Polityka firmy nr 7

Globalne bezpieczeństwo informacji i systemów

Cel

Celem niniejszej Polityki jest określenie zaangażowania firmy Stryker w odpowiednie działania kontrolne w zakresie bezpieczeństwa informacji, systemów i działań zgodnie z obowiązującym prawem.

Zakres

Niniejsza Polityka dotyczy wszystkich pracowników firmy Stryker i stron trzecich (np. sprzedawców, podwykonawców lub przedstawicieli) działających w imieniu firmy Stryker niezależnie od lokalizacji. Jeśli którekolwiek z postanowień niniejszej Polityki nie jest zgodne z prawem lokalnym obowiązującym w odniesieniu do konkretnej jednostki prawnej Stryker, jednostka ta w niezbędnym zakresie opracuje i wprowadzi załącznik do niniejszej Polityki pozwalający na zachowanie zgodności z prawem lokalnym tak, aby zmieniona polityka była nadal w jak największym stopniu zgodna z zasadami zawartymi w niniejszej Polityce. Dodatek taki zostaje zatwierdzony przez CISO. W przypadku, gdy nie wdrożono załącznika lokalnego lub regionalnego, wszystkie postanowienia niniejszej Polityki pozostaną w mocy w zakresie zgodnym z obowiązującym prawem.

Podstawowe zasady

Stryker przestrzega wszystkich przepisów regulujących bezpieczeństwo produktów i systemów firmy Stryker. Ponadto firma Stryker przestrzega standardów określonych poniżej.

1. **Mianowanie głównego kierownika ds. bezpieczeństwa informacji (Chief Information Security Officer — CISO):** CISO odpowiada za ustanowienie i egzekwowanie efektywnego globalnego programu bezpieczeństwa informacji Stryker oraz dostosowanie inicjatyw bezpieczeństwa do programów i celów biznesowych w zakresie ochrony zasobów, produktów, systemów i technologii informatycznych.

2. **Wdrażanie polityk bezpieczeństwa oraz struktur administracyjnych i zarządzania:** Poprzez odpowiednie systemy zarządzania jakością, system zarządzania bezpieczeństwem informacji, standardy nadzoru nad informacjami, standardy dopuszczalnego użytkowania, plan reagowania na incydenty oraz powiązane normy i procedury Stryker wdroży odpowiednie kontrole bezpieczeństwa administracyjnego, technicznego i fizycznego.

3. **Ocena podmiotów zewnętrznych:** Globalny proces oceny bezpieczeństwa musi zostać zakończony przed nawiązaniem współpracy z dowolnym podmiotem zewnętrznym, który ma mieć dostęp do sieci Stryker lub elektronicznych danych wrażliwych lub który zapewnia rozwiązania internetowe lub oprogramowanie do użytku wewnętrznego lub użytkowania w produkcie lub usłudze oferowanej przez Stryker.

4. **Używanie sprzętu i systemów Stryker:** Każdy pracownik Stryker lub podmiot zewnętrzny, który ma dostęp do urządzeń lub systemów firmy Stryker, musi używać tego sprzętu i tych systemów zgodnie z obowiązującymi wymaganiami dopuszczalnego użytkowania.

Obowiązki

Wszyscy pracownicy Stryker i podmioty zewnętrzne są odpowiedzialni za przestrzeganie niniejszej Polityki oraz wszystkich obowiązujących norm i procedur wykonawczych. CISO, wspólnie z odpowiednimi jednostkami biznesowymi i funkcjami, wskaże wszystkie dodatkowe standardy i procedury niezbędne do zapewnienia zgodności z niniejszą polityką oraz opracuje i wdroży takie standardy i procedury.

Zgodność

Wszyscy pracownicy Stryker i podmioty zewnętrzne są zobowiązani do przestrzegania tej Polityki. W przypadku pytań dotyczących niniejszej Polityki lub związanych z nią procedur albo w przypadku wątpliwości dotyczących programu bezpieczeństwa firmy Stryker prosimy o kontakt z lokalnym przedstawicielem działu kadr firmy Stryker, dyrektorem ds. zgodności, radcą prawnym lub infolinią ds. etyki. Wszystkie zgłoszenia zostaną potraktowane poufnie zgodnie z polityką i procedurami infolinii.