Polityka 5 zasad cyberbezpieczeństwa

Cele i zakres dokumentu

Celem „Polityki 5 zasad cyberbezpieczeństwa" jest promowanie odpowiedzialnego korzystania z internetu oraz zasobów IT przez pracowników Banku. Wszyscy z nich mają udział w ochronie danych i są zobowiązani przestrzegać określonych zasad cyberbezpieczeństwa.

Jakie zagadnienia związane z ESG opisuje polityka?

Określone w dokumencie zasady cyberbezpieczeństwa dotyczą zagadnień takich jak:

1) ochrona danych oraz osobistego sprzętu IT,
2) zachowanie pracowników w internecie, w tym w mediach społecznościowych,
3) ochrona przed atakami phishingowymi,
4) odpowiednie stosowanie i ochrona haseł,
5) zgłaszanie podejrzanych sytuacji do odpowiednich zespołów czuwających nad cyberbezpieczeństwem.

Ponadto polityka określa wymogi dotyczące podnoszenia kompetencji pracowników. Precyzuje, że szkolenia oparte na 5 zasadach cyberbezpieczeństwa są obowiązkowe dla każdego pracownika. W zależności od pełnionej roli pracownik może mieć również obowiązek wykonania innych szkoleń dodatkowych. Ponadto określa zasady prowadzenia regularnych testów phishingowych. Stanowią one praktyczny element edukacyjny dla pracowników – uczą się w ten sposób rozpoznawać techniki stosowane przez cyberprzestępców.

Najwyższy szczebel zarządzania, który odpowiada za politykę

Nadzór nad zapisami polityki sprawują:

- Chief Information Security Officer (CISO), który raportuje bezpośrednio do wiceprezesa zarządu kierującego Pionem Transformacji Cyfrowej,
- Zarząd Banku.

Stosowanie w spółkach zależnych Banku

Polityka obowiązuje w Grupie Kapitałowej.