					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P27S					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	
ISO/IEC 27002:2022	Środki kontrolne 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
RODO	Artykuł 28, 32 oraz rozdział V	
Dyrektywa NIS2	Artykuły 21(2)(f), (i)	
Rozporządzenie DORA	Artykuły 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Cel

1.1 Niniejsza polityka określa zasady bezpiecznego korzystania z usług chmurowych w organizacji. Zapewnia ochronę danych przetwarzanych lub przechowywanych w chmurze, właściwą kontrolę dostępu oraz odpowiednie zarządzanie ryzykiem.

1.2 Wspiera MŚP w spełnianiu obowiązków prawnych i oczekiwań klientów w zakresie ochrony informacji wrażliwych, zapobiegania wyciekom danych oraz skutecznego zarządzania ryzykiem związanym z chmurą, bez konieczności utrzymywania infrastruktury klasy korporacyjnej.

1.3 Niniejsza polityka wspiera certyfikację ISO/IEC 27001, zgodność z RODO oraz bezpieczeństwo łańcucha dostaw poprzez spójny nadzór nad wszystkimi usługami chmurowymi świadczonymi przez strony trzecie.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszelkich usług chmurowych wykorzystywanych do przechowywania, przetwarzania lub przesyłania danych organizacji,

2.1.2 całego personelu, wykonawców oraz dostawców usług korzystających z narzędzi chmurowych w imieniu organizacji,

2.1.3 bezpłatnych i płatnych rozwiązań chmurowych, w tym platform poczty elektronicznej, udostępniania dokumentów, narzędzi SaaS, platform do tworzenia kopii zapasowych, wideokonferencji oraz platform obsługi klienta,

2.1.4 wszelkich urządzeń stacjonarnych, mobilnych i tabletów uzyskujących dostęp do informacji organizacji za pośrednictwem aplikacji chmurowych.

2.2 Zakres obejmuje między innymi:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business,

2.2.2 Zoom, Microsoft Teams, Google Meet,

2.2.3 AWS, Azure, GCP,

2.2.4 narzędzia chmurowe do tworzenia kopii zapasowych i odtwarzania po awarii,

2.2.5 foldery współdzielone lub aplikacje wykorzystywane do fakturowania, zarządzania projektami lub komunikacji z klientami.

3. Cele

3.1 Zapobieganie nieuprawnionemu lub obarczonemu wysokim ryzykiem korzystaniu z niezatwierdzonych usług chmurowych.

3.2 Zapewnienie, że dane wrażliwe lub informacje objęte regulacjami, przechowywane w chmurze, są zabezpieczone z zastosowaniem odpowiednich środków technicznych i organizacyjnych.

3.3 Określenie jasnych ról w zakresie zatwierdzania, konfiguracji, monitorowania i wycofywania usług chmurowych.

3.4 Kontrola przepływów danych oraz egzekwowanie wymagań dotyczących retencji, usuwania i ochrony prywatności informacji przechowywanych w chmurze.

3.5 Ograniczenie zależności od kont osobistych lub narzędzi nieobjętych ewidencją poprzez wymóg zatwierdzania wszystkich systemów chmurowych wykorzystywanych do celów biznesowych.

3.6 Spełnienie wymagań ISO/IEC 27001:2022, RODO, NIS2 oraz DORA w zakresie zarządzania zewnętrznymi zależnościami od usług chmurowych.

4. Role i obowiązki

4.1 Dyrektor Generalny (GM)

4.1.1 zatwierdza korzystanie ze wszystkich nowych usług chmurowych,

4.1.2 dokonuje przeglądu ryzyk związanych z dostawcami usług chmurowych i rodzajami usług,

4.1.3 egzekwuje postanowienia polityki i sprawuje nadzór nad decyzjami dotyczącymi wyjątków.

4.2 Dostawca wsparcia IT lub zespół wsparcia technicznego

4.2.1 ocenia i wdraża bezpieczną konfigurację usług chmurowych,

4.2.2 konfiguruje konta, mechanizmy kontroli dostępu i kopie zapasowe,

4.2.3 monitoruje zgodność z wymaganiami dotyczącymi haseł, uwierzytelniania wieloskładnikowego oraz ustawień 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 przez Dyrektora Generalnego, w uzgodnieniu z dostawcą wsparcia IT.

9.2 Formalny przegląd musi zostać przeprowadzony również:

9.2.1 po incydencie bezpieczeństwa związanym z chmurą, np. naruszeniu lub utracie danych,

9.2.2 po wdrożeniu nowej głównej platformy chmurowej,

9.2.3 w przypadku zmiany wymagań prawnych lub regulacyjnych, np. aktualizacji RODO, NIS2, DORA,

9.2.4 jeżeli działania monitorujące ujawnią niewłaściwe użycie lub nowe ryzyka.

9.3 GM musi zapewnić, że:

9.3.1 Rejestr usług chmurowych jest aktualizowany o nowe usługi oraz usługi wycofane z użytkowania,

9.3.2 wymagania prawne i wymagania dotyczące prywatności są nadal spełniane,

9.3.3 wszystkie zmiany są komunikowane właściwym użytkownikom i interesariuszom.

9.4 Wersje archiwalne muszą być bezpiecznie przechowywane, a starsze wersje polityki muszą być obsługiwane zgodnie z obowiązującą w organizacji P14S – Polityką retencji i utylizacji danych.

10. Powiązane polityki i zależności

10.1 Niniejszą politykę należy stosować łącznie z następującymi politykami bezpieczeństwa informacji dostosowanymi do MŚP:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: określa rozliczalność za zatwierdzanie usług chmurowych i zarządzanie relacjami z dostawcami.

10.1.2 P4S – Polityka kontroli dostępu: wspiera bezpieczne logowanie, zarządzanie sesją i praktyki cofania dostępu wymagane dla platform chmurowych.

10.1.3 P14S – Polityka retencji i utylizacji danych: reguluje sposób tworzenia kopii zapasowych danych przechowywanych w chmurze, ich okres przechowywania oraz usuwanie zgodnie z obowiązkami prawnymi.

10.1.4 P17S – Polityka ochrony danych i prywatności: zapewnia, że wszelkie dane osobowe przechowywane w usługach chmurowych są przetwarzane zgodnie z zasadami RODO.

10.1.5 P30S – Polityka reagowania na incydenty: określa ustrukturyzowane procedury reagowania na incydenty bezpieczeństwa w chmurze, w tym gromadzenie dowodów i powiadomienia zewnętrzne.

10.2 Łącznie polityki te zapewniają, że korzystanie z chmury jest bezpieczne, zgodne i odporne operacyjnie.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – wymaga, aby organizacje wdrażały środki operacyjne dotyczące postępowania z danymi, w tym związane z systemami chmurowymi.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 5.23 – wymaga nadzoru nad korzystaniem z usług chmurowych i narzędzi SaaS stron trzecich.

11.2.2 Środek kontrolny 5.24 – wymaga zdefiniowanej polityki korzystania z chmury zgodnej z ryzykiem i wymaganiami regulacyjnymi.

11.2.3 Środek kontrolny 5.25 – wymaga, aby organizacje zapewniły, że środki kontroli bezpieczeństwa w środowiskach chmurowych odpowiadają potrzebom organizacji.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – wymaga formalnych zasad korzystania z systemów zewnętrznych, takich jak usługi chmurowe.

11.3.2 SC-12, SC-13 – odnoszą się do szyfrowania danych w tranzycie i danych w spoczynku w środowiskach chmurowych.

11.3.3 SR-5 – obejmuje środki kontroli ryzyka dotyczące chmury i stron trzecich w ramach łańcucha dostaw.

11.4 RODO (2016/679)

11.4.1 Artykuł 28 – wymaga, aby dostawcy chmurowi działający jako podmioty przetwarzające przestrzegali wiążących obowiązków umownych.

11.4.2 Artykuł 32 – nakłada obowiązek stosowania środków technicznych i organizacyjnych dla przetwarzania danych w chmurze.

11.4.3 Rozdział V – zakazuje nieuprawnionego międzynarodowego przekazywania danych osobowych przechowywanych w chmurze.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(f), (i) – wymaga od podmiotów kluczowych i ważnych wdrożenia odpowiednich polityk dotyczących bezpieczeństwa usług chmurowych i kontroli łańcucha dostaw.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 5(2) – wymaga od MŚP z sektora finansowego uwzględnienia bezpieczeństwa chmury w ramach zarządzania ryzykiem ICT.

11.6.2 Artykuł 28 – ustanawia zasady nadzoru nad krytycznymi zewnętrznymi dostawcami usług ICT, w tym dostawcami usług chmurowych.

11.7 COBIT 2019

11.7.1 DSS01 – „Manage Operations” odnosi się do integralności operacyjnej usług chmurowych.

11.7.2 DSS05 – „Manage Security Services” obejmuje zabezpieczenia i monitorowanie właściwe dla chmury.

11.7.3 BAI04 – „Manage Availability and Capacity” zapewnia ciągłość działania i wydajność w środowiskach chmurowych.