					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P26					Tytuł dokumentu: **Polityka bezpieczeństwa dostawców i stron trzecich**							
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 8	Planowanie operacyjne i nadzór operacyjny: wymaga formalnych zabezpieczeń w odniesieniu do usług stron trzecich wpływających na System Zarządzania Bezpieczeństwem Informacji (SZBI)
ISO/IEC 27002:2022	Środki kontrolne 5.19–5.22	Polityki i procedury dotyczące relacji z dostawcami; zarządzanie ryzykiem dostawców; zarządzanie świadczeniem usług przez dostawców; monitorowanie i przegląd dostawców
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Usługi systemów zewnętrznych; zarządzanie konfiguracją przez deweloperów; połączenia międzysystemowe; bezpieczeństwo personelu stron trzecich
RODO	Artykuły 28, 32, 33	Obowiązki podmiotu przetwarzającego, bezpieczeństwo przetwarzania, zgłaszanie naruszenia ochrony danych osobowych
NIS2	Artykuł 21(2)(e–f)	zarządzanie dostawcami oparte na ryzyku oraz nadzór nad bezpieczeństwem
DORA	Artykuły 28, 30	ryzyko ICT związane ze stronami trzecimi, nadzór nad krytycznymi zewnętrznymi dostawcami ICT
COBIT 2019	BAI05, DSS02, MEA03	Zarządzanie wdrażaniem zmian organizacyjnych; zarządzanie zgłoszeniami serwisowymi i incydentami; monitorowanie, ocena i potwierdzanie zgodności

1. Cel

1.1 Niniejsza polityka określa wymagania bezpieczeństwa informacji dotyczące ustanawiania, zarządzania i utrzymywania bezpiecznych relacji z dostawcami i zewnętrznymi usługodawcami.

1.2 Zapewnia, że wszyscy dostawcy mający dostęp do danych, systemów lub infrastruktury organizacji podlegają rygorystycznym środkom kontroli bezpieczeństwa, zabezpieczeniom umownym oraz stałemu nadzorowi przez cały cykl życia usługi.

1.3 Polityka wspiera środki kontrolne 5.19–5.22 załącznika A do ISO/IEC 27001 poprzez uwzględnienie wymagań bezpieczeństwa w procesach zakupowych, wdrożeniowych, due diligence dostawców, zarządzania umowami, monitorowania usług oraz zakończenia współpracy.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich dostawców zewnętrznych, kontraktorów, dostawców usług chmurowych oraz organizacji świadczących usługi, które przetwarzają aktywa informacyjne organizacji lub uzyskują do nich dostęp

2.1.2 wszystkich ról wewnętrznych zaangażowanych w ocenę dostawców, wdrożenie, zawieranie umów, zarządzanie ryzykiem, monitorowanie lub zakończenie współpracy

2.1.3 wszystkich relacji z dostawcami obejmujących dostęp do danych wrażliwych, integrację z usługami produkcyjnymi lub wsparcie krytycznych funkcji biznesowych

2.2 Polityka obejmuje, w stosownych przypadkach, zarówno dostawców bezpośrednich, jak i ich podwykonawców, a także oprogramowanie podmiotów trzecich, infrastrukturę, wsparcie i usługi zarządzane.

3. Cele

3.1 Zapewnienie, że ryzyka bezpieczeństwa związane z dostawcami są konsekwentnie identyfikowane, oceniane i ograniczane przez cały cykl życia relacji.

3.2 Uwzględnienie standardowych wymagań bezpieczeństwa we wszystkich umowach z dostawcami, w tym obowiązków zgłaszania naruszeń, postanowień dotyczących prawa do audytu oraz obowiązków w zakresie ochrony danych.

3.3 Wymaganie formalnego due diligence dostawców i udokumentowanych ocen ryzyka przed zaangażowaniem nowych dostawców lub odnowieniem umów o świadczenie usług wysokiego ryzyka.

3.4 Ustanowienie mechanizmów ciągłego monitorowania zgodności dostawców, w tym przeglądów wydajności, audytów i eskalacji incydentów.

3.5 Zarządzanie zmianami w usługach dostawców oraz zapewnienie bezpiecznego zakończenia współpracy i zwrotu lub zniszczenia danych przy rozwiązaniu umowy.

3.6 Dostosowanie środków kontroli bezpieczeństwa stron trzecich do mających zastosowanie obowiązków regulacyjnych i umownych, w tym RODO, NIS2, DORA oraz norm ISO/IEC 27001.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia jej zgodność z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI), procesem zarządzania ryzykiem oraz strategią zgodności.

4.1.2 Zatwierdza poziomy klasyfikacji dostawców, wyniki przeglądów bezpieczeństwa oraz wyjątki wysokiego ryzyka.

4.1.3 Uczestniczy w eskalacji poważnych incydentów dotyczących dostawców oraz w negocjacjach umownych dotyczących usług krytycznych.

4.2 Zakupy i zarządzanie dostawcami

4.2.1 Zapewniają, że wszystkie nowe i odnawiane umowy z dostawcami zawierają zatwierdzone klauzule bezpieczeństwa i ochrony danych.

4.2.2 Utrzymują scentralizowany rejestr dostawców i koordynują z funkcją prawną i zgodności dokumentację ryzyka strony trzeciej.

4.2.3 Inicjują procesy wdrożeniowe i zapewniają ich zgodność z ocenami bezpieczeństwa przeprowadzanymi przed zawarciem umowy.

[... 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 lub wcześniej w przypadku:

9.1.1 istotnych zmian strategii zakupowej lub ekosystemu dostawców

9.1.2 aktualizacji ram prawnych lub regulacyjnych (np. DORA, RODO)

9.1.3 poważnych incydentów dotyczących stron trzecich, naruszeń ochrony danych lub nieskuteczności audytu

9.1.4 ustaleń wynikających z ocen ryzyka lub pochodzących od zewnętrznych jednostek certyfikujących

9.2 Za proces przeglądu wspólnie odpowiadają Dyrektor ds. Bezpieczeństwa Informacji (CISO), zakupy, dział prawny i compliance oraz funkcje zarządzania ryzykiem.

9.3 Wszystkie zmiany polityki muszą być udokumentowane w Rejestrze kontroli dokumentów SZBI, objęte kontrolą wersji oraz przekazane odpowiednim interesariuszom za pośrednictwem kanałów nadzoru nad dostawcami i programów podnoszenia świadomości pracowników.

9.4 Wersje wycofane z użycia muszą być archiwizowane przez minimum trzy lata dla zapewnienia identyfikowalności i zgodności z wymaganiami prawnymi.

10. Powiązane polityki i odniesienia

10.1 P1 – Polityka bezpieczeństwa informacji. Określa nadrzędne zobowiązanie do zabezpieczenia wszystkich operacji organizacji, w tym tych realizowanych z udziałem dostawców zewnętrznych i zewnętrznych usługodawców.

10.2 P6 – Polityka zarządzania ryzykiem. Określa zasady identyfikacji, oceny i ograniczania ryzyk związanych z relacjami ze stronami trzecimi, w tym ryzyk odziedziczonych lub systemowych wynikających z ekosystemów dostawców.

10.3 P17 – Polityka ochrony danych i prywatności. Ma zastosowanie do wszystkich dostawców przetwarzających dane osobowe i wymaga odpowiednich postanowień umownych, zabezpieczeń transferu oraz zasad privacy by design.

10.4 P4 – Polityka kontroli dostępu. Reguluje sposób, w jaki personel stron trzecich uzyskuje dostęp do systemów organizacji, wymuszając uprawnienia oparte na rolach, kontrolę sesji oraz procedury cofnięcia dostępu.

10.5 P22 – Polityka logowania i monitorowania. Wymaga, aby dostęp dostawców do systemów był monitorowany, rejestrowany i przeglądany, w szczególności w środowiskach, w których występują działania uprzywilejowane lub operacje na danych.

10.6 P30 – Polityka reagowania na incydenty (P30). Określa procedury eskalacji oraz wymagania dotyczące zgłaszania naruszeń dla zdarzeń bezpieczeństwa informacji pochodzących od dostawcy lub wspólnych dochodzeń obejmujących systemy stron trzecich.

11. Normy referencyjne i ramy odniesienia

11.1 ISO/IEC 27001: Klauzula 8.1 – Planowanie operacyjne i nadzór operacyjny: wymaga formalnych zabezpieczeń w odniesieniu do usług stron trzecich wpływających na SZBI.

11.2 ISO/IEC 27002:2022 – Środki kontrolne 5.19 do 5.22:

11.2.1 Środek kontrolny 5.19 załącznika A – polityki i procedury dotyczące relacji z dostawcami: nakłada obowiązek stosowania środków kontroli na potrzeby zarządzania interakcjami z dostawcami.

11.2.2 Środek kontrolny 5.20 załącznika A – zarządzanie ryzykiem dostawców: koncentruje się na identyfikacji, ocenie oraz bieżącym nadzorze nad profilem ryzyka w obszarze bezpieczeństwa dostawców.

11.2.3 Środek kontrolny 5.21 załącznika A – zarządzanie świadczeniem usług przez dostawców: wymaga zgodności parametrów wydajności i bezpieczeństwa z oczekiwaniami umownymi.

11.2.4 Środek kontrolny 5.22 załącznika A – monitorowanie i przegląd dostawców: wzmacnia potrzebę bieżącej walidacji i ponownej oceny zgodności stron trzecich.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – usługi systemów zewnętrznych: określa wymagania bezpieczeństwa i ryzyka dla systemów obsługiwanych przez podmioty zewnętrzne.

11.3.2 SA-10 – zarządzanie konfiguracją przez deweloperów: ma zastosowanie, gdy strony trzecie dostarczają oprogramowanie lub środowiska.

11.3.3 CA-3 – połączenia międzysystemowe: wymaga nadzoru i uzgodnień dotyczących przepływów danych systemowych pomiędzy podmiotami.

11.3.4 PS-7 – bezpieczeństwo personelu stron trzecich: zapewnia, że kontraktorzy i personel dostawcy są odpowiednio weryfikowani i monitorowani.

11.4 RODO (UE 2016/679):

11.4.1 Artykuł 28 – obowiązki podmiotu przetwarzającego: wymaga pisemnych umów z podmiotami przetwarzającymi dane, obejmujących środki techniczne i organizacyjne (TOM).

11.4.2 Artykuł 32 – bezpieczeństwo przetwarzania: nakłada obowiązek stosowania odpowiednich środków bezpieczeństwa zarówno przez administratorów, jak i podmioty przetwarzające.

11.4.3 Artykuł 33 – zgłaszanie naruszenia ochrony danych osobowych: wymaga niezwłocznego powiadomienia od dostawców w przypadku naruszenia.

11.5 Dyrektywa NIS2 (UE 2022/2555):

11.5.1 Artykuł 21(2)(e–f): wymaga zarządzania dostawcami opartego na ryzyku oraz nadzoru nad bezpieczeństwem, w szczególności w cyfrowych łańcuchach dostaw podmiotów kluczowych i ważnych.

11.6 Rozporządzenie DORA (UE 2022/2554):

11.6.1 Artykuł 28 – ryzyko ICT związane ze stronami trzecimi: nakłada obowiązki dotyczące oceny ryzyka, umownych warunków bezpieczeństwa oraz strategii wyjścia dla dostawców usług finansowych.

11.6.2 Artykuł 30 – nadzór nad krytycznymi zewnętrznymi dostawcami ICT: ustanawia rozszerzone wymagania w zakresie monitorowania i nadzoru wobec kluczowych dostawców.

11.7 COBIT 2019:

11.7.1 BAI05 – zarządzanie wdrażaniem zmian organizacyjnych: zapewnia, że zmiany dotyczące dostawców są nadzorowane w bezpieczny sposób.

11.7.2 DSS02 – zarządzanie zgłoszeniami serwisowymi i incydentami: ma zastosowanie do zgłoszeń raportowanych przez dostawców oraz integracji obsługi incydentów.

11.7.3 MEA03 – monitorowanie, ocena i potwierdzanie zgodności: wzmacnia pomiar wydajności dostawców i monitorowanie zgodności.