

Ogólne zalecenia dla pomieszczeń w których przetwarzane są dane osobowe.

Serwer zawierający dane osobowe musi znajdować się w pomieszczeniu zabezpieczonym systemem kontroli dostępu klasy SA3 lub wyższym, zgodnie z Polską Normą.

Reguluje to ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z dnia z dnia 1 maja 2004 r.)

Zalecane wymogi bezpieczeństwa fizycznego

Obszar, w którym dane osobowe podlegają przetwarzaniu i zbieraniu zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Przebywanie osób nieuprawnionych w tymże obszarze jest dopuszczalne za zgodą administratora danych osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Serwerownia powinna być wydzielonym pomieszczeniem, gdzie ściany zewnętrzne mają solidną konstrukcję, nie ma luk lub punktów przez które łatwo się włamać, oraz jest wyposażona w drzwi antywłamaniowe. Drzwi powinny być wyposażone w dwa zamki, zgodnie z wymaganiami zawartymi w Polskiej Normie PN-90/B-92270 (*Elementy i segmenty ścienne metalowe - Drzwi o zwiększonej odporności na włamanie, zamki klasy C*).

W przypadku, gdy pomieszczenie serwerowni posiada okna, otwory okienne serwerowni zlokalizowanej na parterze winny być okratowane lub zabezpieczone w inny równoważny sposób.

Do pomieszczeń należy wprowadzić system kontroli dostępu, który może być realizowany:

- a) na drodze proceduralnej – dzienniki (rejestry) wejść i wyjść z pomieszczeń prowadzone przez upoważnioną osobę lub
- b) na drodze systemu elektronicznego – elektroniczny rejestr wejść/wyjść. Dostęp do pomieszczenia jest możliwy tylko po okazaniu karty zbliżeniowej. System powinien być sprzężony z zamkami w drzwiach, tj. okazanie prawidłowej karty zbliżeniowej winno wyzwoić otwarcie zamków do serwerowni.

Niezależnie od zabezpieczenia fizycznego opisanego powyżej, należy wprowadzić system alarmowy klasy SA3 (lub wyższej).

Zalecane jest, aby prace związane z instalacją systemu alarmowego prowadzone były przez pracowników posiadających **Licencję pracownika zabezpieczenia technicznego II stopnia**. Licencje wydawane są przez Komendy Wojewódzkie Policji.

Dla systemu klasy SA3 należy stosować urządzenia (peryferia) systemu alarmowego posiadające atest przynajmniej poziomu „C” (czyli zabezpieczenia profesjonalne). Innymi słowy, system alarmowy SA3 zawiera komponenty posiadające atest przynajmniej poziomu „C”. Opcjonalnie dopuszczalne są urządzenia klasy „S” czyli zabezpieczenia specjalne. Inne atesty („A”, „B”) nie mogą być stosowane.