Definicja strategii bezpieczeństwa

1. Bezpieczeństwo Key Solutions Polska to stan określony przez przyjęty zbiór norm, zasad, rozwiązań oraz środków i metod ochrony zasobów, którego miarą jest poziom ryzyka naruszenia dostępności, poufności lub integralności tych zasobów.
2. Bezpieczeństwo informacji Key Solutions Polska jest zapewnione, jeżeli ryzyko naruszenia dostępności, poufności lub integralności chronionych zasobów w Key Solutions nie przekracza akceptowalnych parametrów przy zachowaniu zasad sformułowanych w niniejszej Polityce.
3. Wprowadzenie PBI ma na celu obniżanie zidentyfikowanych ryzyk.

Cel strategii bezpieczeństwa

1. Zapewnienie wymaganego zaangażowania pracowników w utrzymanie bezpieczeństwa systemów informacyjnych, określenie kierunków rozwoju zarządzania bezpieczeństwem tych systemów, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa oraz zagwarantowanie sprawnego funkcjonowania Key Solutions Polska.

Deklaracja Kierownictwa Key Solutions Polska

1. PBI wyznacza kierunek działania Kierownictwa oraz pracowników Key Solutions Polska w celu zapewnienia systemowego nadzoru nad gromadzeniem, przetwarzaniem, przechowywaniem i udostępnianiem informacji, niezależnie od sposobu realizacji tych procesów.
2. Kierownictwo Key Solutions Polska zapewnia bezpieczeństwo zasobów oraz informacji zawartych w systemach informacyjnych Key Solutions Polska i poza nimi, w sposób opisany w PBI, ponieważ mają one fundamentalne znaczenie dla realizacji misji i celów statutowych Key Solutions Polska.
3. PBI wyraża wolę Kierownictwa Key Solutions Polska w zakresie ochrony jej zasobów.
4. Kierownictwo Key Solutions Polska aktywnie wspiera procesy zmierzające do zapewnienia bezpieczeństwa przetwarzania informacji poprzez wdrażanie, rozwój, uaktualnianie PBI oraz regulacji z niej wynikających.
5. PBI oraz regulacje z niej wynikające obowiązują wszystkich pracowników, stażystów, praktykantów, wolontariuszy oraz inne osoby fizyczne, prawne lub nieposiadające osobowości prawnej, które uzyskują dostęp do zasobów Key Solutions Polska, poza użytkownikami informacji publicznie dostępnych.
6. Kierownictwo Key Solutions Polska odpowiada za zapewnienie środków na te cele.
7. PBI ustala wytyczne do stworzenia zasad ochrony systemów informacyjnych, ze szczególnym uwzględnieniem systemu teleinformatycznego Key Solutions Polska i zawartych w nich informacji.

8. Każdy pracownik, stażysta, praktykant, wolontariusz oraz inna osoba fizyczna, prawna lub nieposiadająca osobowości prawnej, która uzyskuje uprawnienie/upoważnienie dostępu do zasobów Key Solutions Polska zostaje zapoznany z PBI, potwierdza ten fakt pisemnym oświadczeniem oraz zobowiązuje się przestrzegać zasady, reguły i postanowienia z nich wynikające.
9. Procedury i regulacje wewnętrzne Key Solutions Polska nie mogą naruszać zapisów określonych w PBI.

Regulacje ogólne

1. Życie i zdrowie osób jest dobrem najwyższym i ich ochrona w sytuacji zagrożenia jest ważniejsza niż ochrona jakichkolwiek innych zasobów.
2. Ponad to ochronie podlegają:
    a. informacje przetwarzane w Key Solutions Polska, niezależnie od ich formy i nośnika, w tym dane osobowe
    b. sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania informacji w Key Solutions Polska,
    c. pomieszczenia, w których znajduje się kluczowy sprzęt informatyczny, dokumenty zawierające tajemnice prawnie chronione, w tym dane osobowe,
    d. oprogramowanie wykorzystywane w Key Solutions Polska,
    e. wizerunek Key Solutions Polska,
    f. pozostałe mienie wykorzystywane w Key Solutions Polska,
3. Celem ustanowienia PBI jest zapewnienie poufności, dostępności, integralności, przy zachowaniu autentyczności, niezaprzeczalności i rozliczalności, informacji przetwarzanych w Key Solutions Polska.
    a. Poufność informacji - oznacza, że jest ona dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji.
    b. Dostępność informacji - oznacza możliwość wykorzystania zasobu przez upoważnioną osobę, na każde uzasadnione żądanie, w ustalonym czasie.
    c. Integralność informacji - oznacza, że informacja nie uległa zmianie od czasu ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób.
    d. Autentyczność - właściwość polegającą na tym, że pochodzenie lub zawartość danych jest taka jak deklarowana.
    e. Niezaprzeczalność - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
    f. Rozliczalność - właściwość pozwalającą przypisać określone działanie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.
4. Bezpieczeństwo informacji w Key Solutions Polska osiąga się wdrażając zabezpieczenia techniczne i organizacyjne w szczególności poprzez: zarządzenia, procedury, zasady, instrukcje zapewniające przejrzystą strukturę organizacyjną oraz przez bieżący przegląd prawidłowego funkcjonowania oprogramowania i sprzętu, służącego do przetwarzania

informacji. Zabezpieczenia te są monitorowane w celu ich ciągłego doskonalenia.

5. Bezpieczeństwo Informacji Key Solutions Polska obejmuje nie tylko siedzibę Key Solutions Polska, ale także wszelkie sytuacje, w których informacje związane z działalnością Key Solutions Polska są przetwarzane poza jego siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci komputerowej Key Solutions Polska.