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

załącznik nr 7 do Polityki Bezpieczeństwa zgodnie z § 4 pkt 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100 poz. 1024)

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

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

3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje Informatyk.

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 Informatyka 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. utworzenie Instrukcji zarządzania systemem informatycznym);

6. Zastosowane środki:

1) ŚRODKI OCHRONY FIZYCZNEJ DANYCH:
   a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),

   b) Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej,

   c) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy,

   d) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer,

   e) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,

   f) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie niemetalowej lub metalowej,

   g) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie niemetalowej lub metalowej, sejfie, lub kasie pancernej,

   h) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy,

   i) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2) ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

a) Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

b) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

c) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,

d) Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł,

e) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych,

f) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,

g) Użyto system Firewall do ochrony dostępu do sieci komputerowej,

h) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

i) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,

j) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych,

k) Zastosowano kryptograficzne środki ochrony danych osobowych,

l) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,

m) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

3) ŚRODKI ORGANIZACYJNE:

a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,

c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

e) 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.

7. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

8. W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą.

9. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

Data i podpis Administratora Danych Osobowych

….....