POLITYKA BEZPIECZEŃSTWA INFORMACJI I DANYCH

Najwyższe Kierownictwo Italmetal Sp. z o. o., będąc Administratorem zarządzającym informacjami i danymi dotyczącymi procesów w Organizacji, przestrzega zasad dotyczących bezpieczeństwa informacji oraz respektuje prawo do ochrony danych każdej organizacji lub osoby i deklaruje przestrzeganie normy PN-EN ISO 27001, ustawy RODO i wymagań prawnych w tym zakresie.

W tym celu w ITALMETAL Sp. z o. o. zastosowano i wdrożono monitorowany system zarządzania informacjami i danymi zapewniający:

- Formalizację dokumentacji systemu ochrony informacji i danych;
- Ochronę informacji i danych pracowników i wszystkich stron zainteresowanych;
- Prawidłowe wykorzystanie tych informacji i danych zapewniając zgodność z przepisami prawa;
- Nienaruszanie praw poszanowania innych organizacji oraz osób fizycznych;
- Zapewnienie każdemu prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu;
- Poszanowanie różnorodności kulturowej, religijnej i językowej.

Dla realizacji Polityki Bezpieczeństwa Informacji i Danych są stosowane następujące metody:

- Ocena potencjalnych skutków poprzez analizy ryzyka, za wykonanie której odpowiada Administrator;
- Nadawanie i anulowanie upoważnień do sporządzania, przekazywania i przetwarzania informacji i danych w zbiorach papierowych, systemach informatycznych i innych nośnikach;
- Wdrożenie instrukcji postępowania z możliwymi incydentami tak, aby zminimalizować potencjalne skutki ich wystąpienia oraz ograniczyć ryzyko powstania zagrożeń i występowania incydentów w przyszłości;
- Zabezpieczenie przed zdarzeniami losowymi zewnętrznymi jak pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności, awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki personelu, użytkowników, utrata/zagubienie danych;
- Zabezpieczenie przed umyślnymi incydentami jak włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania;
- Zakaz świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych;
- Wdrożenie i respektowanie Regulaminu Ochrony Danych zapewniając wymaganą wiedzę osób przetwarzających dane odnośnie bezpiecznych zasad przetwarzania, zapewniają zachowanie poufności informacji i danych;
- Realizację szkoleń każdej osoby przed dopuszczeniem do pracy z informacjami lub danymi;
- Utrzymanie przez Administratora Rejestrów upoważnień i czynności przetwarzania informacji i danych w zbiorach danych;
- Realizację planowanych, regularnych auditów w celu zweryfikowania i ocenie skuteczności podjętych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo informacji i danych;
- Procedury przywrócenia dostępności upoważnionym do informacji i danych w razie incydentu fizycznego lub technicznego osobowych;
- Stosowane zabezpieczeń systemowych w celu ochrony danych, tym okresowe backupy;
- Utrzymanie systemu nadawania lub anulowania upoważnień przez Administratora;
- Współpraca z klientami oraz certyfikowanymi, zakwalifikowanymi dostawcami usług i systemów informatycznych;
- Utrzymanie i zabezpieczenie przed dostępem przez osoby nieupoważnione do obszarów ochronnych i archiwów informacji i danych;
- Szyfrowanie wrażliwych danych przesyłanych metodami informatycznymi;
- Nieodwracalne niszczenie nieaktualnych informacji i danych;
- Zakaz kopiowania i rozpowszechniania informacji i danych bez zgody ich twórcy, właściciela zarządzającego lub Administratora.

Każda osoba, stosownie do swoich obowiązków, jest zobowiązana przyjąć do wiadomości i przestrzegać Politykę Bezpieczeństwa Informacji i Danych oraz powiadamiania o stwierdzeniu nieprawidłowości, podatności lub wystąpieniu incydentu do bezpośredniego przełożonego.

Prezes Zarządu
Girardini Attilio

Jelcz-Laskowice, 2 stycznia 2024.