ZARZĄDZENIE NR 18/2007

Dyrektora Powiatowego Urzędu Pracy w Cieszynie
z dnia 16 listopada 2007r.

w sprawie wprowadzenia Polityki Bezpieczeństwa dla Powiatowego Urzędu Pracy w Cieszynie

Na podstawie § 17 ust. 1 pkt 8 Regulaminu organizacyjnego Powiatowego Urzędu Pracy w Cieszynie (uchwała Zarządu Powiatu Cieszyńskiego nr 82/ZP/II/2006 z dnia 25.05.2006r.

zarządzam, co następuje:

§1

Wprowadzam Politykę Bezpieczeństwa dla Powiatowego Urzędu Pracy w Cieszynie, stanowiącą załącznik do niniejszego zarządzenia.

§2

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
POWIATOWEGO URZĘDU PRACY
mgr Anna Stefaniak-Bacza

RADCA PRAWNY
mgr Anna Mertuszka

Załącznik do
Zarządzenia nr 18/07
Dyrektora
Powiatowego Urzędu Pracy
w Cieszynie
z dnia 16.11.2007.r.

Polityka Bezpieczeństwa
dla Powiatowego Urzędu Pracy
w Cieszynie

Polityka bezpieczeństwa określa sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Podstawa prawna

- Konstytucja Rzeczypospolitej Polskiej art. 47, 51;
- Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (t. j. Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.);
- 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 2004r. Nr 100, poz. 1024).

Polityka bezpieczeństwa została oparta również na zapisach Polskiej Normy PN-ISO/IEC 17799, PN-I-02000 oraz PN-I-13335-1 określających praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, która jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji". W zaleceniach dotyczących dokumentu określającego politykę bezpieczeństwa informacji wskazuje się tam, że dokument polityki bezpieczeństwa powinien być zatwierdzony przez kierownictwo, opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom.

Definicje

- **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
- **Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
- **System informatyczny** - system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. *W szczególności systemem informacyjnym może być system, w którym nie będzie żadnego komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy.* Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;
- **Bezpieczeństwo systemu informatycznego** - wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą
- **Administrator Danych Osobowych (ADO)** - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Dyrektor Urzędu, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;
- **Administrator Bezpieczeństwa Informacji (ABI)** - należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- **Administrator Systemów Informatycznych (ASI)** - należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych zastosowanie technicznych i organizacyjnych środków ochrony danych osobowych,
- **Osoba upoważniona lub użytkownik systemu** - osoba posiadająca

upoważnienie wydane przez ADO lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;

- **Osoba uprawniona** - osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności;
- **Sieć Lokalna (LAN** Local Area Network**)** - Lokalna sieć teleinformatyczna;
- **Sieć rozległa (WAN)** - Rozległa sieć teleinformatyczna;
- **Identyfikator użytkownika (LOGIN) -** ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Hasło (Password)-** ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- **Zalogowanie** - uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Odbiorcy danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą
  - osoby, upoważnionej do przetwarzania danych,
  - przedstawiciela, o którym mowa w art. 31 a ustawy o ochronie danych osobowych,
  - podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Cele

Celem przeprowadzonej analizy bezpieczeństwa jest ochrona systemu informatycznego jako całości, jego poszczególnych elementów, przetwarzanego przez system zbioru danych, obszaru, w którym przetwarzane są dane oraz osób, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.

Niniejsza polityka bezpieczeństwa zawiera:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane (załącznik 1);
2) wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób (załącznik 2);
3) opis struktury zbiorów danych (załącznik 3);
4) opis rejestracji baz danych (załącznik 4);
5) środki techniczne i organizacyjne (załącznik 5);
6) instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji (załącznik 6);
7) instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik 7);
8) wykaz osób upoważnionych do przetwarzania danych osobowych (załącznik 8).

Załącznik Nr 1

Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane

Wykaz pomieszczeń lub części pomieszczeń w których przetwarzane są dane w budynku Powiatowego Urzędu Pracy w Cieszynie ul. Kochanowskiego 8

L.p.	Nr pokoju	Dział / Dyrekcja
1.	1	Dział Informacji Ewidencji i Świadczeń
2.	2	Dział Informacji Ewidencji i Świadczeń
3.	101	Dział Pośrednictwa Pracy i Szkoleń
4.	102	Dział Pośrednictwa Pracy i Szkoleń
5.	103	Dział Pośrednictwa Pracy i Szkoleń
6.	105	Dział Organizacyjno-Prawny i Administracji
7.	106	Dział Programów Rynku Pracy i Poradnictwa Zawodowego
8.	107	Dział Programów Rynku Pracy i Poradnictwa Zawodowego
9.	108	Dział Programów Rynku Pracy i Poradnictwa Zawodowego
10.	109	Dział Pośrednictwa Pracy i Szkoleń
11.	110	Dział Pośrednictwa Pracy i Szkoleń
12.	201	Dział Organizacyjno-Prawny i Administracji
13.	202	Dział Informacji Ewidencji i Świadczeń
14.	203	Dział Programów Rynku Pracy i Poradnictwa Zawodowego
15.	204	Dział Programów Rynku Pracy i Poradnictwa Zawodowego
16.	205	Dział Informacji Ewidencji i Świadczeń, Dział Organizacyjno-Prawny i Administracji
17.	206	Dział Finansowo-Księgowy
18.	206a	Dział Finansowo-Księgowy
19.	207	Dział Organizacyjno-Prawny i Administracji
20.	207a	Dyrektor
21.	207b	Zastępca Dyrektora
22.	208	Dział Organizacyjno-Prawny i Administracji
23.	209	Dział Finansowo-Księgowy
24.	210	Dział Organizacyjno-Prawny i Administracji
25.	217	Dział Organizacyjno-Prawny i Administracji

Załącznik Nr 2

Wykazy zbiorów przetwarzanych elektronicznie lub w inny sposób

8

Wykaz zbiorów przetwarzanych elektronicznie

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania
1.	Dane bezrobotnych	PULS
2.	Dane bezrobotnych	Płatnik
3.	Dane bezrobotnych	SEB
4.	Dane pracowników	Płatnik

Wykaz zbiorów przetwarzanych w inny sposób niż elektro...cznie

Lp.	Nazwa zbioru	Cel przetwarzania danych	Dział	Osoby przetwarzające dane	Rodzaj danych	Pomieszczenie, w którym przetwarza się dane
1.	Baza danych pism i korespondencji	Baza danych pism i korespondencji	Dział Organizacyjny – Sekretariat	Wszyscy pracownicy upoważnieni	Dane w formie papierowej, listy, CV,	Wszystkie pomieszczenia

Załącznik Nr 3

Opis struktury zbiorów danych

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduję się formie elektronicznej na dołączonej płytce w plikach wg poniższej tabeli.

L.p.	Nazwa systemu	Nazwa pliku	Katalog
1.	PULS	PULS_Struktura_Danych	CD:\PULS
2.	Płatnik	PŁATNIK_Struktura_Danych	CD:\PŁATNIK

Załącznik Nr 4

Sposób przepływu danych pomiędzy poszczególnymi systemami

System informatyczny SEB, to poprzedni system używany w Powiatowym Urzędzie Pracy w Cieszynie. Ponieważ nie wszystkie informacje zostały przemigrowane do nowego systemu stanowi on archiwum. Nie ma powiązania z nowym systemem informatycznym PULS oraz systemem Płatnik.

Dane dot. osób bezrobotnych pomiędzy systemem informatycznym PULS a Programem Płatnik przekazywane są za pomocą przekazu elektronicznego (pliki .kdu). W plikach tych przenoszone są następujące dane:

- Nazwisko
- Pierwsze imię
- PESEL
- Numer NIP
- Seria i nr dokumentu tożsamości
- Adres

Natomiast dane dot. Pracowników Urzędu uzupełniane są ręcznie w Programie Płatnik.

Załącznik Nr 5

Środki Techniczne i Organizacyjne

Środki techniczne i organizacyjne

Część ta zawiera opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Szczególny opis zawarto w „**Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji**". (załącznik nr 6)

Środki organizacyjne

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych.
3. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie pisemnego zezwolenia administratora danych osobowych.
7. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
8. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
10. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.

12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

Środki techniczne

1. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
2. Stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
3. W przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu.
4. Po zakończeniu pracy komputery (notebook) taki powinny być zabezpieczone w zamykanych na klucz szafach.
5. Komputerów tych nie wolno wynosić poza budynek.
6. W wypadku potrzeby wyniesienia wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy.
7. Nie należy udostępniać osobom nieupoważnionym tych komputerów.
8. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
9. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
10. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
11. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
12. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
13. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
14. Do zabezpieczenia sieci należy stosować:
    a) firewall,
    b) adresowanie stacji roboczych tylko adresami prywatnymi, nierutowalnymi,
    c) systemy wykrywania włamań IDS,
    d) systemy antywirusowe,

e) zabezpieczenia skrzynek poczty elektronicznej hasłami "trudnymi" (8 znaków w tym litery, cyfry, znaki dodatkowe),

f) zabezpieczenia stacji roboczych poprzez hasła na BIOS, w systemach MS Windows 2000, i XP poprzez użytkowników i hasła.

Załącznik Nr 6

INSTRUKCJA

określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji

1. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.

a) hasło nie powinno zawierać mniej niż 8 znaków,
b) hasło nie może być takie samo jak identyfikator,
c) hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, administratora bezpieczeństwa informacji lub automatycznie przez system,
d) użytkownikowi nie wolno zapisywać hasła na papierze,
e) użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
f) komputery nie pracujące w sieci muszą mieć hasło założone na BIOS,
g) w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, z wyłączeniem sytuacji gdy po 2 minutach uruchomi się wygaszacz ekranu zabezpieczony hasłem,
h) za gospodarkę hasłami odpowiedzialny jest administrator bezpieczeństwa informacji,
i) hasło przy wpisywaniu nie może być wyświetlane na ekranie.

2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

a) administrator bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych , zawierającą ich identyfikatory,

Imię	Nazwisko	Identyfikator Netware	Identyfikator PULS

b) rejestracji użytkowników w systemie dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
c) zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
d) wyłączenie z ewidencji osób upoważnionych do przetwarzania danych,

obliguje administratora bezpieczeństwa informacji do odebrania dostępu do danych osobowych,

e) zalecane jest aby identyfikator składał się z pierwszej litery imienia i nazwiska.

3. Procedury rozpoczęcia i zakończenia pracy

a) administrator bezpieczeństwa informacji danych w porozumieniu z kierownikiem urzędu, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie kierownik jednostki, w formie upoważnienia jednorazowego lub stałego,

b) administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona, nadzoruje rozpoczęcie i zakończenie pracy systemu informatycznego,

c) w pomieszczeniach gdzie przyjmowani są klienci , monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,

d) dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania p-poż i UPS,

e) kontrola wprowadzanych danych prowadzona jest na bieżąco na kadmy stanowisku merytorycznym, nadzór prowadzi kierownik danej komórki organizacyjnej,

f) o przekazywaniu danych osobowych innym podmiotom decyduje ADO,

g) osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się, na tablicy ogłoszeń, z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.

4. Metoda i częstotliwość tworzenia kopii awaryjnych

a) za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,

b) kopii należy dokonywać poprzez przegrywanie (backup) całej bazy danych (bez kompresji),

c) w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia, miesiąca, kwartału i półrocza. Kopie należy zapisywać na taśmach magnetycznych lub płytach CD lub DVD,

d) kopie awaryjne może tworzyć jedynie administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,

e) w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,

f) dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,

g) administrator wykonuje backup lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności.

Praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:

a) przeprowadzić składowanie informacji regularnie,

b) używać różnych typów nośników danych,

c) kopie umieszczać w różnych, oddalonych od siebie miejscach,

d) najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,

e) przed składowaniem danych sprawdzić je programem antywirusowym,

f) dokładnie opisywać składowane dane,

g) trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,

h) sprawdzić, czy składowanie przebiegło prawidłowo,

i) upewnić się, Że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były poprawne,

j) regularnie konserwować urządzenia do składowania.

5. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania

a) za ochronę antywirusową odpowiedzialny jest administrator bezpieczeństwa informacji,

b) do ochrony antywirusowej należy stosować zintegrowany program z konsolą administratora, z której istnieje możliwość kontrolowania wykrywania wirusów przez programy kliencie zainstalowane na każdej stacji roboczej,

c) sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w tygodniu,

d) zalecane jest wykorzystanie programów pracujących w tle,

e) przy kontroli szczególną uwagę należy zwrócić na makra,

f) każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym,

g) korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody administratora bezpieczeństwa informacji,

h) w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w urzędzie.

6. **Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków**

a) nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,

b) za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik komórki organizacyjnej, za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest administrator bezpieczeństwa informacji,

c) zbędne dokumenty konwencjonalne powinny być zniszczone w niszczarce dokumentów lub podarte na drobne fragmenty,

d) kopie bezpieczeństwa na taśmach magnetycznych oraz płytach CD i DVD powinny być przechowywane w zamkniętej metalowej szafie,

e) kopie na taśmach magnetycznych oraz płytach CD i DVD nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,

f) kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu - co najmniej jednorazowo po przegraniu danych,

g) wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane,

h) osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, w szczególności komputera nie należy pozostawiać

w samochodzie,

i) kopie przechowuje się co najmniej:
   - dzienne przez czternaście dni,
   - tygodniowe przez 4 tygodnie,
   - miesięczne przez 6 miesięcy,

7. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych

a) przeglądu i konserwacji dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku,

b) zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia -min. czas podtrzymania pracy wynosi 5 min,

c) w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez administratora danych, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,

d) o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić administratora bezpieczeństwa informacji,

e) do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników),

f) zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

8. Sposób postępowania w zakresie komunikacji w sieci komputerowej

System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem (załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 poz. 1024).

a) przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione",
b) administrator bezpieczeństwa informacji z administratorem danych określi zasoby dostępne dla każdego użytkownika,
c) użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania np. za pomocą login scriptu,
d) dostęp do serwerowni ma tylko AB I i pracownicy przez niego upoważnieni,
e) dostęp do konsoli serwera winien być zabezpieczony hasłem,
f) administrator bezpieczeństwa informacji winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików .log,
g) w pomieszczeniu, gdzie ustawiony jest serwer powinien pracować tylko administrator bezpieczeństwa informacji, lub osoby przez niego upoważnione,
h) nie wolno instalować w sieci własnego oprogramowania bez zgody administratora bezpieczeństwa informacji,
i) „zwykli" użytkownicy nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i wolumenów z poziomu systemu operacyjnego,
j) dostęp do archiwalnych plików pocztowych należy zabezpieczyć hasłem,
k) wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do kancelarii,
l) w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,
m) uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą administratora bezpieczeństwa informacji,
n) komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

Załącznik Nr 7

INSTRUKCJA

postępowania w sytuacji naruszenia ochrony danych osobowych

1. Postanowienia ogólne

a) instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzanych, zarówno w zbiorach informatycznych, jak i w zbiorach manualnych. Instrukcję stosuje się także w przypadku gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

b) przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych, przetwarzanie danych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie) oraz usuwanie (zmiana lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą),

c) osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:
   - pracownicy upoważnieni do przetwarzania danych osobowych,
   - kierownicy komórek organizacyjnych,
   - administrator bezpieczeństwa informacji - w przypadku naruszenia systemów informatycznych.

2. Tryb postępowania w sytuacji naruszenia ochrony danych osobowych

a) każdy pracownik, który podejmie wiadomość lub stwierdzi naruszenie ochrony danych osobowych zobowiązany jest do natychmiastowego poinformowania o tym bezpośredniego przełożonego, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych administratora bezpieczeństwa informacji (stosowny zapis w dzienniku ABI),

b) gdy stan urządzeń, zawartość zbioru danych osobowych ujawnione metody pracy, sposób działania programu, lub jakość komunikacji w sieci teleinformatycznej mogą wskazać na naruszenie zabezpieczenie tych baz, to fakt ten należy zgłosić administratorowi bezpieczeństwa informacji (stosowny zapis w dzienniku ABI),

c) administrator bezpieczeństwa informacji razem z kierownikiem komórki organizacyjnej doraźnie usuwają przyczynę naruszenia systemu informatycznego, sprawdzają cały system i dokonuje wpisu do dziennika

ABI,

d) w przypadku naruszenia bezpieczeństwa danych osobowych w zbiorach naturalnych kierownik komórki organizacyjnej sporządza protokół, który powinien zawierać:
   - kto zgłosił, kiedy(data), o której godzinie,
   - na czym polega naruszenie ochrony danych osobowych,
   - zabezpieczone dowody naruszenia danych,
   - propozycje wniosków co do dalszego trybu postępowania, w tym dotyczących zmiany systemu ochrony danych.

e) protokół przedstawia się niezwłocznie Dyrektorowi jednostki,

f) dyrektor jednostki wdraża postępowanie wyjaśniające. Jeżeli stwierdzone zostanie naruszenie ochrony danych osobowych z winy pracownika wszczyna się postępowanie dyscyplinarne (wg odrębnych przepisów). Jeżeli naruszenie ochrony danych wyczerpuje znamiona przestępstwa określone w art. 49 - 52 i 54 ustawy sporządza się doniesienie (wniosek) do odpowiednich organów ścigania,

g) administrator bezpieczeństwa informacji przeprowadza niezwłocznie analizę systemu i wprowadza dodatkowe zabezpieczenia w celu zmniejszenia zagrożenia, i podatności systemu komputerowego na naruszenie bezpieczeństwa informacji.

3. Postanowienia końcowe

Pracownicy Urzędu, po zapoznaniu się z przepisami prawa dotyczącymi ochrony danych osobowych, składają pisemne oświadczenie, które przechowywane jest w aktach osobowych każdego pracownika (wzór oświadczenia jest załącznikiem do instrukcji).

(WZÓR)

Oświadczenie pracownika

.....

(imię i nazwisko)

.....

(Dział)

.....

(stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałem (łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz Rozporządzeniem Ministra Spraw Wewnętrznych I Administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemu informatyczne, służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024 z późn. zm.) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną instrukcją określającą sposób zarządzania systemem informatycznym i ręcznym, służącym przetwarzaniu danych osobowych i instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w placówce:

Powiatowy Urząd Pracy w Cieszynie

ul. Kochanowskiego 8

43-400 Cieszyn

Otrzymałem (łam) dnia:

.....

(podpis pracownika)

....., dnia .....

(WZÓR)

..... , dnia .....

.....

(pieczątka)

UPOWAŻNIENIE nr .....

z dnia .....

Na podstawie art.37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity *Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.)* upoważniam Panią/a ..... zatrudnioną/ego w Powiatowym Urzędzie Pracy, ul. Kochanowskiego 8, 43-400 Cieszyn na stanowisku

.....

Do przetwarzania danych osobowych.

Zadania i czynności do wykonania:

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych *(t. j. Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.).*
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym.
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.
4. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.
5. W szczególności przetwarzanie danych osobowych w następujących zbiorach danych *(numer i nazwa)*:..... ....

Data i podpis Administratora Danych Osobowych *Data i podpis pracownika*

Załączniki Nr 8

Wykaz osób upoważnionych do przetwarzania danych osobowych

Nr Upoważnienia	Nazwisko i Imię	Data nadania	Upoważniający	Data odebrania	Odbierający