					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P07S					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**

Powiązanie z normami i regulacjami, w stosownych przypadkach

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 6.2, 7	Wymagania dotyczące bezpieczeństwa zasobów ludzkich i podnoszenia świadomości
ISO/IEC 27002:2022	Środki kontrolne 6.2, 6.5	Praktyki bezpieczeństwa dotyczące wdrażania i zakończenia zatrudnienia
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Zakończenie współpracy personelu; cykl życia kont; planowanie
Dyrektywa UE NIS2	Artykuł 21(2)(h)	Bezpieczeństwo zasobów ludzkich i cykl życia dostępu
Rozporządzenie UE DORA	Artykuł 12	Kontrola dostępu i cofanie uprawnień dostępu do systemów ICT
COBIT 2019	APO07, DSS01	Bezpieczeństwo personelu, kontrola dostępu logicznego i fizycznego
RODO	Artykuł 32	Bezpieczeństwo danych osobowych w trakcie zatrudnienia

1. Cel

1.1 Niniejsza polityka określa proces wdrażania nowych pracowników lub kontraktorów oraz bezpiecznego usuwania dostępu w przypadku odejścia danej osoby lub zmiany pełnionej przez nią roli.

1.2 Zapewnia ona, że dostęp jest nadawany zgodnie z zasadą najmniejszych uprawnień, wszystkie aktywa są rozliczane, a działania krytyczne, takie jak dezaktywacja kont i odzyskiwanie danych, są realizowane terminowo.

1.3 Niniejsza polityka wspiera zgodność, integralność operacyjną oraz ochronę danych poprzez ustrukturyzowane i audytowalne działania związane z wdrażaniem i zakończeniem współpracy.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników stałych i tymczasowych,

2.1.2 kontraktorów, konsultantów i stażystów,

2.1.3 zewnętrznych dostawców usług posiadających dostęp do systemów lub dostęp fizyczny.

2.2 Obejmuje ona:

2.2.1 wdrażanie: tworzenie kont użytkowników, nadawanie dostępu, wydawanie sprzętu,

2.2.2 zakończenie współpracy: usuwanie dostępu, odzyskiwanie aktywów organizacji oraz bezpieczne zamykanie tożsamości cyfrowych,

2.2.3 wewnętrzne zmiany ról wymagające rekonfiguracji dostępu lub ponownego przypisania aktywów.

2.3 Ma zastosowanie do wszystkich urządzeń, platform i lokalizacji wykorzystywanych do realizacji oficjalnych zadań biznesowych.

3. Cele

3.1 Zapewnienie, że nowy personel otrzymuje dostęp i zasoby na podstawie zweryfikowanych ról i odpowiedzialności.

3.2 Potwierdzenie, że użytkownicy kończący współpracę są całkowicie usuwani z systemów i obiektów najpóźniej do końca ich ostatniego dnia pracy.

3.3 Zapobieganie sytuacjom, w których osierocone konta oraz niezwrócone aktywa stwarzają ryzyko bezpieczeństwa.

3.4 Utrzymywanie udokumentowanych zapisów dotyczących wdrażania, transferów wewnętrznych i zakończenia współpracy.

3.5 Wspieranie rozliczalności poprzez stosowanie list kontrolnych i koordynację ról między funkcjami.

4. Role i obowiązki

4.1 Dyrektor Generalny

4.1.1 Zatwierdza dostęp dla ról o wysokich uprawnieniach i nadzoruje program wdrażania oraz zakończenia współpracy.

4.1.2 Zapewnia, że odstępstwa są uzasadnione, a działania korygujące podejmowane, gdy procesy nie są przestrzegane.

4.2 Office Manager / dział kadr (HR)

4.2.1 Inicjuje wdrażanie nowych pracowników i powiadamia IT o odejściach.

4.2.2 Zapewnia zakończenie formalności prawnych (np. umowy o zachowaniu poufności) oraz uzyskanie potwierdzeń zapoznania się z politykami bezpieczeństwa.

4.2.3 Utrzymuje listy kontrolne przyjęcia i zakończenia zatrudnienia oraz monitoruje zgodność z polityką.

[... 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

9.1.1 Niniejsza polityka musi być przeglądana co najmniej raz w roku przez Dyrektora Generalnego oraz osoby odpowiedzialne po stronie HR i IT.

9.2 Wcześniejsze przesłanki przeglądu

9.2.1 Aktualizacje muszą zostać wprowadzone, jeżeli:

9.2.1.1 wdrożono nowe systemy HR lub IT,

9.2.1.2 nastąpiła zmiana zewnętrznego dostawcy usług IT lub dostawcy zarządzanych usług HR,

9.2.1.3 audyty bezpieczeństwa ujawnią luki procesowe,

9.2.1.4 zmienią się obowiązki regulacyjne (np. aktualizacje RODO),

9.2.1.5 wystąpi krytyczna nieskuteczność procesu zakończenia współpracy lub naruszenie bezpieczeństwa.

9.3 Kontrola wersji i zatwierdzanie

9.3.1 Każda wersja niniejszej polityki musi zawierać:

9.3.1.1 numer wersji i datę,

9.3.1.2 podsumowanie zmian,

9.3.1.3 zatwierdzenie przez Dyrektora Generalnego,

9.3.1.4 zarchiwizowane poprzednie wersje przechowywane przez co najmniej trzy lata.

9.4 Komunikacja i potwierdzenie zapoznania się

9.4.1 Wszyscy pracownicy odpowiedzialni za wdrażanie lub zakończenie współpracy muszą zostać powiadomieni o każdej aktualizacji polityki. Coroczne działania uświadamiające lub szkolenia przypominające są obowiązkowe.

10. Polityki powiązane i zależności

10.1 Niniejsza polityka wspiera i jest wspierana przez:

10.1.1 P2S – Polityka ról i obowiązków w ramach ładu organizacyjnego: zapewnia rozliczalność w procesach nadawania dostępu i wdrażania,

10.1.2 P4S – Polityka kontroli dostępu: ustanawia techniczne mechanizmy nadawania dostępu w oparciu o role i dezaktywacji,

10.1.3 P6S – Polityka zarządzania ryzykiem: ocenia ryzyka wynikające z nieskuteczności kontroli w procesach wdrażania i zakończenia współpracy,

10.1.4 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: ustanawia wymagania dotyczące wprowadzenia personelu podczas wdrażania,

10.1.5 P30S – Polityka reagowania na incydenty: traktuje brak odebrania uprawnień dostępu lub kradzież aktywów jako incydenty bezpieczeństwa.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.2 – określa wymagania dotyczące bezpieczeństwa zasobów ludzkich.

11.1.2 Klauzula 7.2 – nakłada obowiązek przeprowadzenia szkoleń uświadamiających dla nowego personelu.

11.2 ISO/IEC 27002

11.2.1 Środki kontrolne 6.2 i 6.5 – określają praktyki bezpieczeństwa dotyczące wdrażania i zakończenia zatrudnienia.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – procedury zakończenia współpracy personelu, w tym dezaktywacja dostępu.

11.3.2 AC-2 – zapewnia zarządzanie cyklem życia kont dla dostępu użytkowników.

11.3.3 PL-4 – wymaga planowania zmian personelu.

11.4 RODO

11.4.1 Artykuł 32 – zapewnia odpowiednie bezpieczeństwo w trakcie i po zakończeniu zatrudnienia, w szczególności w odniesieniu do dostępu do danych osobowych.

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21(2)(h) – wymaga środków kontroli bezpieczeństwa zasobów ludzkich oraz cyklu życia dostępu.

11.6 Rozporządzenie UE DORA

11.6.1 Artykuł 12 – wymaga, aby regulowane podmioty finansowe kontrolowały dostęp personelu do systemów ICT, w tym stosowały procedury cofania uprawnień dostępu.

11.7 COBIT 2019

11.7.1 APO07 – Zarządzanie zasobami ludzkimi: ustanawia wymagania bezpieczeństwa dla cyklu życia personelu.

11.7.2 DSS01 – Zarządzanie operacjami: obejmuje kontrolę dostępu logicznego i fizycznego podczas zmian statusu zatrudnienia.