POLITYKA BEZPIECZEŃSTWA

POLITYKA BEZPIECZEŃSTWA JEST ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.

SPIS TREŚCI

03

POLITYKI, PROCEDURY, INSTRUKCJE

Polityka jest formalnym, krótkim i (high-level statement) wysokopoziomowym oświadczeniem lub planem, który określa ogólne cele organizacji jak również ustala ważne założenia, wartości i zobowiązania którymi kieruje się firma i powinni kierować się pracownicy. Dodatkowo może zawierać odnośniki do procedur dla konkretnych obszarów tematycznych które doprecyzowują politykę lub polityki. Najbardziej szczegółowe jednak są instrukcje, które z kolei mogą być uzupełnieniem procedur.

Innymi słowy: polityki określają, co należy chronić i jakie są podstawowe zasady i cele. Procedury określają, w jaki sposób chronić zasoby lub jak prowadzić politykę. Na przykład w polityce zasady dotyczące haseł opisują zasady budowy haseł, zasady ochrony hasła i częstotliwość ich zmiany. Procedura zarządzania hasłami natomiast nakreśliłaby proces tworzenia nowych haseł, przekazywania ich, a także proces zapewniania zmiany haseł na krytycznych urządzeniach (jednak nie zawsze będzie istniał stosunek jeden do jednego między polityką a procedurami).

Główna polityka powinna być ogólnodostępnym dokumentem, zakomunikowanym wszystkim zainteresowanym stronom (pracownikom oraz stronom zewnętrznym). Z kolei bardziej szczegółowe polityki, czy instrukcje mogą być dokumentami poufnymi, dostępnymi tylko do określonych grup odbiorców.

Polityka powinna być dokumentem zatwierdzonym przez kierownictwo firmy.

04

PRZYKŁAD POLITYKI BEZPIECZEŃSTWA

Wprowadzenie

CEL

Celem polityki jest ochrona aktywów i zapewnienie ciągłości biznesowej podmiotu. Zawiera ona wytyczne służące osiągnięciu tych celów. Została przygotowana zgodnie z najlepszymi praktykami i standardami ..... (i.e. PPBW Standard)

ZAKRES

Zasady tej Polityki określają minimalne wymagania dotyczące zapewnienia bezpiecznego środowiska IT w firmie. Zasady te dotyczą kierownictwa firmy, pracowników, kontrahentów, agentów i dostawców. Obejmują one również technologię i wyposażenie zasobów informacyjnych firmy.

COMPLIANCE (ZGODNOŚĆ)

Wszyscy pracownicy firmy są odpowiedzialni za zrozumienie i przestrzeganie wszystkich zasad bezpieczeństwa zawartych w niniejszej polityce i towarzyszących jej dokumentach. Nieprzestrzeganie polityki/łamanie jej zapisów może skutkować postępowaniem dyscyplinarnym, włącznie z natychmiastowym zwolnieniem, postępowaniem karnym i / lub utratą dostępu do zasobów firmy.

Wszelkie sytuacje związane z niezgodnościami należy zgłaszać.

05

POLITYKA FIRMY

Informacje korporacyjne, obiekty i wszystkie inne aktywa będą wykorzystywane w sposób zatwierdzony, etyczny i zgodny z prawem, aby uniknąć szkody lub utraty ciągłości działalności, negatywnego wpływu na interesy finansowe lub wizerunek firmy. Celem jest także przestrzeganie oficjalnych akceptowanych zasad i procedur użytkowania. Personel skontaktuje się z szefem ds. Bezpieczeństwa informacji (CISO) przed podjęciem jakichkolwiek działań, które nie są wyraźnie objęte tymi zasadami.

ROLE I OBOWIĄZKI

Role i obowiązki dotyczące akceptowalnego wykorzystania są określone w następujących sekcjach.

Główny odpowiedzialny ds. Bezpieczeństwa informacji

Główny osoba odpowiedzialna za aspekty Bezpieczeństwa informacji odpowiada za ustanowienie, egzekwowanie i aktualizacje korporacyjnej polityki bezpieczeństwa.

Kadra zarządzająca

Menedżerowie (kadra zarządzająca) są odpowiedzialni za:

- informowanie personelu o zasadach korporacyjnych dotyczących dopuszczalnego wykorzystania zasobów informacyjnych,
- Zapewnienie, że personel pod ich nadzorem przestrzega tych zasad i procedur.

06

ROLE I OBOWIĄZKI

Administratorzy systemów

Administratorzy są odpowiedzialni za:

- zapewnienie dostępności, integralności i poufności systemów oraz przetwarzanych w nich danych,
- zgłaszanie podejrzeń lub wystąpienie nieupoważnionej działalności.

Wszyscy pracownicy

Cały personel będzie odpowiedzialny za:

- przestrzeganie oficjalnych zasad korporacyjnych dotyczących dopuszczalnego wykorzystania zasobów informacyjnych,
- natychmiastowe zgłaszanie podejrzenia lub wystąpienia wszelkich incydentów.

Audytorzy

- Audytorzy są odpowiedzialni za kontrolę zgodności.

07

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Organizacja musi rejestrować, utrzymywać i aktualizować wykaz swoich zasobów (lub aktywów) informacyjnych i zapewniać odpowiednie środki, aby zapewnić ochronę poufności, integralności i dostępności informacji będących własnością Spółki lub powierzonych firmie.

Klasyfikacja informacji

Wszystkie informacje, dane i dokumenty muszą być skategoryzowane i oznakowane, aby wszyscy użytkownicy byli świadomi własności i klasyfikacji informacji.

Przechowywanie i obsługa informacji

Wszyscy użytkownicy systemów informatycznych muszą zarządzać tworzeniem, przechowywaniem, przesyłaniem, poprawianiem, kopiowaniem i usuwaniem/niszczeniem plików danych w sposób, który chroni poufność, integralność i dostępność takich plików.

Kontrola dostępu

Standardy kontroli dostępu do systemów informatycznych muszą zostać ustanowione przez kierownictwo i powinny uwzględniać potrzebę równoważenia ograniczeń, tak aby był zachowany balans między poziomem ograniczeń dostępu a potrzebami biznesowymi. Dostęp do zasobów powinien być tylko w takim zakresie jak wymaga tego potrzeba biznesowa.

08

BEZPIECZEŃSTWO FIZYCZNE

Należy zastosować odpowiednie zabezpieczenia fizycznego dostępu do zasobów, współmierne do zidentyfikowanego poziomu akceptowalnego ryzyka.

CIĄGŁOŚĆ DZIAŁANIA

Gwarantuje się ciągłość ważnych procesów biznesowych poprzez ustanowienie formalnego i kompleksowego planu ciągłości działania.

ŚWIADOMOŚĆ BEZPIECZEŃSTWA

W celu zwiększenia świadomości pracowników firmy i edukowania ich w zakresie zagrożeń i odpowiednich zabezpieczeń powinien być realizowany program edukacyjny uświadamiający bezpieczeństwo informacji.

ZGODNOŚĆ Z POLITYKĄ BEZPIECZEŃSTWA

Zgodność z zasadami bezpieczeństwa jest obowiązkowa dla wszystkich pracowników firmy, wykonawców, agentów i dostawców. Zgodność z polityką musi być egzekwowana przez okresowe audyty.

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Polska Platforma Bezpieczeństwa Wewnętrznego

ul. Słowackiego 17/11
60-822 Poznań
www.ppbw.pl
tel.: (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

Fundusze Europejskie Inteligentny Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.