POLITYKA BEZPIECZEŃSTWA INFORMACJI

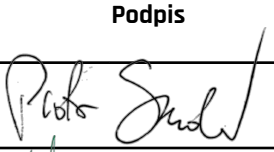
v.1

Warszawa – 22.08.2025

Dokument opracowany i przygotowany przez:

Imię i nazwisko	**Podpis**
Agnieszka Tarasiewicz	

Dokument zatwierdzony przez:

Imię i nazwisko	**Podpis**
Piotr Smoleń	
Daniel Wartołowski	

Symmetrical Payroll Sp. z o.o. zapewnia bezpieczeństwo informacji poprzez wdrożenie i utrzymanie skutecznego systemu zarządzania, który gwarantuje poufność, integralność i dostępność informacji oraz ochronę przed zagrożeniami wewnętrznymi i zewnętrznymi.

1. Zakres

Niniejsza polityka stanowi część Zintegrowanego Systemu Zarządzania i dotyczy wszystkich zasobów informacyjnych firmy – zarówno kontrolowanych indywidualnie, jak i komórek organizacyjnych, zarządzanych centralnie, samodzielnych lub sieciowych. Obejmuje wszystkie urządzenia komputerowe i komunikacyjne będące własnością firmy, dzierżawione, obsługiwane lub objęte umową, a także urządzenia sieciowe, telefony, urządzenia bezprzewodowe, stacje robocze, przenośne nośniki danych oraz powiązane oprogramowanie i peryferia. Obejmuje również dokumenty papierowe sklasyfikowane w niniejszych wytycznych.

Polityka obowiązuje wszystkich pracowników, współpracowników oraz kontrahentów zewnętrznych, a także inne osoby mające dostęp do zasobów informacyjnych Symmetrical. Wszyscy użytkownicy zasobów ponoszą odpowiedzialność za ich ochronę.

2. Cele Polityki

Celem bezpieczeństwa informacji jest ochrona zasobów firmy przed nieuprawnionym dostępem lub uszkodzeniem. Podstawowe zasady obejmują m.in.:

1. **Poufność** – zapewnienie, że dostęp do informacji mają wyłącznie osoby uprawnione.
2. **Integralność** – ochrona przed nieuprawnioną modyfikacją danych i systemów.
3. **Dostępność** – zapewnienie, że informacje oraz systemy są dostępne zawsze, gdy są potrzebne do realizacji procesów biznesowych.
4. **Zgodność** – spełnianie wymagań prawnych, normatywnych i kontraktowych związanych z bezpieczeństwem informacji.
5. **Świadomość i odpowiedzialność** – budowanie kultury bezpieczeństwa wśród pracowników poprzez szkolenia, komunikację i zaangażowanie.

3. Zobowiązania

- Zarząd Spółki zobowiązuje się do zapewnienia zasobów niezbędnych dla skutecznego funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.
- Wszelkie incydenty bezpieczeństwa są rejestrowane, analizowane i wykorzystywane do doskonalenia systemu ochrony informacji.
- Polityka podlega okresowym przeglądom i aktualizacji w celu zapewnienia jej adekwatności do zmieniających się warunków i wymagań.

4. Polityka

4.1. Dostęp do informacji, poufność i ujawnianie

- Dane nie mogą być ujawniane osobom lub podmiotom nieupoważnionym.
- Dystrybuowanie informacji musi odbywać się wyłącznie w ramach zatwierdzonych procedur.
- Użytkownicy muszą ograniczać dostęp do danych tylko do zakresu niezbędnego do wykonywania obowiązków.

4.2. Incydenty bezpieczeństwa i naruszenia danych

- Wszystkie podejrzenia naruszeń muszą być natychmiast zgłaszane zgodnie z Procedurą Identyfikowania i Reagowania na Zagrożenia do Zespołu ds. Bezpieczeństwa Informacji
- Symmetrical ma obowiązek powiadomić wszystkie osoby, których dane zostały naruszone, w ciągu 72 godzin od wykrycia incydentu.

4.3. Podział odpowiedzialności

- **Pracownicy i osoby uprawnione -** Każdy odpowiedzialny jest za ochronę informacji, zgodnie z obowiązującymi procedurami i regulacjami wewnętrznymi.
- **Zespół ds. Bezpieczeństwa Informacji** - utrzymanie polityki, główny nadzór nad incydentami bezpieczeństwa.
- **Kwalifikowani dostawcy** – zobowiązani do przestrzegania polityki bezpieczeństwa i natychmiastowego zgłaszania naruszeń.
- **Inspektor Danych Osobowych** - wsparcie w zakresie polityk i interpretacji prawa, kontakt z organami prawa.

4.4. Rodzaje danych

- **Dane publiczne** – dostępne publicznie, wymagają niskiego poziomu ochrony.
- **Dane poufne (SECRET)** – dane poufne, utrzymywane przez firmę, wymagają umiarkowanego do wysokiego poziomu ochrony.
- **Dane ograniczone (RESTRICTED)** – najbardziej wrażliwe, wymagają najwyższego poziomu ochrony.

4.5. Przechowywanie i usuwanie informacji

- **Dokumenty papierowe** – dane publiczne można utylizować w procesie recyklingu, dane ograniczone należy niszczyć (np. przez szatkowanie).
- **Dane elektroniczne** – muszą być przechowywane w bezpiecznych centrach danych i szyfrowane zgodnie z wytycznymi szyfrowania.
- **Urządzenia prywatne** – muszą być zgodne z polityką Polityka używania prywatnych urządzeń w pracy (BYOD).