesów wdrażania, zakończenia współpracy i kontroli dostępu.

4.1.2 Zapewnia, że zmiany personalne nie narażają organizacji na nadmierne ryzyko bezpieczeństwa ani ryzyko prawne.

4.2 Dział zasobów ludzkich (HR)

4.2.1 Inicjuje procesy wdrażania i zakończenia współpracy dla pracowników oraz powiadamia właściwe działy o zmianach.

4.2.2 Zapewnia, że weryfikacja przeszłości, umowy, NDA oraz potwierdzenia zapoznania się z politykami są zakończone przed przyznaniem dostępu.

4.2.3 Informuje IT i administrację obiektami o odejściach pracowników zgodnie z uzgodnionym SLA dotyczącym powiadomień.

4.2.4 Współpracuje z działem prawnym w celu egzekwowania obowiązków po zakończeniu zatrudnienia (np. klauzul poufności).

[... 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 Częstotliwość przeglądu polityki

9.1.1 Niniejsza polityka musi być poddawana przeglądowi:

9.1.1.1 Corocznie, lub

9.1.1.2 Po każdym istotnym incydencie związanym z niewłaściwym użyciem dostępu, utratą aktywów lub niepowodzeniem proceduralnym

9.1.1.3 Przy wdrażaniu istotnych zmian w HR lub platformie IAM

9.1.1.4 Po aktualizacjach regulacyjnych lub prawnych wpływających na dane personelu lub obowiązki

9.2 Proces przeglądu i odpowiedzialność

9.2.1 Menedżer SZBI i Dyrektor HR koordynują przegląd przy udziale bezpieczeństwa IT, działu prawnego i zgodności.

9.2.2 Wszystkie zmiany muszą zostać zatwierdzone przez kadrę zarządzającą i Komitet Sterujący SZBI.

9.2.3 Zmienione wersje muszą zostać ponownie przekazane właściwym działom i personelowi do ponownego potwierdzenia.

9.3 Nadzór nad dokumentem i okres przechowywania

9.3.1 Niniejsza polityka musi zawierać:

9.3.2 Kontrolę wersji, historię zmian i datę wejścia w życie

9.3.3 Właściciela dokumentu i osoby dokonujące przeglądu

9.3.4 Klasyfikację polityki i zapis zatwierdzenia

9.3.5 Nieaktualne wersje muszą być archiwizowane przez co najmniej 3 lata zgodnie z Polityką zarządzania dokumentacją.

10. Powiązane polityki i zależności

10.1.1 Niniejsza polityka jest bezpośrednio powiązana z:

10.1.2 P1 – Polityka bezpieczeństwa informacji: Określa cele bezpieczeństwa organizacji, w tym nadzór nad dostępem personelu.

10.1.3 P4 – Polityka kontroli dostępu: Określa wymagania operacyjne dotyczące nadawania i odbierania dostępu do systemów oraz dostępu fizycznego na podstawie zdarzeń wdrożenia i zakończenia współpracy.

10.1.4 P3 – Polityka dopuszczalnego użytkowania: Wymaga potwierdzenia podczas wdrożenia i wspiera egzekwowanie postanowień po zakończeniu współpracy.

10.1.5 P6 – Polityka zarządzania ryzykiem: Zapewnia ocenę i ograniczanie ryzyk związanych z dostępem użytkowników i zmianami personalnymi zgodnie z zasadami SZBI.

10.1.6 P11 – Polityka zarządzania kontami użytkowników i uprawnieniami: Reguluje techniczne środki kontrolne nadawania i odbierania dostępu na potrzeby niniejszej polityki.

10.2 Polityki te tworzą zintegrowany system środków kontrolnych służący bezpiecznemu i rozliczalnemu zarządzaniu zdarzeniami w cyklu życia personelu.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo ramami bezpieczeństwa, ochrony prywatności i ładu IT, aby zapewnić, że procesy wdrażania i zakończenia współpracy są bezpieczne, audytowalne oraz zgodne z wymaganiami prawnymi i organizacyjnymi.

11.2 ISO/IEC 27001:

11.2.1 Klauzula 7.2 – Kompetencje oraz Klauzula 6.2 – Cele bezpieczeństwa informacji: Niniejsza polityka wspiera zapewnienie kompetencji personelu oraz bezpieczne wdrażanie osób do ról, w których wpływają one na cele SZBI.

11.2.2 Środek kontrolny 6.5 załącznika A – Obowiązki po zakończeniu zatrudnienia lub zmianie warunków zatrudnienia: Niniejsza polityka w pełni egzekwuje środki kontrolne dotyczące pozostałych uprawnień dostępowych, pieczy nad danymi oraz obowiązków umownych po odejściu.

11.2.3 Środek kontrolny 5.9 załącznika A – Weryfikacja oraz 6.2 – Warunki zatrudnienia: Procedury wdrożeniowe obejmują mechanizmy weryfikacji przeszłości oraz potwierdzania zapoznania się z politykami zgodnie z tymi klauzulami.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Zakończenie zatrudnienia personelu) oraz PS-5 (Przeniesienie personelu): Niniejsza polityka egzekwuje uporządkowane usuwanie lub modyfikowanie uprawnień dostępowych, identyfikatorów fizycznych i aktywów.

11.3.2 AC-2 (Zarządzanie kontami) oraz AC-6 (Najmniejsze uprawnienia): Postanowienia zapewniają zgodność dostępu z rolą oraz jego szybkie odebranie, gdy przestaje być potrzebny.

11.3.3 IA-4 (Zarządzanie identyfikatorami) oraz IA-5 (Zarządzanie mechanizmami uwierzytelniania): Wspiera bezpieczne zarządzanie danymi uwierzytelniającymi w trakcie i po zmianach personalnych.

11.3.4 CM-5 (Ograniczenia dostępu przy zmianach): Zapobiega nieuprawnionym zmianom po zakończeniu współpracy poprzez cofnięcie podwyższonych uprawnień dostępowych.

11.3.5 AU-2 oraz AU-6: Rejestrowanie zdarzeń i możliwość prześledzenia zdarzeń dostępowych są wzmacniane poprzez integrację IAM i ścieżkę audytową.

11.4 RODO (2016/679):

11.4.1 Artykuł 5(1)(f): Chroni dane osobowe przed nieuprawnionym dostępem, co jest tutaj realizowane poprzez odebranie dostępu użytkownika w procesie zakończenia współpracy.

11.4.2 Artykuł 32: Nakłada obowiązek stosowania odpowiednich technicznych i organizacyjnych środków kontrolnych w celu zabezpieczenia danych osobowych w całym cyklu zatrudnienia.

11.4.3 Artykuł 25 – Ochrona danych w fazie projektowania: Zapewnia, że wdrażanie i zakończenie współpracy obejmują minimalizację danych, okres retencji i zgodne z prawem środki kontroli dostępu.

11.4.4 Motyw 39: Podkreśla ograniczenie dostępu i poufność, wspierane przez strukturę niniejszej polityki.

11.5 Dyrektywa NIS2 (2022/2555):

11.5.1 Artykuł 21(2)(b, c, d): Wymaga środków bezpieczeństwa dotyczących personelu i działań operacyjnych odnoszących się do kontroli dostępu, ograniczania zagrożeń wewnętrznych oraz procesów cyklu życia, co znajduje odzwierciedlenie w niniejszej polityce.

11.6 Rozporządzenie DORA (2022/2554):

11.6.1 Artykuł 5 – Ład organizacyjny i kontrola wewnętrzna: Niniejsza polityka wspiera wewnętrzny ład ICT związany z ryzykiem ludzkim i zarządzaniem dostępem.

11.6.2 Artykuł 8 – Zarządzanie ryzykiem ICT: Stosuje środki kontrolne do zmian personalnych, które mogą narazić aktywa krytyczne lub środowiska regulowane.

11.6.3 Artykuł 9 – Klasyfikacja incydentów i zarządzanie incydentami: Zapewnia, że naruszenia związane z zakończeniem współpracy podlegają zgłoszeniu i ograniczeniu poprzez właściwe odebranie dostępu i postępowanie z aktywami.

11.7 COBIT 2019:

11.7.1 APO07 – Zarządzane zasoby ludzkie: Definiuje role, obowiązki i działania w cyklu życia związane z wdrażaniem i zakończeniem współpracy zgodnie z celami nadzorczymi.

11.7.2 BAI08 – Zarządzanie wiedzą: Wzmacnia dokumentowanie procedur, zachowanie wiedzy i przekazanie kontroli na koniec zatrudnienia.

11.7.3 DSS05 – Zarządzane usługi bezpieczeństwa: Egzekwuje dezaktywację użytkowników, kontrolę aktywów i rozliczalność podczas zmian ról.

11.7.4 MEA03 – Monitorowanie, ocena i analiza zgodności: Zapewnia ocenę środków kontrolnych dotyczących wdrażania i zakończenia współpracy podczas audytów wewnętrznych i zewnętrznych.