POLITYKA BEZPIECZEŃSTWA INFORMACJI

1. Przeznaczenie i zakres stosowania

1.1. Niniejsza Polityka bezpieczeństwa informacji, zwana dalej „Polityką", została opracowana zgodnie z wymaganiami normy ISO 27001:2022 i określa podejście Spółki do zarządzania bezpieczeństwem informacji.

1.2. Przez bezpieczeństwo informacji Spółka rozumie zapewnienie poufności, integralności i dostępności aktywów informacyjnych podczas wykonywania działalności, świadczenia usług klientom oraz współpracy z zainteresowanymi stronami.

1.3. Przy stosowaniu Polityki uwzględnia się cele, wymagania i kontekst Spółki, charakter wykonywanej działalności, mające zastosowanie wymagania prawne, umowne, normatywne i inne obowiązujące wymagania, a także bieżące i prognozowane ryzyka oraz zagrożenia bezpieczeństwa informacji.

1.4. Wymagania systemu zarządzania bezpieczeństwem informacji są stosowane w Spółce z uwzględnieniem ustalonego zakresu stosowania systemu zarządzania bezpieczeństwem informacji i obejmują osoby wykonujące zadania w ramach tego zakresu oraz wykorzystywane aktywa informacyjne, z uwzględnieniem klasy informacji, mających zastosowanie wymagań i poziomu ryzyka.

2. Cele

2.1. Cele Polityki obejmują:

- zapewnienie poufności, integralności i dostępności informacji w ramach zakresu stosowania systemu zarządzania bezpieczeństwem informacji;
- zapewnienie zgodności z wymaganiami prawnymi, umownymi, normatywnymi i innymi obowiązującymi wymaganiami związanymi z bezpieczeństwem informacji;
- zapewnienie adekwatnych środków zarządzania ryzykiem związanym z bezpieczeństwem informacji;
- kształtowanie kultury bezpieczeństwa informacji wśród pracowników Spółki.

3. Zobowiązania najwyższego kierownictwa

3.1. Najwyższe kierownictwo Spółki zatwierdza niniejszą Politykę i zapewnia jej stosowanie.

3.2. Najwyższe kierownictwo zobowiązuje się do:

- zapewnienia spełniania wymagań normy ISO 27001:2022, wymagań prawnych, umownych, normatywnych i innych obowiązujących wymagań związanych z bezpieczeństwem informacji;
- zapewnienia zgodności systemu zarządzania bezpieczeństwem informacji z celami, kontekstem i kierunkiem rozwoju Spółki;
- ustanawiania ram dla określania celów bezpieczeństwa informacji;
- stosowania podejścia opartego na ryzyku w zarządzaniu bezpieczeństwem informacji;
- wyznaczania ról, odpowiedzialności i uprawnień niezbędnych do funkcjonowania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji;
- zapewnienia niezbędnych zasobów do funkcjonowania systemu zarządzania bezpieczeństwem informacji;
- zapewnienia ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji;
- zatwierdzania zmian niniejszej Polityki.

4. Podstawowe zasady bezpieczeństwa informacji

4.1. W Spółce stosuje się następujące podstawowe zasady bezpieczeństwa informacji:

- informacje są chronione z uwzględnieniem ich znaczenia, klasy, mających zastosowanie wymagań oraz bieżącego i prognozowanego ryzyka i zagrożeń bezpieczeństwa informacji;
- dostęp do informacji i aktywów informacyjnych jest przyznawany wyłącznie w ramach potrzeby służbowej i zatwierdzonych uprawnień;
- ryzyka bezpieczeństwa informacji są identyfikowane, oceniane, modyfikowane i przeglądane;
- środki ochrony informacji są ustanawiane z uwzględnieniem ryzyka, wymagań biznesowych, wymagań prawnych i umownych;
- obowiązki w zakresie bezpieczeństwa informacji są przypisywane określonym rolom;
- wyjątki i odstępstwa od wymagań bezpieczeństwa informacji są rozpatrywane, zatwierdzane, rejestrowane i przeglądane w ustalonym trybie;
- zdarzenia i incydenty bezpieczeństwa informacji są rejestrowane i obsługiwane w ustalonym trybie;
- pracownicy, wykonawcy, dostawcy i inne osoby uzyskujące dostęp do informacji Spółki lub klientów przestrzegają mających zastosowanie wymagań bezpieczeństwa informacji.

5. Komunikacja, dostępność i przegląd

5.1. Polityka stanowi podstawę do ustanawiania celów bezpieczeństwa informacji.

5.2. Polityka jest utrzymywana jako udokumentowana informacja, komunikowana pracownikom i innym osobom w zakresie odpowiednim do ich roli i wykonywanych zadań, a także dostępna dla zainteresowanych stron, jeżeli ma to zastosowanie.

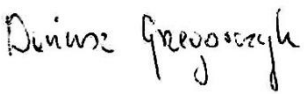
5.3. Polityka jest przeglądana w sposób planowy, przy istotnych zmianach działalności Spółki, zakresu stosowania systemu zarządzania bezpieczeństwem informacji, mających zastosowanie wymagań, ryzyka lub wyników przeglądu systemu zarządzania bezpieczeństwem informacji.

5.4. Polityka wchodzi w życie z dniem zatwierdzenia i obowiązuje do czasu zastąpienia jej nową wersją.

W imieniu Zarządu:

Donat Thomanek

Dariusz Grzegorczyk



SQD Alliance Sp. z o.o.
PL 43-200 Pszczyna, ul. Batorego 19
tel.: +48 32 326 30 08, fax: +48 32 447 09 18
e-mail: office.poland@sqda.pl