Środki Techniczne i Organizacyjne
Minimalne środki techniczne i organizacyjne gwarantujące bezpieczeństwo powierzonych do przetwarzania danych osobowych

1. Kontrola dostępu do lokali i obiektów, w których przetwarzane są dane.
Ryzyko nieuprawnionego dostępu do danych (w sensie fizycznym).

Wymagane środki techniczne i organizacyjne służące do kontroli dostępu do lokali i obiektów, w szczególności do kontroli autoryzacji:

a) system kontroli dostępu (czytnik identyfikatorów, karta magnetyczna, karta z chipem),
b) ochrona, dozorcy,
c) sejfy,
d) urządzenia do nadzoru (system alarmowy, monitor wideo/CCTV),
e) regularne przeglądy pozwoleń na stały dostęp.

2. Kontrola dostępu do systemów.
Ryzyko nieuprawnionego dostępu do systemów informatycznych.

Wymagane techniczne (identyfikator/zabezpieczenie hasłem) i organizacyjne (podstawowe dane użytkownika) środki służące do identyfikacji użytkownika i uwierzytelniania:

a) procedury dotyczące hasła (minimalna długość, złożoność hasła, regularna zmiana hasła),
b) automatyczna blokada dostępu (np. koniec czasu w systemie),
c) zarządzanie reakcjami na incydenty.

3. Kontrola dostępu do danych.
Ryzyko dostępu do danych przez osoby nieuprawnione.

Wymagane zabezpieczenia:

a) zróżnicowane prawa dostępu (profile, role, grupy uprawnień, transakcje i obiekty),
b) raporty z wykonywnych prac,
c) unikalny identyfikator użytkownika.

4. Kontrola ujawnienia**.**
Ryzyko ujawnienia danych: przesyłanie elektronicznie, transport danych, przekazywanie danych itp., aby zapobiegać utracie, zmianie lub nieuprawnionemu ujawnieniu.

Wymagane zabezpieczenia:

a) szyfrowanie/tunelowanie (VPN = Virtual Private Network - Wirtualna Sieć Prywatna),

b) szyfrowanie SSL,
c) logowanie do nośników.

5. Zasada rozliczalności wprowadzanych danych.
Ryzyko braku zapewnienia rozliczalności danych poprzez umożliwienie weryfikacji osób dokonujących operacji na danych.

Wymagane zabezpieczenia:

a) raporty z wykonywanych prac,
b) unikalny identyfikator użytkownika.

6. Kontrola dostępności/ integralności danych.
Dane należy chronić przed przypadkowym zniszczeniem lub utratą poprzez stosowanie fizycznych/logicznych środków zabezpieczeń.

Wymagane zabezpieczenia:

a) procedury dotyczące kopii zapasowych,
b) nieprzerwana dostawa zasilania (UPS),
c) systemy antywirusowe / firewalle,
d) plan odzyskiwania na wypadek katastrofy.

Podmiot Przetwarzający

Podpis:

_____
Imię, nazwisko, data

Podpis:

_____
Imię, nazwisko, data