					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P29S					Tytuł dokumentu: **Polityka danych testowych i środowisk testowych**							
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	Klauzule 6.1, 8	
ISO/IEC 27002:2022	Zabezpieczenia 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
RODO	Artykuły 5 ust. 1 lit. c, 25, 32	
Dyrektywa NIS2	Artykuł 21 ust. 2 lit. e, h	
Rozporządzenie DORA	Artykuł 9	
COBIT 2019	BAI07, DSS05	

1. Cel

1.1 Niniejsza polityka określa zasady zarządzania danymi testowymi i środowiskami testowymi w celu zapobiegania przypadkowemu ujawnieniu informacji, naruszeniom ochrony danych oraz zakłóceniom operacyjnym podczas działań testowych.

1.2 Zapewnia ona, że rzeczywiste dane klientów nigdy nie są wykorzystywane w testach w sposób niewłaściwy oraz że środowiska testowe są logicznie i technicznie odseparowane od systemów produkcyjnych.

1.3 Polityka ma wspierać MŚP w spełnianiu wymagań certyfikacyjnych ISO/IEC 27001 oraz właściwych przepisów dotyczących ochrony danych, przy jednoczesnym zachowaniu praktycznego i wykonalnego charakteru dla organizacji bez dedykowanego zespołu IT.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich środowisk testowych (np. serwerów testowych typu staging, systemów typu sandbox, środowisk testowych wykorzystywanych w pracach rozwojowych),

2.1.2 wszystkich danych testowych, niezależnie od tego, czy zostały utworzone ręcznie, wygenerowane czy pozyskane na podstawie danych produkcyjnych,

2.1.3 całego personelu zaangażowanego w działania testowe, w tym pracowników, wykonawców, freelancerów i dostawców usług IT,

2.1.4 wszelkich testów, które mogą wpływać na platformy dostępne dla klientów, wewnętrzne systemy biznesowe lub usługi stron trzecich.

2.2 Obejmuje ona zarówno środowiska techniczne, jak i procesy wykorzystywane do wspierania:

2.2.1 rozwoju stron internetowych, aplikacji i narzędzi,

2.2.2 aktualizacji systemów, testów konfiguracji oraz testów integracyjnych,

2.2.3 zautomatyzowanych i ręcznych testów funkcjonalnych lub testów bezpieczeństwa.

3. Cele

3.1 Zapobieganie wykorzystywaniu w testach rzeczywistych, możliwych do zidentyfikowania danych klientów, chyba że zostały one zanonimizowane i wyraźnie zatwierdzone.

3.2 Utrzymanie ścisłej separacji pomiędzy systemami testowymi i produkcyjnymi w celu uniknięcia niezamierzonego ujawnienia danych lub zakłóceń operacyjnych.

3.3 Ochrona systemów testowych i danych testowych przed nieuprawnionym dostępem, przypadkowym ujawnieniem lub ponownym wykorzystaniem pomiędzy środowiskami bez zastosowania odpowiednich zabezpieczeń.

3.4 Zapewnienie zgodności z właściwymi przepisami dotyczącymi ochrony danych (np. RODO, NIS2) przez zapewnienie, że wszystkie dane testowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób bezpieczny.

3.5 Wspieranie gotowości organizacji do audytów zewnętrznych i certyfikacji ISO/IEC 27001 przez dokumentowanie praktyk testowych oraz stosowanie spójnych zabezpieczeń.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Ponosii ogólną odpowiedzialność za ochronę danych testowych i bezpieczeństwo systemów testowych.

4.1.2 Zatwierdza każde wykorzystanie rzeczywistych danych w testach po potwierdzeniu zastosowania odpowiednich zabezpieczeń (np. anonimizacji lub maskowania danych).

4.1.3 Weryfikuje, czy działania testowe są właściwie udokumentowane i zgodne z niniejszą polityką.

4.2 Właściciel projektu

4.2.1 Koordynuje projektowanie i realizację procesów testowych.

4.2.2 Zapewnia, że wszyscy członkowie zespołu rozumieją niniejszą politykę i jej przestrzegają.

4.2.3 Potwierdza, że systemy testowe są skonfigurowane w sposób bezpieczny przed rozpoczęciem testów.

4.2.4 Zgłasza GM wszelkie incydenty dotyczące środowisk testowych lub wycieki danych.

[... 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 Planowe przeglądy

9.1.1 Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku przez Dyrektora Generalnego (GM). Przegląd ma zapewnić, że polityka pozostaje aktualna w odniesieniu do:

9.1.1.1 zmian w narzędziach, platformach lub środowiskach rozwoju oprogramowania,

9.1.1.2 zaktualizowanych obowiązków prawnych, w tym wymagań dotyczących ochrony danych lub odporności cyfrowej,

9.1.1.3 certyfikacji MŚP i gotowości do audytu zgodnie z ISO/IEC 27001.

9.2 Zdarzenia wyzwalające przegląd doraźny

9.2.1 Dodatkowe przeglądy muszą być przeprowadzane po wystąpieniu:

9.2.1.1 incydentu obejmującego ujawnienie danych lub naruszenie bezpieczeństwa w środowiskach testowych,

9.2.1.2 wykorzystania danych rzeczywistych w testach, nawet jeżeli zostały zanonimizowane,

9.2.1.3 wdrożenia nowych metod testowych, systemów lub dostawców,

9.2.1.4 zmian regulacyjnych wpływających na sposób postępowania z danymi podczas testów.

9.3 Zarządzanie zmianą i komunikacja

9.3.1 GM odpowiada za:

9.3.1.1 aktualizację niniejszej polityki i dokumentowanie wszelkich zmian wraz z historią wersji,

9.3.1.2 informowanie personelu, Programistów i właściwych dostawców usług o aktualizacjach,

9.3.1.3 potwierdzenie, że cały personel zaangażowany w testy rozumie i stosuje najnowsze zasady,

9.3.1.4 utrzymywanie dostępnej aktualnej wersji polityki do celów przeglądu i audytu.

9.4 Audyt i dokumentacja

9.4.1 Zapisy dotyczące wszystkich przeglądów polityki, zatwierdzeń użycia danych rzeczywistych oraz uzasadnień wyjątków muszą być:

9.4.1.1 bezpiecznie przechowywane do celów audytowych,

9.4.1.2 dostępne na żądanie podczas audytów wewnętrznych lub audytów stron trzecich,

9.4.1.3 przeglądane corocznie w celu zapewnienia spójności z praktykami testowymi.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka musi być stosowana łącznie z następującymi politykami SME, aby utrzymać bezpieczeństwo i zgodność podczas testów:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: określa, kto odpowiada za nadzór nad rozwojem, testowaniem i obowiązkami związanymi z separacją systemów.

10.1.2 P4S – Polityka kontroli dostępu: reguluje nadawanie, zarządzanie i usuwanie poświadczeń dostępu do systemów testowych.

10.1.3 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że personel rozumie ryzyka związane z danymi testowymi, bezpieczne praktyki postępowania oraz prawidłową separację środowisk.

10.1.4 P13S – Polityka klasyfikacji i oznaczania informacji: wspiera jednoznaczną klasyfikację danych testowych i określa podejścia do anonimizacji lub maskowania danych.

10.1.5 P17S – Polityka ochrony danych i prywatności: zapewnia zgodność z obowiązkami wynikającymi z RODO, w tym ze środkami bezpieczeństwa dotyczącymi przetwarzania i przechowywania danych osobowych, również w środowiskach testowych.

10.1.6 P24S – Polityka bezpiecznego rozwoju oprogramowania: określa ogólne oczekiwania w zakresie bezpieczeństwa wobec zespołów deweloperskich, w tym bezpieczne wykorzystywanie danych podczas etapów testowych.

10.1.7 P30S – Polityka reagowania na incydenty: określa sposób reagowania na każde naruszenie lub problem wykryty w środowisku testowym albo spowodowany niewłaściwym postępowaniem z danymi testowymi.

10.2 Polityki te tworzą spójne ramy bezpieczeństwa wspierające integralność testów, minimalizację danych oraz pełne dostosowanie do ISO/IEC 27001 w obszarze rozwoju i zapewnienia jakości.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1 – wymaga oceny ryzyka i podejmowania działań w ramach postępowania z ryzykiem, w tym w odniesieniu do ryzyk związanych z testowaniem.

11.1.2 Klauzula 8.1 – wymaga planowania i nadzoru nad procesami operacyjnymi, w tym nad przygotowaniem środowisk testowych.

11.2 ISO/IEC 27002

11.2.1 Zabezpieczenie 8.28 – wymaga, aby organizacje chroniły dane testowe i zapewniały, że nie zawierają one danych wrażliwych ani danych produkcyjnych.

11.2.2 Zabezpieczenie 8.29 – wymaga wyraźnej separacji środowisk rozwojowych, testowych i produkcyjnych.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – obejmuje wymagania kontrolne dotyczące rozwoju i testowania.

11.3.2 SA-12 – dotyczy ryzyk testowych w łańcuchu dostaw i ocen bezpieczeństwa.

11.3.3 SC-32 – wymaga separacji środowisk oraz ochrony poufności i integralności danych testowych.

11.4 RODO

11.4.1 Artykuł 5 ust. 1 lit. c – wymaga minimalizacji danych, w tym wykorzystywania wyłącznie danych niezbędnych do testów.

11.4.2 Artykuł 25 – wymaga ochrony danych w fazie projektowania, co obejmuje także zabezpieczenia dla środowisk testowych.

11.4.3 Artykuł 32 – nakłada obowiązek bezpiecznego przetwarzania danych osobowych we wszystkich systemach, w tym w środowiskach nieprodukcyjnych.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21 ust. 2 lit. e, h – wymaga bezpiecznego rozwoju i testowania systemów, w szczególności tam, gdzie usługi cyfrowe są narażone na ryzyko cybernetyczne.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – podkreśla znaczenie cyfrowej odporności operacyjnej, w tym bezpiecznego testowania systemów ICT przez MŚP w sektorze finansowym.

11.7 COBIT 2019

11.7.1 BAI07 – Zarządzanie akceptacją zmian i przejściem do eksploatacji: obejmuje zabezpieczenia testowe służące walidacji nowych systemów i sposobu postępowania z danymi.

11.7.2 DSS05 – Zarządzanie usługami bezpieczeństwa: wymaga praktyk testowych i rozwojowych, które zapobiegają niewłaściwemu wykorzystaniu lub ujawnieniu danych biznesowych.