					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P26S					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	Środki operacyjne dotyczące relacji ze stronami trzecimi i dostawcami
ISO/IEC 27002:2022	Środki kontrolne 5.19–5.22	Środki kontrolne dotyczące bezpieczeństwa dostawców, umownych warunków bezpieczeństwa, zarządzania zmianą, monitorowania i przeglądu
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Pozyskiwanie, konfiguracja, uzgodnienia dotyczące połączeń między systemami oraz kontrole dotyczące personelu zewnętrznego
RODO	Artykuły 28, 32	umowa powierzenia przetwarzania danych, wymagania bezpieczeństwa dla podmiotów przetwarzających
Dyrektywa NIS2	Artykuły 21(2)(a)(b)(i), 23(1)	zarządzanie ryzykiem w łańcuchu dostaw, nadzór nad usługami stron trzecich
Rozporządzenie DORA	Artykuły 5(1)(2), 28(1)(2)	zarządzanie ryzykiem ICT dotyczącym dostawców usług stron trzecich
COBIT 2019	APO10, APO12, DSS05	zarządzanie dostawcami i integracja ryzyka

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe wymagania bezpieczeństwa dotyczące nawiązywania, zarządzania oraz kończenia relacji ze stronami trzecimi i dostawcami, którzy uzyskują dostęp do danych, systemów lub usług organizacji albo wywierają na nie wpływ.

1.2 Zapewnia ona, że podmioty zewnętrzne — w tym dostawca wsparcia IT, operatorzy usług chmurowych, programiści oprogramowania oraz kontraktorzy realizujący procesy biznesowe — postępują z aktywami organizacji w sposób bezpieczny i zgodny z mającymi zastosowanie przepisami oraz normami.

1.3 Niniejsza polityka ogranicza ryzyka, takie jak wycieki danych, nieuprawnione zmiany w systemach, kary regulacyjne lub zakłócenia działalności spowodowane przez niebezpieczne lub niewłaściwie nadzorowane modele współpracy ze stronami trzecimi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich stron trzecich, które:

2.1.1 Dostarczają oprogramowanie, infrastrukturę, usługi hostingowe lub usługi chmurowe

2.1.2 Uzyskują dostęp do systemów wewnętrznych, urządzeń lub aplikacji albo nimi zarządzają

2.1.3 Przetwarzają dane organizacji, dokumenty lub dane z kopii zapasowych

2.1.4 Wspierają operacje biznesowe, zasoby ludzkie (HR), finanse lub obsługę klienta

2.2 Polityka ma również zastosowanie do:

2.2.1 Personelu wewnętrznego uczestniczącego w wyborze, angażowaniu lub nadzorowaniu dostawców

2.2.2 Każdego członka personelu zarządzającego wdrożeniem dostawcy, umowami, dostępem lub przeglądami

2.2.3 Każdego systemu lub procesu zależnego od komponentów lub usług stron trzecich

3. Cele

3.1 Zapewnienie, że wszyscy dostawcy spełniają jednoznacznie określone oczekiwania w zakresie bezpieczeństwa.

3.2 Wymaganie, aby umowy z dostawcami zawierały egzekwowalne zobowiązania dotyczące bezpieczeństwa, prywatności i reagowania na incydenty.

3.3 Ocena i dokumentowanie ryzyk związanych z dostawcą przed podpisaniem umowy lub nadaniem dostępu.

3.4 Prowadzenie regularnych przeglądów dostawców krytycznych lub wysokiego ryzyka w celu potwierdzenia zgodności.

3.5 Ustanowienie formalnego procesu obsługi odstępstw, zarządzania incydentami i aktualizacji umów.

3.6 Wspieranie zgodności z obowiązkami wynikającymi z ISO/IEC 27001:2022, RODO, NIS2 i DORA w zakresie nadzoru nad dostawcami.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Ponosi ostateczną odpowiedzialność za wybór dostawców i zgodność z wymaganiami bezpieczeństwa

4.1.2 Zatwierdza umowy, odstępstwa i eskalacje dotyczące dostawców

4.1.3 Nadzoruje reagowanie na incydenty oraz podejmowanie decyzji w sytuacji, gdy dostawcy nie spełniają swoich zobowiązań

4.2 Dostawca wsparcia IT lub wewnętrzna osoba kontaktowa ds. bezpieczeństwa

4.2.1 Ocenia techniczny zakres dostępu wnioskowanego przez dostawców

4.2.2 Wdraża zasady kontroli dostępu, przegląda logi oraz weryfikuje bezpieczne postępowanie z danymi

4.2.3 Weryfikuje dowody stosowania środków kontrolnych, certyfikaty bezpieczeństwa lub wyniki audytów (jeżeli dotyczy)

[... 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 poddawana przeglądowi co najmniej raz w roku przez Dyrektora Generalnego, przy udziale dostawcy wsparcia IT lub menedżera dostawców.

9.2 Polityka musi być również poddawana przeglądowi:

9.2.1 Po każdej istotnej zmianie obowiązków prawnych, regulacyjnych lub umownych

9.2.2 Po incydencie bezpieczeństwa związanym z dostawcą lub ustaleniu audytowym

9.2.3 Przy wprowadzaniu nowych kategorii dostawców (np. krytycznych platform SaaS)

9.3 Wszystkie aktualizacje muszą być:

9.3.1 Udokumentowane wraz z historią wersji i uzasadnieniem

9.3.2 Zatwierdzone przez Dyrektora Generalnego

9.3.3 Przekazane odpowiedniemu personelowi wewnętrznemu oraz osobom zarządzającym dostawcami

9.3.4 Przechowywane wraz z poprzednimi wersjami zgodnie z P14S – Polityka retencji i utylizacji danych

10. Powiązane polityki i zależności

10.1 Skuteczność niniejszej polityki zależy od koordynacji z następującymi politykami bezpieczeństwa informacji dla SME:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: przypisuje odpowiedzialność za nadzór nad dostawcami i egzekwowanie postanowień umownych.

10.1.2 P4S – Polityka kontroli dostępu: określa zasady ograniczania dostępu, które muszą być stosowane, gdy dostawcom nadawany jest dostęp do systemów.

10.1.3 P17S – Polityka ochrony danych i prywatności: zapewnia, że dostawcy przetwarzający dane osobowe przestrzegają zasad ochrony danych i wymagań prawnych.

10.1.4 P14S – Polityka retencji i utylizacji danych: ma zastosowanie do wszelkich danych lub zapisów udostępnianych dostawcom lub przez nich przechowywanych i reguluje bezpieczną utylizację po zakończeniu umowy.

10.1.5 P30S – Polityka reagowania na incydenty: określa sposób postępowania, gdy dostawca powoduje incydent bezpieczeństwa lub jest w niego zaangażowany, w tym procedury eskalacji i postępowania z dowodami.

10.2 Polityki te działają łącznie, aby zapewnić kontrolę ryzyka dostawców w całym cyklu życia umowy.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – Wymaga wdrożenia środków operacyjnych, w tym stosowanych wobec relacji ze stronami trzecimi i dostawcami.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 5.19 – Zapewnia, że środki bezpieczeństwa dostawców są zgodne z wymaganiami organizacji.

11.2.2 Środek kontrolny 5.20 – Wymaga formalnych umów obejmujących warunki bezpieczeństwa, odpowiedzialność i obowiązki dotyczące naruszeń.

11.2.3 Środek kontrolny 5.21 – Obejmuje zarządzanie zmianą w usługach dostawców, które mogą wpływać na profil ryzyka w obszarze bezpieczeństwa.

11.2.4 Środek kontrolny 5.22 – Wymaga monitorowania i przeglądu usług dostawców oraz zgodności.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Reguluje pozyskiwanie systemów i usług zewnętrznych, wymagając oceny ryzyka i jasno określonych oczekiwań.

11.3.2 SA-10 – Obejmuje procedury konfiguracji i zmian dotyczące systemów zarządzanych przez strony trzecie.

11.3.3 CA-3 – Wymaga uzgodnień dotyczących połączeń między systemami z udziałem podmiotów zewnętrznych.

11.3.4 PS-7 – Określa wymagania w zakresie weryfikacji i rozliczalności personelu zewnętrznego.

11.4 RODO (2016/679)

11.4.1 Artykuł 28 – Wymaga zawarcia umowy powierzenia przetwarzania danych z dostawcami działającymi jako podmioty przetwarzające.

11.4.2 Artykuł 32 – Nakłada obowiązek stosowania odpowiednich technicznych i organizacyjnych środków bezpieczeństwa przez wszystkie podmioty przetwarzające.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(a), (b), (i) – Wymaga zarządzania ryzykiem w łańcuchu dostaw ICT oraz stosowania kontroli wobec stron trzecich.

11.5.2 Artykuł 23(1) – Wymaga udokumentowanego nadzoru nad usługami stron trzecich dla podmiotów kluczowych i ważnych.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 5(1) – Wymaga ram zarządzania ryzykiem ICT obejmujących wszystkich krytycznych dostawców zewnętrznych.

11.6.2 Artykuł 5(2) – Określa umowne i operacyjne środki kontrolne dla zależności od usług ICT.

11.6.3 Artykuł 28(1), (2) – Ustanawia zasady nadzoru nad ryzykiem ICT stron trzecich w sektorze finansowym.

11.7 COBIT 2019

11.7.1 APO10 – „Zarządzanie dostawcami” określa środki kontroli sourcingu i oczekiwania w zakresie zarządzania relacjami.

11.7.2 APO12 – „Zarządzanie ryzykiem” integruje ryzyko dostawców z organizacyjnym ładem zarządzania ryzykiem.

11.7.3 DSS05 – „Zarządzanie usługami bezpieczeństwa” ma zastosowanie do zarządzanych dostawców zewnętrznych i usług outsourcingowych.