| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Wprowadź tutaj nazwę zarejestrowanej osoby prawnej | | | | | | | |
| Numer dokumentu:<br>P28S | | | | | Tytuł dokumentu:<br>**Polityka rozwoju oprogramowania w outsourcingu** | | | | | | | |
| Wersja:<br>1.0 | | Data wejścia w życie:<br>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 5.1, 6.1, 8 | Mające zastosowanie zabezpieczenia SZBI oraz zabezpieczenia dotyczące dostawców |
| ISO/IEC 27002:2022 | Zabezpieczenia 5.19, 5.20, 8.25–8.27 | Zabezpieczenia dotyczące dostawców i bezpiecznego cyklu życia wytwarzania oprogramowania |
| NIST SP 800-53 Rev.5 | SA-4, SA-9, SA-11, SA-15, SR-3 | Wymagania dotyczące pozyskiwania, łańcucha dostaw, bezpiecznego rozwoju oraz umów z dostawcami |
| RODO | Artykuł 28 | Wymagania umowne oraz wymagania w zakresie ochrony danych dotyczące przetwarzania przez strony trzecie |
| Dyrektywa NIS2 | Artykuł 21(2)(a), (h) | Zabezpieczenia dotyczące bezpieczeństwa łańcucha dostaw i bezpiecznego rozwoju aplikacji |
| Rozporządzenie DORA | Artykuł 10 | Zarządzanie ryzykiem ICT związanym ze stronami trzecimi, w tym outsourcingiem prac rozwojowych |
| COBIT 2019 | BAI03, DSS05 | Wymagania dotyczące zewnętrznych prac rozwojowych i zewnętrznych dostawców usług IT |

**1. Cel**

1.1 Niniejsza polityka zapewnia, że wszystkie prace związane z outsourcingiem rozwoju oprogramowania — niezależnie od tego, czy są realizowane przez freelancerów, agencje czy dostawców zewnętrznych — są prowadzone w sposób bezpieczny, objęty kontrolą umowną oraz zgodny z mającymi zastosowanie wymaganiami prawnymi, regulacyjnymi i audytowymi.

1.2 Polityka chroni organizację przed ryzykami związanymi z niebezpiecznym kodem, niejednoznaczną własnością, ujawnieniem danych oraz niewłaściwym zarządzaniem dostawcami poprzez egzekwowanie wiążących standardów wytwórczych i nadzoru nad dostawcami, nawet przy braku dedykowanego działu IT.

1.3 Niniejsza polityka wspiera certyfikację ISO/IEC 27001:2022 poprzez określenie jednoznacznych oczekiwań dotyczących prac rozwojowych, rozliczalności oraz udokumentowanych zabezpieczeń nad działaniami rozwojowymi realizowanymi przez strony trzecie.

**2. Zakres**

**2.1 Niniejsza polityka ma zastosowanie do:**

2.1.1 wszystkich zewnętrznych programistów, w tym freelancerów i agencji programistycznych;

2.1.2 wszelkich prac rozwojowych obejmujących narzędzia wewnętrzne, publicznie dostępne strony internetowe, aplikacje lub automatyzację procesów biznesowych;

2.1.3 personelu odpowiedzialnego za wybór, zarządzanie lub nadzorowanie zewnętrznych programistów;

2.1.4 wszelkich integracji z systemami stron trzecich, skryptów lub prac rozwojowych, które wchodzą w interakcję z danymi lub systemami organizacji.

2.2 Zakres obejmuje również każdą stronę lub platformę posiadającą dostęp do poświadczeń organizacji, repozytoriów danych, repozytoriów kodu źródłowego, środowisk testowych lub systemów produkcyjnych.

**3. Cele**

3.1 Zapewnić, że wszystkie prace rozwojowe realizowane w modelu outsourcingu są zgodne z zasadami bezpiecznego wytwarzania oprogramowania oraz że programiści są umownie zobowiązani do przestrzegania udokumentowanych standardów i klauzul poufności.

3.2 Ustanowić własność wszystkich rezultatów prac — kodu, zasobów, poświadczeń i dokumentacji — zapewniając pełne przeniesienie praw na organizację oraz możliwe do prześledzenia przekazanie po zakończeniu projektu.

3.3 Zapobiegać typowym ryzykom rozwojowym, w tym ponownemu wykorzystaniu zastrzeżonego kodu, atakom na łańcuch dostaw z wykorzystaniem bibliotek, użyciu niewspieranych frameworków oraz niezweryfikowanemu dostępowi administracyjnemu.

3.4 Wymagać dokumentacji przed rozpoczęciem współpracy dla każdego projektu realizowanego w modelu outsourcingu, w tym umów, umowy o zachowaniu poufności oraz minimalnych wymagań bezpieczeństwa.

3.5 Chronić dane klientów, systemy i procesy wewnętrzne poprzez zapewnienie skutecznego nadzoru nad pracami rozwojowymi, testów po dostarczeniu oraz bezpiecznego zarządzania dostępem do systemów.

**4. Role i odpowiedzialności**

**4.1 Dyrektor Generalny (GM)**

4.1.1 Zatwierdza wszystkie relacje z dostawcami i podpisuje umowy dotyczące prac rozwojowych.

4.1.2 Zapewnia, że wszystkie prace rozwojowe realizowane w modelu outsourcingu są zgodne z niniejszą polityką.

4.1.3 Usuwa dostęp do systemów organizacji po zakończeniu projektu.

4.1.4 Dokonuje przeglądu dokumentacji i wyników po dostarczeniu.

**4.2 Właściciel projektu (zwykle pracownik wewnętrzny lub wyznaczony koordynator)**

4.2.1 Zarządza bieżącą koordynacją współpracy z zewnętrznym programistą.

4.2.2 Weryfikuje, czy wymagania funkcjonalne zostały spełnione oraz czy rezultaty prac zostały przetestowane.

4.2.3 Zapewnia bezpieczne przekazanie kodu i poświadczeń.

4.2.4 Zgłasza GM wszelkie problemy lub incydenty związane z pracami rozwojowymi.

[ ... 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 Coroczny przegląd**

**9.1.1 Niniejsza polityka musi być poddawana przeglądowi przez Dyrektora Generalnego (GM) co najmniej raz w roku. Przegląd ma zapewnić, że polityka nadal spełnia:**

9.1.1.1 wymagania certyfikacyjne ISO/IEC 27001;

9.1.1.2 zmiany obowiązków prawnych (np. artykuł 28 RODO, artykuł 10 DORA);

9.1.1.3 aktualne praktyki rozwojowe w MŚP oraz ryzyka związane ze stronami trzecimi.

**9.2 Przeglądy doraźne**

**9.2.1 Przeglądy polityki muszą być również przeprowadzane, gdy:**

9.2.1.1 następuje wdrożenie nowego dostawcy lub platformy realizującej outsourcing prac rozwojowych;

9.2.1.2 wystąpi istotny incydent związany z outsourcingiem prac rozwojowych;

9.2.1.3 nastąpią istotne zmiany w wykorzystywanych narzędziach, platformach lub środowiskach.

**9.3 Proces przeglądu**

**9.3.1 GM odpowiada za:**

9.3.1.1 weryfikację, że umowy, umowy o zachowaniu poufności i procesy kontroli dostępu pozostają skuteczne;

9.3.1.2 potwierdzenie, że obecni dostawcy i freelancerzy działają zgodnie z polityką;

9.3.1.3 aktualizację postanowień na podstawie informacji zwrotnych z poprzednich projektów lub incydentów.

**9.4 Kontrola wersji i komunikacja**

**9.4.1 Wszystkie zmiany muszą być:**

9.4.1.1 rejestrowane wraz z datą, przyczyną i opisem zmiany;

9.4.1.2 zatwierdzane przez GM i dodawane do historii wersji;

9.4.1.3 komunikowane całemu personelowi lub właścicielom projektów współpracującym z zewnętrznymi programistami;

9.4.1.4 w razie potrzeby ponownie przekazywane wszystkim odpowiednim dostawcom i stronom trzecim.

**10. Powiązane polityki i zależności**

**10.1 Niniejsza polityka bezpośrednio wspiera wdrożenie poniższych polityk dostosowanych do potrzeb MŚP i jest od nich zależna:**

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach nadzoru: wyjaśnia, kto odpowiada za zatwierdzanie dostawców, kontrolę dostępu i akceptację ryzyka przy korzystaniu z zewnętrznych programistów.

10.1.2 P4S – Polityka kontroli dostępu: określa prawidłowe tworzenie, ograniczanie i zamykanie kont użytkowników oraz dostępu administracyjnego wykorzystywanego podczas outsourcingu prac rozwojowych.

10.1.3 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że personel wewnętrzny rozumie, jak bezpiecznie koordynować współpracę z zewnętrznymi programistami, w tym w zakresie obsługi poświadczeń i plików projektowych.

10.1.4 P17S – Polityka ochrony danych i prywatności: ustanawia wymagania bezpieczeństwa i wymagania prawne dotyczące przetwarzania danych osobowych, które mogą być przetwarzane przez zewnętrznych programistów zgodnie z RODO.

10.1.5 P24S – Polityka bezpiecznego rozwoju oprogramowania: określa, w jaki sposób wewnętrzne i zewnętrzne prace rozwojowe muszą stosować praktyki bezpiecznego wytwarzania oprogramowania oraz weryfikację bibliotek i frameworków.

10.1.6 P30S – Polityka reagowania na incydenty: ma zastosowanie, gdy outsourcing prac rozwojowych prowadzi do incydentów bezpieczeństwa lub podatności, określając zasady skoordynowanego dochodzenia i remediacji.

10.2 Polityki te muszą być wdrażane równolegle, aby outsourcing prac rozwojowych nie powodował niezarządzanego ryzyka ani nie prowadził do naruszenia obowiązków zgodności właściwych dla MŚP.

## 11. Normy i ramy odniesienia

### 11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1 – Organizacje muszą oceniać i traktować ryzyka bezpieczeństwa informacji związane z dostawcami.

11.1.2 Klauzula 8.1 – Wymaga planowania operacyjnego i nadzoru, w tym w odniesieniu do usług stron trzecich, takich jak outsourcing prac rozwojowych.

### 11.2 ISO/IEC 27002

11.2.1 Zabezpieczenie 5.19 – Zaleca ocenę zdolności dostawców do spełnienia wymagań bezpieczeństwa informacji.

11.2.2 Zabezpieczenie 5.20 – Zachęca do regularnego monitorowania i okresowego przeglądu usług stron trzecich.

11.2.3 Zabezpieczenia 8.25–8.27 – Określają praktyki bezpiecznego cyklu życia rozwoju mające zastosowanie do outsourcingu prac rozwojowych.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Wymaga, aby strategie pozyskiwania obejmowały zabezpieczenia bezpieczeństwa informacji.

11.3.2 SA-9 – Odnosi się do zewnętrznego rozwoju systemów i ryzyk w łańcuchu dostaw.

11.3.3 SA-11 – Definiuje praktyki bezpiecznego rozwoju, w tym przeglądy kodu i usuwanie błędów.

11.3.4 SA-15 – Zachęca do stosowania narzędzi zautomatyzowanych do wykrywania błędów i zapewnienia jakości oprogramowania.

11.3.5 SR-3 – Wymaga, aby umowy z dostawcami obejmowały wymagania z zakresu cyberbezpieczeństwa.

### 11.4 Rozporządzenie ogólne o ochronie danych (RODO)

11.4.1 Artykuł 28 – Wymaga zawierania umów z podmiotami przetwarzającymi będącymi stronami trzecimi w celu zapewnienia odpowiednich środków ochrony danych, co ma bezpośrednie zastosowanie do programistów przetwarzających dane osobowe lub mających do nich dostęp.

### 11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(a), (h) – Wymaga zabezpieczeń dotyczących bezpieczeństwa łańcucha dostaw oraz praktyk bezpiecznego rozwoju oprogramowania dla dostawców usług cyfrowych objętych zakresem, w tym dla MŚP, jeżeli ma to zastosowanie.

### 11.6 Rozporządzenie UE DORA

11.6.1 Artykuł 10 – Wymaga zarządzania ryzykiem ICT związanym ze stronami trzecimi, w tym umowami rozwojowymi, obowiązkami bezpieczeństwa i zabezpieczeniami ryzyka związanymi z dostawcami zewnętrznymi.

### 11.7 COBIT 2019

11.7.1 BAI03 – Zarządzanie identyfikacją rozwiązań i ich budową – zapewnia, że zewnętrzne prace rozwojowe spełniają wymagania biznesowe i oczekiwania w zakresie bezpieczeństwa.

11.7.2 DSS05 – Zarządzanie usługami bezpieczeństwa – wymaga, aby zewnętrzne usługi bezpieczeństwa i dostawcy prac rozwojowych działali zgodnie z egzekwowanymi zasadami bezpieczeństwa i pod odpowiednim nadzorem.