					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P29					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**

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	Klauzula 8	Dotyczy bezpiecznego planowania i nadzoru nad danymi testowymi oraz środowiskami testowymi
ISO/IEC 27002:2022	Środki kontrolne 8.28–8.29	Obejmuje bezpieczne dane testowe oraz ochronę środowisk testowych
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Odnosi się do testowania i oceny przez programistów, ochrony danych w spoczynku oraz integralności informacji
RODO	Artykuły 5, 25, 32	Obejmuje minimalizację danych, ochronę danych w fazie projektowania oraz bezpieczeństwo przetwarzania w kontekście testów
Dyrektywa NIS2	Artykuł 21(2)(e), (h)	Odnosi się do bezpiecznych praktyk rozwoju i testowania
Rozporządzenie DORA	Artykuł 9	Dotyczy systemów i protokołów ICT oraz bezpieczeństwa danych testowych
COBIT 2019	DSS05, BAI07	Obejmuje zarządzanie usługami bezpieczeństwa oraz akceptację zmian i przejście do eksploatacji

1. Cel

1.1. Niniejsza polityka określa obowiązkowe wymagania dotyczące zarządzania środowiskami testowymi i danymi testowymi w celu zapewnienia bezpieczeństwa, poufności oraz integralności operacyjnej w całym cyklu życia rozwoju i testowania oprogramowania.

1.2. Jej celem jest zapobieganie nieuprawnionemu dostępowi, wyciekom danych oraz przenikaniu do systemów produkcyjnych, wynikającym z niewłaściwie zarządzanych środowisk testowych lub wykorzystywania w testach danych rzeczywistych.

1.3. Polityka wymaga bezpiecznego postępowania z danymi wykorzystywanymi do testów, utwardzania infrastruktury testowej oraz stosowania kontroli dostępu opartej na rolach (RBAC), przy jednoczesnym zapewnieniu zgodności z mającymi zastosowanie wymaganiami regulacyjnymi i umownymi.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich środowisk testowych, danych, narzędzi i procesów wykorzystywanych do testowania oprogramowania, systemów, aplikacji i infrastruktury w całej organizacji.

2.2. Obejmuje ona:

2.2.1. Środowiska testowe udostępniane w infrastrukturze lokalnej, chmurze obliczeniowej lub za pośrednictwem platform podmiotów trzecich

2.2.2. Dane testowe wykorzystywane w testach funkcjonalnych, wydajnościowych, regresyjnych i bezpieczeństwa

2.2.3. Testowanie ręczne, skryptowe lub zautomatyzowane (np. potoki CI/CD)

2.2.4. Cały personel zaangażowany w testowanie, w tym zespoły wewnętrzne, dostawców i kontraktorów

2.3. Polityka obowiązuje niezależnie od krytyczności systemu, typu aplikacji oraz tego, czy rozwój jest realizowany wewnętrznie, czy w modelu outsourcingowym.

3. Cele

3.1. Zapobieganie wykorzystywaniu w środowiskach testowych danych produkcyjnych, danych rzeczywistych, danych wrażliwych lub informacji regulowanych (np. danych osobowych umożliwiających identyfikację osoby (PII), danych posiadaczy kart), chyba że zostały zanonimizowane lub wyraźnie zatwierdzone.

3.2. Zapewnienie pełnej segregacji sieciowej i dostępowej między środowiskami testowymi a produkcyjnymi, aby uniknąć nieuprawnionego dostępu do danych lub przenikania do systemów.

3.3. Wymaganie stosowania szyfrowania, maskowania danych lub generowania danych syntetycznych, gdy do celów testowych potrzebne są dane reprezentatywne.

3.4. Ograniczenie prawdopodobieństwa naruszeń zgodności, ujawnienia danych klientów lub zakłóceń operacyjnych wynikających z niezabezpieczonych danych testowych lub środowisk testowych.

3.5. Zapewnienie zgodności postępowania z danymi testowymi z normami branżowymi (ISO, NIST, COBIT) oraz regulacjami takimi jak RODO, NIS2 i DORA.

4. Role i odpowiedzialności

4.1. Dyrektor ds. bezpieczeństwa informacji (CISO)

4.1.1. Jest właścicielem niniejszej polityki i odpowiada za wdrożenie zabezpieczeń technicznych i organizacyjnych dla danych testowych oraz środowisk testowych.

4.1.2. Zatwierdza wykorzystanie danych rzeczywistych lub wrażliwych w testach na podstawie odpowiedniego uzasadnienia i przy zastosowaniu środków kompensujących.

4.2. Liderzy QA/Testów

4.2.1. Koordynują planowanie testów i zapewniają, że wszystkie działania testowe są zgodne z wymaganiami niniejszej polityki.

4.2.2. Weryfikują prawidłową segregację, dostęp oraz przygotowanie danych dla każdego etapu testów.

[... 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 corocznemu przeglądowi i aktualizowana w razie potrzeby w celu uwzględnienia:

9.1.1. Zmian wymagań regulacyjnych (np. RODO, DORA, NIS2)

9.1.2. Wdrożenia nowych narzędzi testowych, platform lub potoków automatyzacji

9.1.3. Ustaleń audytu wewnętrznego lub rekomendacji po incydentach

9.1.4. Rozszerzenia procesów rozwojowych lub QA, które zmieniają sposób postępowania z danymi testowymi lub wykorzystania środowisk testowych

9.2. CISO odpowiada za zainicjowanie przeglądu we współpracy z:

9.2.1. Liderami QA/Testów

9.2.2. Menedżerami DevOps i infrastruktury

9.2.3. Zespołami rozwoju aplikacji

9.2.4. Inspektorem Ochrony Danych (IOD) oraz doradcą prawnym

9.3. Wszystkie zmiany muszą być:

9.3.1. Objęte kontrolą wersji i przechowywane w centralnym repozytorium dokumentów

9.3.2. Komunikowane odpowiednim osobom poprzez formalne kanały (np. powiadomienia SZBI, briefingi zespołowe)

9.3.3. Powiązane z aktualizacjami odpowiednich standardów technicznych, środków kontrolnych i procedur operacyjnych

9.4. Doraźne przeglądy inicjowane zdarzeniem muszą być przeprowadzane niezwłocznie po wystąpieniu:

9.4.1. Wycieku danych lub naruszenia z udziałem środowisk testowych

9.4.2. Niezgodności audytowej związanej z postępowaniem z danymi testowymi

9.4.3. Istotnych zmian obowiązków prawnych lub architektury IT

10. Powiązane polityki i zależności

10.1. Niniejsza polityka jest ściśle powiązana z poniższymi politykami w celu zapewnienia bezpiecznego i zgodnego z wymaganiami postępowania z danymi testowymi oraz środowiskami testowymi:

10.1.1. P1 – Polityka bezpieczeństwa informacji: określa nadrzędne zasady bezpieczeństwa regulujące ochronę danych testowych i zarządzanie środowiskami testowymi.

10.1.2. P5 – Polityka zarządzania zmianami: ma zastosowanie do tworzenia, aktualizacji i wycofania z eksploatacji środowisk testowych oraz potoków wdrożeniowych.

10.1.3. P13 – Polityka klasyfikacji i oznaczania informacji: określa zasady doboru danych testowych i stosowania środków kontrolnych zależnych od poziomu wrażliwości.

10.1.4. P14 – Polityka retencji i utylizacji danych: określa terminy przechowywania i wymagania bezpiecznej utylizacji zbiorów danych testowych.

10.1.5. P15 – Polityka tworzenia kopii zapasowych i odtwarzania: określa wymagania dotyczące kopii zapasowych oraz walidacji odzyskiwania dla środowisk testowych.

10.1.6. P18 – Polityka zabezpieczeń kryptograficznych: określa obowiązkowe standardy szyfrowania dla danych w spoczynku i danych w tranzycie w ramach platform testowych.

10.1.7. P22 – Polityka logowania i monitorowania: reguluje widoczność działań w środowiskach testowych oraz wykrywanie anomalii.

10.1.8. P30 – Polityka reagowania na incydenty: określa eskalację i działania naprawcze dla naruszeń lub incydentów dotyczących systemów testowych.

10.1.9. P33 – Polityka monitorowania audytu i zgodności: umożliwia weryfikację przestrzegania polityki oraz ciągłe zapewnienie zgodności.

11. Normy i ramy odniesienia

11.1. Niniejsza polityka jest zgodna z globalnymi normami cyberbezpieczeństwa i ramami regulacyjnymi wymagającymi bezpiecznego postępowania z danymi testowymi oraz ochrony środowisk nieprodukcyjnych.

11.2. ISO/IEC 27001:

11.2.1. Klauzula 8.1 - wymaga bezpiecznego planowania i nadzoru nad danymi testowymi oraz środowiskami testowymi.

11.3. ISO/IEC 27002:2022 – Środki kontrolne 8.28–8.29:

11.3.1. Załącznik A, środek kontrolny 8.28 – Bezpieczne dane testowe: wymaga ochrony danych testowych wykorzystywanych w fazach rozwoju i testowania poprzez anonimizację, maskowanie danych lub generowanie danych syntetycznych.

11.3.2. Załącznik A, środek kontrolny 8.29 – Ochrona środowisk testowych: wymaga segregacji od środowiska produkcyjnego, kontroli dostępu oraz utwardzania środowisk testowych.

11.3.3. Środki te określają wymagania dotyczące bezpiecznego zarządzania danymi wykorzystywanymi podczas testów oraz ochrony systemów nieprodukcyjnych przed niewłaściwym użyciem, naruszeniem lub zanieczyszczeniem.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testowanie i ocena przez programistów: określa oczekiwania wobec bezpiecznych, powtarzalnych procedur testowych z odpowiednimi środkami kontroli danych.

11.4.2. SC-28 – Ochrona informacji w spoczynku: odpowiada wymaganiom dotyczącym szyfrowania danych testowych przechowywanych w systemach nieprodukcyjnych.

11.4.3. SC-32 – Integralność informacji: wspiera walidację danych, zapobieganie uszkodzeniu danych oraz kontrole wejścia/wyjścia podczas testów.

11.5. RODO (2016/679):

11.5.1. Artykuł 5 – Minimalizacja danych: zakazuje zbędnego wykorzystywania danych osobowych w testach.

11.5.2. Artykuł 25 – Ochrona danych w fazie projektowania: wymaga stosowania technik ochrony danych od początku cyklu rozwoju i testowania.

11.5.3. Artykuł 32 – Bezpieczeństwo przetwarzania: nakazuje stosowanie środków bezpieczeństwa dla środowisk testowych przetwarzających dane osobowe lub dane wrażliwe.

11.6. Dyrektywa UE NIS2 (2022/2555):

11.6.1. Artykuł 21(2)(e, h): wymaga bezpiecznych procesów rozwoju i testowania oprogramowania, z naciskiem na ochronę przed nieuprawnionym dostępem i wyciekami danych.

11.7. Rozporządzenie UE DORA (2022/2554):

11.7.1. Artykuł 9 – Systemy i protokoły ICT: wymaga, aby procesy testowania wspierały odporność operacyjną i chroniły dane operacyjne przed naruszeniem lub nieuprawnionym ujawnieniem.

11.8. COBIT 2019:

11.8.1. DSS05 – Zarządzanie usługami bezpieczeństwa: wspiera stosowanie polityk bezpieczeństwa we wszystkich środowiskach, w tym nieprodukcyjnych.

11.8.2. BAI07 – Zarządzanie akceptacją zmiany i przejściem: obejmuje formalny proces przejścia z testów do produkcji, w tym środki kontroli danych i środowisk.