Załącznik nr 8 do „Polityki Bezpieczeństwa"

Określenie środków technicznych i organizacyjnych
niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. ABI wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

5. Środki ochrony, zastosowane przez ABI dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   - środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
   - środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS) ;
   - środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym);

6. Zastosowane środki ochrony fizycznej pomieszczeń:

LP	ZASTOSOWANY ŚRODEK OCHRONY FIZYCZNEJ
1.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C
3.	Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy
4.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.
5.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.
6.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej
7.	Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie
8.	Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy
9.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów

7. Zastosowane środki techniczne obejmują:

LP	ZASTOSOWANY ŚRODEK OCHRONY TECHNICZNEJ
1.	Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.

2.	Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
3.	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4.	Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
5.	Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
6.	Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
7.	Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
8.	Użyto system Firewall do ochrony dostępu do sieci komputerowej.
9.	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
10.	Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
11.	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
12.	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
13.	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
14.	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

8. Zastosowane środki organizacyjne obejmują:

LP	ZASTOSOWANY ŚRODEK OCHRONY ORGANIZACYJNEJ
1.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych
2.	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego
3.	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
4.	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane
5.	Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.
W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

BURMISTRZ

Administrator Danych

01.07.2015 r. inż. Tadeusz Mikulski