					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P41					Tytuł dokumentu: **Polityka zarządzania ryzykiem zależności od dostawców**							
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**

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.
Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.
W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
RODO	Art. 28, Art. 32(1)(d)	
Dyrektywa NIS2	Art. 21(2)(d), Art. 21(3), Art. 22	
Rozporządzenie DORA	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Cel

1.1 Celem niniejszej polityki jest wzmocnienie praktyk bezpieczeństwa łańcucha dostaw w organizacji poprzez ustanowienie procesu identyfikacji i zarządzania krytycznymi zależnościami od dostawców i usługodawców, zgodnie z art. 21 ust. 3 dyrektywy NIS2 oraz ocenami ryzyka łańcucha dostaw prowadzonymi na poziomie Unii.

1.2 Polityka ma zapewnić, że ryzyka wynikające z koncentracji lub uzależnienia od pojedynczych dostawców są identyfikowane i ograniczane oraz że wszelkie sektorowe ryzyka łańcucha dostaw (wskazane przez właściwe organy na podstawie art. 22 dyrektywy NIS2) są uwzględniane w zarządzaniu ryzykiem i planowaniu ciągłości działania.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich kluczowych dostawców i usługodawców, od których organizacja jest zależna w zakresie operacji krytycznych, w szczególności w łańcuchu dostaw ICT (sprzęt, oprogramowanie, chmura obliczeniowa, telekomunikacja, usługi zarządzane).

2.2 Obejmuje ona funkcje wewnętrzne, w tym zakupy, zarządzanie dostawcami, zarządzanie ryzykiem oraz odpowiednie działy operacyjne. Obejmuje również samych dostawców w zakresie niezbędnym do pozyskiwania informacji o ryzyku. „Dostawcy krytyczni” to dostawcy, których nieskuteczność, niedostępność lub naruszenie bezpieczeństwa mogłyby istotnie wpłynąć na zdolność organizacji do świadczenia usług lub wywiązywania się z obowiązków prawnych.

3. Cele

3.1 Uzyskanie pełnej widoczności zależności w łańcuchu dostaw, w szczególności poprzez identyfikację pojedynczych punktów awarii lub wysokiego ryzyka koncentracji w bazie dostawców (np. zależności od jednego dostawcy usług chmurowych dla wszystkich usług).

3.2 Wdrożenie środków ograniczających i zarządzających ryzykiem związanym z dostawcami, takich jak dywersyfikacja, plany awaryjne lub wymaganie wzmocnienia zabezpieczeń po stronie dostawców, aby zwiększyć odporność na awarie dostawców lub ataki pochodzące z łańcucha dostaw.

3.3 Zapewnienie zgodności z wymaganiami dyrektywy NIS2 poprzez włączenie wyników wszelkich skoordynowanych ocen ryzyka bezpieczeństwa krytycznych łańcuchów dostaw (zgodnie z art. 22) do decyzji w zakresie ryzyka w organizacji oraz przez zapewnienie, że podejście do ryzyka łańcucha dostaw jest udokumentowane i możliwe do wykazania.

4. Role i odpowiedzialności

4.1 Biuro Zarządzania Dostawcami (VMO): odpowiada za rejestr zależności od dostawców i koordynuje oceny ryzyka. Zapewnia, że podczas wdrożenia dostawcy oraz okresowo po jego zakończeniu każdy kluczowy dostawca jest oceniany pod kątem krytyczności i poziomu zależności.

4.2 Funkcja zarządzania ryzykiem (Komitet ds. Ryzyka Przedsiębiorstwa): dokonuje przeglądu ryzyka koncentracji i analiz zależności, zatwierdza strategie postępowania z ryzykiem (np. akceptuje dodanie alternatywnego dostawcy lub utrzymywanie dodatkowych zapasów komponentów krytycznych). Włącza ryzyko łańcucha dostaw do rejestru ryzyk i raportuje do najwyższego kierownictwa.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Monitorowanie i audyt

9.1 Rejestr zależności oraz oceny ryzyka będą podlegały corocznemu audytowi wewnętrznemu. Funkcja audytu wewnętrznego / zgodności zweryfikuje, czy wszyscy dostawcy krytyczni są ujęci, czy ich oceny ryzyka są aktualne oraz czy plany ograniczania ryzyka istnieją i są realizowane. Sprawdzi również, czy zewnętrzne dane wejściowe z ocen ryzyka (raporty na podstawie art. 22 itd.) zostały należycie uwzględnione.

9.2 Skuteczność środków dywersyfikacji i działań awaryjnych będzie okresowo testowana. Przykładowo może zostać przeprowadzona planowana symulacja, w której zakłada się awarię głównego dostawcy, aby przetestować plany ciągłości działania i rozwiązania alternatywne (analogicznie do ćwiczenia DR, lecz dla niedostępności dostawcy). Wyniki tych testów są dokumentowane, a wszelkie stwierdzone słabości usuwane.

9.3 Metryki: funkcja zarządzania ryzykiem będzie śledzić takie wskaźniki jak „% usług krytycznych z co najmniej jednym dostawcą alternatywnym lub dostępnym rozwiązaniem zastępczym” albo „5 największych zależności od dostawców i trend ich ryzyka”. Wskaźniki te będą uwzględniane w panelach ryzyka przekazywanych kierownictwu. Trend spadkowy ryzyka zależności w czasie jest celem; jeżeli wskaźniki pokażą wzrost zależności, musi to wywołać dyskusję na poziomie kierownictwa.

10. Przegląd i utrzymanie

10.1 Niniejsza polityka będzie podlegała przeglądowi co najmniej raz w roku przez zespoły zarządzania dostawcami i zarządzania ryzykiem. Przegląd będzie uwzględniał wszelkie zmiany w krajobrazie dostawców (np. gdy nowy dostawca stanie się krytyczny lub dotychczasowy zostanie wycofany) oraz wszelkie nowe wymagania regulacyjne dotyczące outsourcingu lub ryzyka strony trzeciej.

10.2 Jeżeli organy sektorowe opublikują zaktualizowane wytyczne lub jeśli incydent ujawni luki (na przykład gdy niedostępność dostawcy miała większy wpływ niż przewidywano, co wskazuje, że ocena ryzyka błędnie oszacowała zależność), polityka zostanie zaktualizowana w celu doprecyzowania kryteriów lub strategii ograniczania ryzyka.

10.3 Zmienione wersje polityki muszą zostać zatwierdzone przez najwyższe kierownictwo. Istotne zmiany zostaną zakomunikowane wszystkim odpowiednim działom, a materiały szkoleniowe zostaną odpowiednio zaktualizowane tak, aby odzwierciedlały nowe procedury lub normy.

11. Polityki powiązane i odniesienia

11.1 P01 – Polityka bezpieczeństwa informacji. Przypisuje rozliczalność za nadzór nad zależnościami od dostawców.

11.2 P02 – Polityka ról i odpowiedzialności w ramach ładu zarządczego. Doprecyzowuje właścicielstwo decyzji dotyczących ryzyka dostawców.

11.3 P06 – Polityka zarządzania ryzykiem. Włącza ryzyko koncentracji do korporacyjnego rejestru ryzyk.

11.4 P26 – Polityka bezpieczeństwa dostawców i stron trzecich. Ustanawia bazowy poziom bezpieczeństwa; P41 dodaje środki kontrolne dotyczące zależności i koncentracji.

11.5 P27 – Polityka korzystania z chmury obliczeniowej. Stosuje kryteria zależności do wdrażania usług w chmurze obliczeniowej i planów wyjścia.

11.6 P28 – Polityka rozwoju oprogramowania w modelu outsourcingowym. Obejmuje ryzyka zależności w zewnętrznych pracach inżynieryjnych.

11.7 P32 – Polityka ciągłości działania i odtwarzania po awarii. Obejmuje planowanie dla scenariuszy niedostępności dostawcy lub jego zastąpienia.

11.8 P37 – Polityka zgodności prawnej i regulacyjnej. Zapewnia, że umowy i obowiązki odzwierciedlają środki kontrolne dotyczące zależności.

12. Odniesienia

12.1 Dyrektywa NIS2 (UE 2022/2555), art. 21 ust. 3 (wymagający uwzględnienia podatności właściwych dla każdego bezpośredniego dostawcy/usługodawcy oraz jakości ich cyberbezpieczeństwa, w tym wyników skoordynowanych ocen ryzyka łańcucha dostaw)

12.2 Dyrektywa NIS2, art. 22 ust. 1 (skoordynowane na poziomie Unii oceny ryzyka bezpieczeństwa krytycznych łańcuchów dostaw – informujące podmioty o ryzykach sektorowych związanych z dostawcami)

12.3 Rozporządzenie wykonawcze Komisji (UE) 2024/2690, załącznik, sekcja 5 (wymagania bezpieczeństwa łańcucha dostaw dla podmiotów, w tym kryteria wyboru dostawców, dywersyfikacji i obowiązków umownych)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – zalecenia dotyczące identyfikacji dostawców krytycznych i zarządzania powiązanymi ryzykami

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022