Polityka Bezpieczeństwa Informacji

SoftFlow Sp. z o.o. prowadzi działalność przy zachowaniu najwyższych standardów, profesjonalnie, uczciwie, w sposób godny zaufania oraz w zgodzie z przyjętymi zasadami ochrony danych osobowych i bezpieczeństwa informacji. Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów naszej Spółki oraz warunkiem ciągłego jej rozwoju. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa oraz zastosowanie adekwatnych rozwiązań technicznych.

Stosownie do zidentyfikowanych ryzyk, najlepszych branżowych praktyk bezpieczeństwa informacji i zobowiązań umownych SoftFlow Sp. z o.o. wdrożyła środki techniczne i organizacyjne, aby zapewnić adekwatny stopień bezpieczeństwa informacji.
Dla zapewnienia wysokiego poziomu ochrony danych i prywatności stosujemy następujące zasady:

- wszystkie procesy związane z bezpieczeństwem informacji są poddawane regularnym przeglądom (minimum raz w roku),
- regularnie (minimum raz w roku) wykonywany jest proces oceny ryzyka bezpieczeństwa informacji,
- wszyscy pracownicy SoftFlow Sp. z o.o. są co roku szkoleni w zakresie bezpieczeństwa informacji,
- zwracamy szczególną uwagę na dobór kompetentnej kadry pracowniczej oraz odpowiedni nadzór nad powierzonymi im procesami, w tym związanych z przetwarzaniem danych osobowych,
- zbieramy informacje i analizujemy wszelkie incydenty związane z naruszeniem bezpieczeństwa i podejmujemy niezwłoczne działania w celu wyeliminowania tych zagrożeń,
- stale monitorujemy skuteczność stosowanych zabezpieczeń,
- kładziemy duży nacisk na ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji.

Wszyscy pracownicy i współpracownicy SoftFlow Sp. z o.o. zobowiązani są do przestrzegania wymagań wynikających z niniejszej Polityki bezpieczeństwa informacji jak również związanych z nimi regulacjami (w tym procedurami, instrukcjami, wytycznymi, zaleceniami). W szczególności obowiązani są do:

- dbałości o bezpieczeństwo informacji,
- stosowania zabezpieczeń dokumentów i sprzętu informatycznego,
- zgłaszania wszystkich incydentów bezpieczeństwa informacji,
- zgłaszania propozycji rozwiązań systemowych i organizacyjnych służących poprawie poziomu bezpieczeństwa informacji.