					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P27					Tytuł dokumentu: **Polityka korzystania z chmury obliczeniowej**							
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	Wymagania dotyczące planowania operacyjnego i nadzoru w środowisku chmury obliczeniowej.
ISO/IEC 27002:2022	Zabezpieczenia 5.23–5.25	Wymagania dotyczące korzystania z usług chmurowych, polityki oraz bezpieczeństwa usług chmurowych.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Korzystanie z systemów zewnętrznych, wymagania umowne i techniczne, ochrona kryptograficzna oraz bezpieczeństwo łańcucha dostaw.
RODO	Artykuły 28, 32, Rozdział V	Wymagania wobec podmiotów przetwarzających w chmurze obliczeniowej, bezpieczeństwo przetwarzania oraz transfery danych.
NIS2	Artykuł 21(2)(f, i)	Wymagania dotyczące ryzyka stron trzecich i łańcucha dostaw.
DORA	Artykuły 5(2), 28	Nadzór nad ICT i podmiotami trzecimi (chmura obliczeniowa) dla podmiotów finansowych.
COBIT 2019	BAI04, DSS01, DSS05	Dostępność usług chmurowych, operacje oraz zarządzanie bezpieczeństwem.

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe wymagania organizacji dotyczące bezpiecznego, zgodnego z przepisami i odpowiedzialnego korzystania z usług chmury obliczeniowej w modelach Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oraz Software as a Service (SaaS).

1.2 Celem polityki jest zapewnienie, że usługi chmury obliczeniowej są wdrażane i nadzorowane w sposób chroniący poufność, integralność i dostępność (CIA) aktywów informacyjnych, przy jednoczesnym spełnieniu wymagań regulacyjnych, prawnych i umownych.

1.3 Polityka określa zabezpieczenia służące zarządzaniu ryzykiem związanym z chmurą obliczeniową, ochronie danych, monitorowaniu zgodności dostawców oraz eliminowaniu nieuprawnionego użycia. Wspiera również innowacje biznesowe realizowane z wykorzystaniem platform chmurowych poprzez zapewnienie równowagi między bezpieczeństwem, niezawodnością operacyjną i efektywnością kosztową.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich pracowników, wykonawców, dostawców zewnętrznych oraz konsultantów zewnętrznych, którzy nadają uprawnienia, konfigurują, uzyskują dostęp, administrują lub korzystają z usług chmury obliczeniowej w imieniu organizacji.

2.2 Polityka ma zastosowanie do wszystkich środowisk, w których przetwarzane są dane lub obciążenia organizacji, w tym:

2.2.1 wdrożeń chmury publicznej, prywatnej, hybrydowej i społecznościowej,

2.2.2 wszystkich modeli usług chmurowych (IaaS, PaaS, SaaS),

2.2.3 architektur wielochmurowych i federacyjnych,

2.2.4 wykorzystania shadow IT lub prywatnych kont chmurowych do celów biznesowych.

2.3 Polityka obejmuje wszystkie poziomy klasyfikacji danych i ma zastosowanie zarówno do systemów wewnętrznych, jak i platform utrzymywanych przez dostawcę, na których przechowywane lub przetwarzane są dane należące do organizacji lub dane podlegające regulacjom.

3. Cele

3.1 Zapewnienie bezpiecznego i spójnego wykorzystania technologii chmurowych poprzez jednoznacznie zdefiniowane zasady użytkowania, bazowe zestawy zabezpieczeń i role nadzorcze.

3.2 Ograniczenie ryzyk operacyjnych i regulacyjnych związanych z przetwarzaniem w chmurze obliczeniowej, w tym nieuprawnionego dostępu, naruszeń bezpieczeństwa danych, błędnej konfiguracji, niezgodności oraz zakłóceń świadczenia usług.

3.3 Egzekwowanie wymagań bezpieczeństwa i prywatności wobec wszystkich dostawców usług chmurowych oraz weryfikowanie zgodności za pomocą postanowień umownych, ocen i prawa do audytu.

3.4 Umożliwienie skalowalnego i odpornego wdrażania chmury obliczeniowej bez pogarszania profilu ryzyka bezpieczeństwa, naruszania wymagań prawnych lub ciągłości działania.

3.5 Zapewnienie zgodności nadzoru nad chmurą obliczeniową i jej wykorzystania z ramami SZBI organizacji, obowiązkami prawnymi (np. RODO, DORA), wytycznymi sektorowymi oraz uznanymi dobrymi praktykami branżowymi (np. NIST, COBIT).

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza Politykę korzystania z chmury obliczeniowej oraz strategiczną mapę drogową wdrażania chmury obliczeniowej.

4.1.2 Dokonuje przeglądu i zatwierdza wyjątki o wysokim poziomie ryzyka od standardowych wymagań nadzorczych dotyczących chmury obliczeniowej.

4.1.3 Zapewnia, aby inicjatywy chmurowe otrzymywały odpowiednie finansowanie, nadzór oraz integrację z korporacyjnymi ramami zarządzania ryzykiem.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.2.1 Odpowiada za niniejszą politykę oraz organizacyjny Rejestr usług chmurowych.

4.2.2 Zatwierdza wdrożenie nowych dostawców usług chmurowych na podstawie due diligence dostawcy i oceny ryzyka.

4.2.3 Dokonuje przeglądu dokumentacji zgodności dostawców oraz potwierdza zgodność z wymaganiami bezpieczeństwa.

[... 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 podlegać przeglądowi co najmniej raz w roku i być aktualizowana w razie potrzeby w celu zapewnienia stałej zgodności z:

9.1.1 zmieniającymi się wymaganiami prawnymi i regulacyjnymi (np. RODO, NIS2, DORA),

9.1.2 zmianami w normach ISO/IEC 27001 lub ISO/IEC 27002,

9.1.3 aktualizacjami architektury chmury obliczeniowej organizacji, krajobrazu zagrożeń lub portfela usług,

9.1.4 działaniami po incydentach, wynikami audytów lub wnioskami z eksploatacji operacyjnej.

9.2 CISO odpowiada za zainicjowanie przeglądu i zwołanie odpowiednich interesariuszy, w tym:

9.2.1 architekta bezpieczeństwa chmury,

9.2.2 zespołu prawnego i zgodności,

9.2.3 zespołów zakupów i menedżerów dostawców,

9.2.4 właścicieli usług oraz operacji IT.

9.3 Wszystkie aktualizacje muszą być:

9.3.1 objęte kontrolą wersji i opatrzone datą,

9.3.2 zatwierdzone przez kierownictwo wykonawcze,

9.3.3 zakomunikowane zainteresowanym stronom, w tym pracownikom, wykonawcom i podmiotom trzecim,

9.3.4 archiwizowane zgodnie z wewnętrznymi zasadami zarządzania dokumentacją.

9.4 Przeglądy doraźne mogą zostać uruchomione przez:

9.4.1 nowe relacje z CSP lub istotne migracje,

9.4.2 nowe zagrożenia dla infrastruktury chmury obliczeniowej,

9.4.3 istotne zmiany obowiązków umownych, prawnych lub sektorowych.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest ściśle powiązana z następującymi politykami wewnętrznymi i od nich zależna:

10.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia nadrzędne zasady bezpiecznego funkcjonowania systemów i usług, które niniejsza polityka egzekwuje w kontekście chmury obliczeniowej.

10.1.2 P5 – Polityka zarządzania zmianą: wszystkie zmiany konfiguracji w chmurze obliczeniowej muszą być realizowane zgodnie z procedurami kontroli zmian określonymi w P5.

10.1.3 P13 – Polityka klasyfikacji i oznaczania informacji: określa sposób oceny danych przed ich przeniesieniem do chmury obliczeniowej oraz sposób stosowania zabezpieczeń, takich jak szyfrowanie i rezydencja danych.

10.1.4 P18 – Polityka zabezpieczeń kryptograficznych: określa standardy dotyczące szyfrowania, zarządzania kluczami i stosowania algorytmów kryptograficznych, bezpośrednio stosowane w konfiguracji usług chmurowych.

10.1.5 P22 – Polityka logowania i monitorowania: określa wymagania dotyczące gromadzenia, przechowywania i analizy logów, które muszą być egzekwowane w środowiskach chmurowych.

10.1.6 P30 – Polityka reagowania na incydenty: określa procedury eskalacji, ograniczania skutków i działań naprawczych dla zdarzeń bezpieczeństwa informacji związanych z chmurą obliczeniową.

10.1.7 P33 – Polityka monitorowania audytu i zgodności: wspiera gotowość audytową oraz ciągłe zapewnianie, że zabezpieczenia w chmurze obliczeniowej są egzekwowane i monitorowane.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001: Klauzula 8.1 – planowanie operacyjne i nadzór: wymaga, aby organizacje wdrażały i nadzorowały procesy niezbędne do spełnienia wymagań bezpieczeństwa informacji, w tym dotyczące środowisk chmury obliczeniowej.

11.2 ISO/IEC 27002:2022 – Zabezpieczenia 5.23 do 5.25:

11.2.1 Załącznik A, zabezpieczenie 5.23 – korzystanie z usług chmurowych: wymaga oceny opartej na ryzyku, formalnej autoryzacji oraz dokumentowania korzystania z usług chmurowych.

11.2.2 Załącznik A, zabezpieczenie 5.24 – polityka korzystania z chmury obliczeniowej: wymaga ustanowienia i stosowania formalnych polityk korzystania z chmury obliczeniowej, zgodnych z potrzebami i ryzykiem organizacji.

11.2.3 Załącznik A, zabezpieczenie 5.25 – bezpieczeństwo w usługach chmurowych: wymaga integracji bezpieczeństwa, zabezpieczeń umownych oraz monitorowania obciążeń i danych hostowanych w chmurze obliczeniowej.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – korzystanie z systemów zewnętrznych: wymaga zdefiniowania zasad i warunków dostępu do zasobów organizacji z systemów zewnętrznych lub systemów opartych na chmurze obliczeniowej.

11.3.2 SA-9(5) – usługi zewnętrznych systemów informacyjnych: wymaga umownych wymagań bezpieczeństwa, nadzoru i ciągłego monitorowania systemów chmurowych stron trzecich.

11.3.3 SC-12 do SC-28 – ochrona kryptograficzna, ochrona granic i integralność transmisji: pozostają zgodne z wymaganiami dotyczącymi szyfrowania, tożsamości i dostępu dla usług hostowanych w chmurze obliczeniowej oraz danych w tranzycie.

11.3.4 SR-5 – bezpieczeństwo łańcucha dostaw: wspiera weryfikację i kontrolę umowną wobec CSP uczestniczących w świadczeniu usług.

11.4 RODO (2016/679):

11.4.1 Artykuł 28 – obowiązki podmiotu przetwarzającego: wymaga formalnych umów z dostawcami chmury obliczeniowej w celu zapewnienia bezpieczeństwa, poufności oraz rozliczalności audytowej przetwarzania danych osobowych.

11.4.2 Artykuł 32 – bezpieczeństwo przetwarzania: wspiera stosowanie szyfrowania, kontroli dostępu, rejestrowania oraz innych zabezpieczeń w środowiskach chmury obliczeniowej.

11.4.3 Rozdział V – międzynarodowe transfery danych: wymaga zgodnego z prawem transferu danych poza UE/EOG z zastosowaniem zabezpieczeń, takich jak standardowe klauzule umowne (SCC) lub decyzje stwierdzające odpowiedni stopień ochrony.

11.5 Dyrektywa NIS2 (UE) 2022/2555:

11.5.1 Artykuł 21(2)(f, i): wymaga, aby podmioty zarządzały ryzykiem związanym z dostawcami usług chmurowych będącymi stronami trzecimi oraz zapewniały integralność cyfrowego łańcucha dostaw za pomocą środków umownych i technicznych.

11.6 DORA (UE) 2022/2554:

11.6.1 Artykuł 5(2) – zarządzanie ryzykiem ICT: wymaga włączenia ryzyka stron trzecich w obszarze ICT, w tym usług chmurowych, do ogólnego nadzoru nad ryzykiem.

11.6.2 Artykuł 28 – nadzór nad krytycznymi zewnętrznymi dostawcami usług ICT: wymaga, aby podmioty finansowe monitorowały, kontrolowały i raportowały zależności od dostawców chmury obliczeniowej, ich profil ryzyka bezpieczeństwa oraz odporność.

11.7 COBIT 2019:

11.7.1 BAI04 – zarządzanie dostępnością i pojemnością: zapewnia, że usługi chmurowe są odporne, monitorowane i spełniają określone kryteria wydajności.

11.7.2 DSS01 – zarządzanie operacjami: wspiera integrację operacyjną, obsługę incydentów oraz konfiguracje bazowe na platformach hostowanych w chmurze obliczeniowej.

11.7.3 DSS05 – zarządzanie usługami bezpieczeństwa: ukierunkowuje wdrożenie zabezpieczeń specyficznych dla chmury obliczeniowej, monitorowania oraz zapobiegania incydentom w usługach cyfrowych.