

Zarządzenie nr 41/2014
z dnia 31 grudnia 2014
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie w Opolu
w sprawie wprowadzenia do stosowania Instrukcji zarządzania systemem informatycznym
w Miejskim Ośrodku Pomocy Rodzinie w Opolu

Na podstawie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 z późn. zm) oraz § 3 pkt. 3 obowiązującego Regulaminu Organizacyjnego Miejskiego Ośrodka Pomocy Rodzinie w Opolu, zarządzam co następuje:

§ 1

W celu określenia sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Rodzinie w Opolu, wprowadzam do stosowania Instrukcję zarządzania systemem informatycznym w Miejskim Ośrodku Pomocy Rodzinie w Opolu, stanowiącą załącznik do niniejszego zarządzenia.

§2

Wykonanie zarządzenia powierza się wszystkim pracownikom korzystającym z zasobów sieciowych Ośrodka przy realizacji powierzonych zadań służbowych.

§3

Zarządzenie wchodzi w życie z dniem 1 stycznia 2015r.

§4

Z dniem wejścia w życie niniejszego zarządzenia traci moc Zarządzenie nr 45/2012 Dyrektora Miejskiego ośrodka Pomocy Rodzinie w Opolu z dnia 11 lipca 2012r. w sprawie wprowadzenia do stosowania Instrukcji zarządzania systemem informatycznym w Miejskim Ośrodku Pomocy Rodzinie w Opolu.

Dyrektor Miejskiego Ośrodka Pomocy Rodzinie w Opolu
Zdzisław Markiewicz

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

**w Miejskim Ośrodku Pomocy Rodzinie
w Opolu**

§ 1

Instrukcja została opracowana w oparciu o Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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.04.100.1024) i ma na celu określenie sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Rodzinie, zwanym dalej MOPR.

§ 2

1. Administratorem danych jest dyrektor Miejskiego Ośrodka Pomocy Rodzinie – Zdzisław Markiewicz.
2. Administratorem bezpieczeństwa danych w Miejski Ośrodku Pomocy Rodzinie jest Sylwester Klimowicz.
3. Osobą upoważnioną do rejestracji i uaktualnień w GIODO jest Sylwester Klimowicz.

§ 3

Informacje ogólne

W MOPR w Opolu podstawową systemową platformą sieciową jest oprogramowanie Windows w wersji 2008 . Za prawidłowe funkcjonowanie systemu Windows 2008 , jego zabezpieczenie, nadzór i odpowiedzialność ponosi informatyk.

Instrukcja przeznaczona jest dla użytkowników, pracowników, którzy korzystają z zasobów sieciowych realizując obowiązki służbowe.

§ 4

- I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności**

Przydział haseł i identyfikatorów dla użytkowników.

Systemy, w których przetwarza się dane osobowe w zbiorach Miejskiego Ośrodka Pomocy Rodzinie w Opolu wyposażone w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do nich osób.

1. Hasła dostępu opracowuje się indywidualnie dla każdego uprawnionego użytkownika systemu i natychmiast zmienia w wypadku podejrzenia lub stwierdzenia ujawnienia ich osobom trzecim.
2. Każdy użytkownik sam ustala dla siebie hasła dostępu do poszczególnych systemów informatycznych. Wykaz haseł deponuje się w zamkniętej kopercie w sejfie.
3. Hasła dostępu zapisywane są na ekranie monitora w formie niejawnej i mogą być znane tylko użytkownikowi.
4. Osobą odpowiedzialną za techniczny sposób ustalania, przechowywania i wprowadzania haseł jest administrator lub osoba zastępująca administratora.
5. Identyfikatory dla użytkowników przydziela administrator. Po usunięciu danej osoby z systemu, identyfikator nie może być przydzielony innemu użytkownikowi.
6. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora lub hasła, którymi posługuje.
7. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Rejestrowanie i wyrejestrowywanie użytkowników.

1. Rejestracji i wyrejestrowania użytkowników z systemu dokonuje administrator na podstawie informacji uzyskanej od przełożonego użytkownika, wprowadzając dane do ewidencji.
2. Ewidencja zawiera:
 - imię i nazwisko użytkownika;
 - numer identyfikatora;
 - datę zarejestrowania w systemie;
 - datę wyrejestrowania z systemu.
3. Każda zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.
4. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez administratora o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.
5. Użytkownika wyrejestrowuje się z systemu po utracie uprawnień dostępu do przetwarzania danych, co może mieć miejsce w sytuacjach:

- a) ustania zatrudnienia użytkownika u Administratora;
- b) zmiany zakresu obowiązków użytkownika.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
 - a) sprawdzić stan sprzętu informatycznego;
 - b) po włączeniu komputera ocenić jakość jego pracy i stwierdzić zmiany.
2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem:
 - a) maksymalna ilość prób wprowadzenia hasła do systemu wynosi 3;
 - b) po przekroczeniu liczby prób logowania system blokuje dostęp do zbioru danych na poziomie użytkownika. Użytkownik powinien poinformować o tym zdarzeniu administratora, który podejmuje stosowne czynności;
 - c) po zalogowaniu się należy ocenić pracę systemu i stan zbioru danych.
3. Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
 - a) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych;
 - b) użytkownik, który chce się oddalić od stanowiska komputerowego jest zobowiązany do zabezpieczenia systemu poprzez zapisanie danych oraz wyjście z programu komputerowego.
4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
 - a) wylogować się z systemu i poczekać na jego wyłączenie się;
 - b) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji;
5. W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia zabezpieczenia, zmian w systemie bezpieczeństwa lub zauważenia, że stan urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych należy to zgłosić Administratorowi.
6. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w pkt. 1 i przypadku ich zaistnienia natychmiast informować Administratora i przełożonego.
7. Po godzinach pracy stosowana jest ochrona pomieszczeń, w których przetwarzane są dane osobowe, w postaci systemu alarmowego pomieszczeń monitorowanych całodobowo.

IV. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Tworzenie Kopii bazy danych wraz z programami z następujących systemów informatycznych :

1. Program "Pomost Std" firmy "Sygnity"
2. Program "Kadry-Płace" firmy "TETA"
3. Program "Finanse", "Stołówka", "Kasa", "Wyposażenie" firmy "Progman"

Dotyczy kopii danych z programów :

1. Program POMOST Std (całość)

Kopia sporządzana jest przez informatyka

2. Program "Kadry-Płace" firmy "TETA" Wrocław (całość)

- Kadry
- Płace
- Archiwum

Kopia sporządzana jest przez informatyka

3. Program "Finanse", "Stołówka", "Kasa", "Wyposażenie" firmy "Progman"

Kopia sporządzana jest przez informatyka

Kopię zapasową tworzy się na koniec każdego dnia roboczego o godz.20⁰⁰ na serwerze za pomocą streamera i zapisuje się na kasetę z widoczną datą sporządzenia. Kopia zawiera dane z podanych wyżej systemów informatycznych. Oprócz tego na koniec każdego miesiąca oraz na koniec roku nagrywa się kopię zapasową na nośniku laserowym DVD .

V. Sposób , miejsce i okres przechowywania kopii zapasowych oraz elektronicznych nośników informacji

Sposób przechowywania kopii elektronicznych nośników informacji zawierających dane osobowe –w postaci kasyty nagranej na streamerze oraz nośników DVD

Miejsce przechowywania kopii zapasowych oraz elektronicznych nośników informacji - szafa pancerna znajdująca się w pomieszczeniu serwerowni za pokójem informatyka) .Pokój serwerowni jest wyposażony w alarm oraz jest objęty monitoringiem .

Okres przechowywania kopii

Kopie zapasowych zbiorów danych, programów i narzędzi programowych służących do ich przetwarzania oraz elektronicznych nośników informacji zawierających dane osobowe zapisywane są na streamerze (codziennie) , na nośniku laserowym DVD na koniec każdego m-ca oraz dodatkowo na nośniku laserowym DVD i kasecie , nagrywanej za pomocą streamera na koniec każdego roku .

Elektroniczne nośniki informacji zawierające dane osobowe i kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania przechowuje się stosownie do ważności danych:

1. Roczne dane - 5 lat
2. Miesięczne dane - 1 rok
3. Dienne dane - 5 dni

VI. Sposób zabezpieczenia systemu informatycznego przed uzyskaniem nieuprawnionego dostępu do systemu informatycznego

Zabezpieczenie przed naruszeniem obszaru przetwarzania danych osobowych

1. Dane osobowe przetwarza się w budynkach, pomieszczeniach lub częściach pomieszczeń, tworzących obszar przetwarzania danych osobowych.
2. Budynki lub pomieszczenia, w których przetwarza się dane osobowe, są zamykane na czas nieobecności użytkowników, w sposób uniemożliwiający do nich dostęp osób trzecich.
3. Otwarcia pomieszczeń oraz zamknięcia dokonuje pracownik ochrony, który uruchamia system monitoringu Ośrodka.

Kontrola przestrzegania zasad zabezpieczenia systemu ochrony danych osobowych

1. Dzienną kontrolę w zakresie ochrony danych osobowych sprawuje użytkownik.
2. Nadzór nad przestrzeganiem zasad ochrony danych osobowych w komórce organizacyjnej sprawuje przełożony.
3. Administrator sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, przetwarzanych w systemach informatycznych.
4. Administrator dokonuje stałych kontroli i oceny funkcjonowania mechanizmów technicznych zabezpieczeń systemów, w których przetwarzane są dane osobowe.
5. Czynności o których mowa w ustępie 3, Administrator może zlecić osobie wyznaczonej przez przełożonego użytkownika.

Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz Administratora lub osobę upoważnioną przez Administratora.

1. Użytkownik do momentu przybycia administratora lub osoby przez niego upoważnionej powinien:
 - a) zabezpieczyć dostęp do pomieszczenia lub urządzenia;
 - b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;
 - c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony.
2. Administrator po otrzymaniu informacji o naruszeniu lub próbie naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.
3. Po przybyciu na miejsce, Administrator realizuje czynności w kolejności:
 - a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;
 - b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;

- c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;
- d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;
- e) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, Administrator powiadamia o zdarzeniu Dyrektora MOPR.

Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, wyraża administrator lub osoba przez niego upoważniona.

W przypadku stwierdzenia:

- a) błędu użytkownika systemu – Administrator przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej;
- b) uaktywnienia wirusa – należy ustalić źródło jego pochodzenia oraz uaktualnić zabezpieczenia antywirusowe;
- c) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;
- d) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę;
- e) złego stanu urządzenia lub złego działania programu – należy niezwłocznie przeprowadzić kontrolę czynności serwisowo-programowych.

Ochrona systemu informatycznego przed wirusami komputerowymi.

1. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
2. Obowiązkiem Administratora jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.
3. O każdorazowym nieprawidłowym działaniu systemu użytkownik zobowiązany jest niezwłocznie powiadomić Administratora, który sprawdza system programem antywirusowym i przywraca go do pełnej funkcjonalności.
4. Administrator po przeprowadzeniu analizy zasad działania wirusa, zobowiązany jest do usunięcia wirusa.

VII. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Okresowe przeglądy i konserwację sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Miejskiego Ośrodka Pomocy Rodzinie w Opolu wykonuje administrator w porozumieniu z serwisem firm komputerowych.
2. Bieżącą konserwację i naprawę sprzętu wykonuje informatyk.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy w autoryzowanych firmach zewnętrznych, pozbawia się przed naprawą zapisanych danych osobowych, albo naprawia się je pod nadzorem Administratora.
4. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić danych, a w przypadku gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

5. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych .

§ 5

Polityka bezpieczeństwa

I. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe:

1. MOPR Opole ul. Armii Krajowej 36 budynek A administracji MOPR
 - pomieszczenia biurowe nr 1-16 – parter
 - nr 17-30,30A – I piętro
 - Rejon Opiekuńczy Nr 1, 3
2. Budynek administracji MOPR ul. Małopolska 20A :
 - a) Ośrodek Interwencji Kryzysowej
 - wszystkie pomieszczenia biurowe - parter
 - b) Ośrodek Readaptacji Społecznej "Szansa"
 - wszystkie pomieszczenia biurowe - parter
 - c) Klub Integracji Społecznej
 - wszystkie pomieszczenia biurowe - parter
 - d) Specjalistyczny Ośrodek Wsparcia dla Osób Przemocy w Rodzinie
 - wszystkie pomieszczenia biurowe - parter
 - e) Zespół ds. programów i analiz
 - wszystkie pomieszczenia biurowe - parter
3. MOPR Opole ul. Armii Krajowej 36 budynek B administracji MOPR - Dział Opieki nad Rodziną i Dzieckiem
 - wszystkie pomieszczenia biurowe - parter
4. Budynek administracji MOPR Rejon opiekuńczy Nr 2 ,ul. Wrocławska 44
 - Rejon Opiekuńczy Nr 2
 - wszystkie pomieszczenia biurowe – parter
5. Budynek administracji MOPR ul. Barlickiego 1-3
 - wszystkie pomieszczenia biurowe - parter
6. Budynek administracji MOPR ul. Gorzolki 4
 - Rejon Opiekuńczy Nr 4,
 - wszystkie pomieszczenia biurowe - parter

7. Budynek administracji MOPR ul. Hubala 4, Piotrkowska 2

- Rejon opiekuńczy Nr 5
- wszystkie pomieszczenia biurowe - parter, I piętro

II. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Nazwisko
2. Imię
3. Płeć
4. Data urodzenia
5. PESEL
6. NIP
7. Nr Dowodu Osobistego
8. Adres zamieszkania
9. Adres zameldowania
10. Nazwisko małżonka
11. Imię małżonka
12. Nazwisko członków rodziny
13. Imiona członków rodziny
14. Data urodzenia członków rodziny
15. Adres zamieszkania członków rodziny
16. Adresy oraz nazwy firm, w których zatrudniona osoba
17. Adresy firm, w których zatrudniony członek rodziny
18. Adresy szkół, do których uczestniczą dzieci podopiecznych
19. Konta osobiste pracowników MOPR oraz podopiecznych Ośrodka

Systemy informatyczne stosowane w MOPR Opole (programy aplikacyjne), które korzystają z w/w zbiorów danych osobowych

- a) System informatyczny „**POMOST Std**” firmy "Sygnity" Kraków (serwer MOPR Armii Krajowej 36 pok.17A oraz pomieszczenia biurowe parter w budynku A i B)
 - moduł obsługa klienta
 - moduł sprawozdania
 - moduł rodziny zastępcze
 - moduł umieszczanie w DPS
 - moduł piecza zastępcza
- b) System informatyczny "**Kadry-Place**" firmy "TETA" Wrocław (serwer MOPR Armii Krajowej 36 pok.17A, pok.20, pok. 24)
 - moduł Kadry
 - moduł Place
 - moduł Fundusz Bezosobowy
 - moduł Komunikacja z bankami
 - moduł archiwum

- c) System informatyczny **"Płatnik"** firmy "PROKOM" Warszawa (MOPR Armii Krajowej 36 : Kadry - pok. 20, Płace- pok. 24, Sekcja Świadczeń - pok.7)
 - moduł obsługi druków zgłoszeniowych oraz innych w Dziale Kadr
 - moduł obsługi druków rozliczeniowych oraz innych w Dziale Płac
 - moduł obsługi druków zgłoszeniowych, rozliczeniowych oraz innych dla podopiecznych ośrodka
 - moduł elektronicznej transmisji danych do ZUS
- d) Program **"Millenet"** w Banku Millennium (MOPR Armii Krajowej 36 pok. 28, pok.29,30A -I piętro)
w/w program stosuje się do teletransmisji z bankiem Millennium.
- e) Program **"Finanse"** autor firma „Progman”
(MOPR Armii Krajowej 36 serwer pok. 17A,24,28,29,30,30A - I piętro)
- f) Program **"Wyposażenie"** autor firma „Progman” (MOPR Armii Krajowej 36 serwer pok. 17A, pok. 29 - I piętro)
- g) Program **"Kasa"** autor firma „Progman” (MOPR Armii Krajowej 36 serwer pok. 17A, pok.11 - parter)
- h) Program **"Stolówka"** autor firma „Progman” (MOPR Armii Krajowej 36 serwer pok. 17A, ul. Barlickiego 1-3 pok.5 parter, ul.Hubala 4 pomieszczenie biurowe - parter)
- i) Program **"PFRON"**(MOPR Armii Krajowej 36 pok. 20 -Dział Kadr - I piętro)
- j) Obsługa **Portalu sprawozdawczego** na stronie **www.stat.gov.pl** w **zakresie** wykonania sprawozdań GUS Z03,Z05 oraz innych sprawozdań dla potrzeb Działu Kadr i Płac (MOPR Armii Krajowej 36 pok. 20 - Dział Kadr - I piętro)

III. Sposób przepływu danych pomiędzy systemami informatycznymi.

1. System Kadry-Płace dotyczy to danych wprowadzonych w systemie Kadry, automatycznie przenoszonych są do systemu Płace.

Pola: Identyfikator pracownika Imię, Nazwisko, Kod pocztowy, Miejscowość, Ulica, Nr domu /mieszkania, pesel, NIP, konto bankowe, nazwa banku, informacje o nieobecnościach w pracy, dział, wydział, oddział, komórka , stanowisko, ilość dzieci, kalendarze pracy, identyfikator kodu tytułu ubezpieczenia, data powstania obowiązku ubezpieczenia, data wyrejestrowania z ubezpieczenia, kod tytułu ubezpieczenia (dla wyrejestrowania)

2.System Kadry- Program Płatnik - dotyczy to danych wprowadzonych w systemie Kadry, które automatycznie przenoszone są do systemu Płace, a następnie przenoszone są do systemu Płatnik.

Pola: Identyfikator pracownika Imię, Nazwisko, Kod pocztowy, Miejscowość, Ulica, Nr domu /mieszkania, pesel, identyfikator kodu tytułu ubezpieczenia, data powstania obowiązku ubezpieczenia, data wyrejestrowania z ubezpieczenia, kod tytułu ubezpieczenia (dla wyrejestrowania)

3.System Płace- Program Płatnik - dotyczy to danych wprowadzonych w systemie Płace a następnie przenoszone są do systemu Płatnik.

Pola: Identyfikator pracownika w postaci Imię, Nazwisko, składki ubezpieczeniowe, kod tytułu ubezpieczenia, data powstania obowiązku ubezpieczenia

4.System POMOST Std – Program Millenet - dotyczy to danych z systemu "POMOST Std" firmy "Sygnity" przenoszonych do systemu Millenet za pomocą importu oraz przekazywanych do banku transmisją elektroniczną .

Pola: Identyfikator podopiecznego lub instytucji - Imię, nazwisko, bank, Nr konta, kwota wypłaty

5.System Kadry Płace – Program Millenet dane dotyczące systemu "Kadry-Płace" firmy „Teta” przenoszone do systemu Millenet za pomocą importu oraz przekazywanych do banku transmisją elektroniczną

Pola: Imię, nazwisko, nazwa banku, numer konta osobistego, kwota wypłaty.

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

1.do technicznych środków należą:

- a) stosowanie programu antywirusowego w celu wykrycia wirusów komputerowych,
- b) selekcja połączeń z siecią zewnętrzną (firewall),
- c) uwierzytelnienie użytkowników do systemów informatycznych za pomocą haseł o złożonej postaci (odpornych na atak słownikowy), w celu weryfikacji deklarowanej tożsamości osoby.

2. do organizacyjnych zabezpieczeń należą:

- a) zabezpieczenie pomieszczeń gdzie odbywa się przetwarzanie danych, przechowywane dokumenty zawierające dane osobowe, nośniki danych, komputery oraz serwery przed dostępem do nich osób nieupoważnionych,
- b) monitoring obiektu Miejskiego Ośrodka Pomocy Rodzinie w Opolu,
- c) przechowywanie programów informatycznych, kopii zapasowych baz danych w szafie pancerniej w pokoju z alarmem,
- d) stosowanie wygaszaczy ekranu, zabezpieczanych hasłem.

*Dyrektor Miejskiego Ośrodka Pomocy Rodzinie w Opolu
Zdzisław Markiewicz*

