Polityka Bezpieczeństwa Informacji

BMETERS Polska Sp. z o.o. jest liderem w dziedzinie importu, eksportu, sprzedaży wodomierzy, ciepłomierzy, systemów zdalnego odczytu oraz produkcji wodomierzy i podzielników kosztów ogrzewania jak również doradztwa w zakresie rozliczania wody i ciepła. Poprzez śledzenie najnowszych światowych trendów i technologii oraz bogate doświadczenie i wiedzę naszych pracowników, możemy zaoferować najwyższą jakość i kompleksową obsługę na wszystkich etapach współpracy.

Mając świadomość znaczenia bezpieczeństwa informacji BMETERS POLSKA ustanowiła system zarządzania bezpieczeństwem informacji (SZBI), który jest projektowany, wdrażany, utrzymywany i systematycznie doskonalony zgodnie z wymaganiami normy ISO/IEC 27001:2022. Przyjęcie systemu zarządzania bezpieczeństwem informacji jest dla Spółki decyzją strategiczną. Skuteczne zarządzanie systemem i zgodność działania z wymaganiami systemu ma dla Spółki kluczowe znaczenie.

Nasze podejście do bezpieczeństwa informacji opiera się na modelu obejmującym: identyfikację, ochronę, wykrywanie, reagowanie oraz odzyskiwanie (Identify, Protect, Detect, Respond, Recover), przy czym koncentrujemy się na działaniach proaktywnych, monitorowaniu oraz skutecznym reagowaniu na zdarzenia lub incydenty.

Cele strategiczne BMETERS POLSKA w obszarze bezpieczeństwa informacji obejmują:

- opracowanie, wdrożenie oraz doskonalenie SZBI w celu zapewnienia poufności, integralności i dostępności informacji,
- utrzymanie adekwatności systemu i stosowanych zabezpieczeń względem zmieniających się zagrożeń, ryzyk oraz potrzeb Spółki oraz potrzeb stron zainteresowanych,
- integrację SZBI z procesami biznesowymi oraz strukturą zarządzania, w tym uwzględnienie bezpieczeństwa informacji w zarządzaniu projektami i w rozwoju systemów ICT,
- skuteczne zarządzanie ryzykiem w celu budowania zaufania interesariuszy,
- rozwój zabezpieczeń organizacyjnych i technicznych zgodnie z wynikami analizy ryzyka oraz obowiązującymi regulacjami,

- zapewnienie ciągłości działania, w tym zdolności do szybkiego odtworzenia dostępu do danych,
- minimalizowanie zakłóceń operacyjnych oraz utrzymanie bezpieczeństwa informacji w sytuacjach awaryjnych,
- bezpieczne i prawidłowe użytkowanie zasobów przetwarzania informacji,
- ochronę danych podczas ich przechowywania i transmisji,
- zapewnienie dostępu do systemów wyłącznie dla uprawnionych użytkowników,
- efektywne zarządzanie zdarzeniami i incydentami bezpieczeństwa informacji,
- podnoszenie świadomości i kompetencji personelu w zakresie bezpieczeństwa informacji.

Realizacja powyższych celów odbywa się poprzez:

- systematyczne gromadzenie i analizę informacji o zagrożeniach,
- cykliczne wyznaczanie celów bezpieczeństwa informacji w powiązaniu ze strategią Spółki,
- stosowanie mechanizmów kryptograficznych, kontroli dostępu oraz zarządzania aktywami,
- prowadzenie szkoleń z zakresu bezpieczeństwa informacji,
- zapewnienie odpowiednich zabezpieczeń fizycznych,
- regularne testowanie i ocenę skuteczności wdrożonych środków bezpieczeństwa.

Podejście Spółki do bezpieczeństwa informacji podlega regularnym, niezależnym przeglądom, a także jest aktualizowane w odpowiedzi na istotne zmiany.

Wszyscy pracownicy oraz osoby działające pod nadzorem Spółki są zobowiązani do przestrzegania zasad bezpieczeństwa informacji. Każda z tych osób ponosi odpowiedzialność za ochronę powierzonych informacji.

Zobowiązujemy się do spełniania mających zastosowanie wymagań w zakresie bezpieczeństwa informacji oraz do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji.

Psary, maj 2026