Uchwała Nr 36/X /2011

Zarządu Międzygminnego Związku Komunikacyjnego w Jastrzębiu Zdroju
z dnia 5 października 2011 roku

w sprawie: przyjęcia instrukcji „Polityka Bezpieczeństwa Danych Osobowych" oraz ustalenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze zbiorów Międzygminnego Związku Komunikacyjnego z siedzibą w Jastrzębiu-Zdroju

Na podstawie art. 36-39 Ustawy o ochronie danych osobowych z dn. 29 sierpnia 1997 r. (Dz.U. Nr 133 poz. 883 z późniejszymi zmianami) oraz § 18 ust.1 i 6 Statutu Związku.

Zarząd Związku

u c h w a l a :

§ 1

1. Przyjąć instrukcję „Polityka Bezpieczeństwa Danych Osobowych w Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu Zdroju" stanowiący załącznik nr 1 do niniejszej uchwały.
2. Przyjąć „Instrukcję Zarządzania Systemem Informatycznym" stanowiący załącznik nr 2 do niniejszej uchwały.
3. Powierzyć prawa i obowiązki Administratora Danych Osobowych Dyrektorowi Biura Związku.

§ 2

Nadzór nad wykonaniem uchwały powierza się Przewodniczącemu Zarządu.

. § 3

Traci moc uchwała 297/V/2001 z dnia 21 maja 2001r.

§ 4

Uchwała wchodzi w życie z dniem podjęcia.

PRZEWODNICZĄCY
ZARZĄDU MZK
Krzysztof Baradziej

Załącznik nr 1
do Uchwały Zarządu MZK
nr 36/X/2011 z dnia 05.10.2011r.

Polityka Bezpieczeństwa Danych Osobowych w Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzęniu-Zdroju

1. Wstęp

W systemie MZK przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.). Osobą odpowiedzialną za właściwy i niezakłócony przebieg przetwarzania danych w tym systemie jest Administrator Bezpieczeństwa Informacji.

2. Definicje

a. **MZK** – w tym dokumencie jest rozumiany, jako Międzygminny Związek Komunikacyjny z siedzibą w Jastrzębiu-Zdroju, ul. Przemysłowa 1.
b. **Administrator Bezpieczeństwa Informacji (ABI)** – firma lub osoba upoważniona przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych zgodnie z **załącznikiem nr 1** do Polityki Bezpieczeństwa.
c. **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie zgodnie z **załącznikiem nr 2, 3 i 4** do Polityki Bezpieczeństwa.
d. **Identyfikator użytkownika** – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
e. **Administrator systemu informatycznego**– pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie.

3. Obowiązki Administratora Bezpieczeństwa Informacji

Zgodnie z Instrukcją Zarządzania Systemem Informatycznym

4. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych w systemie stanowią pomieszczenia

Lp.	Adres – budynek	Nr pomieszczenia
1	44-335 Jastrzębie-Zdrój ul. Przemysłowa 1	35,36,37.38

Kopie zapasowe zawierające zbiory danych osobowych przechowywane są w archiwum w budynku przy ul. Przemysłowej w Jastrzębiu-Zdroju.

5. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym MZK

W systemie zbierane są dane zawierające informacje o osobach będących dłużnikami MZK, które przetwarzane są zgodnie z prawem. Dane tworzą „Bazę danych dłużników"

W skład systemu wchodzą:

1. Dokumentacja papierowa (korespondencja obywateli, firm, protokoły-wezwania)
2. Urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.
3. Wydruki komputerowe.
4. Do przetwarzania danych osobowych w systemie informatycznym MZK stosuje się aplikacje: WINDYKATOR, PŁATNIK, RATUSZ firmy REKORD,

6. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i wyćwiczalności danych przetwarzanych w systemie

a. Środki ochrony fizycznej

Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym.
Zastosowano szafy stalowe zamykane na zamki patentowe do przechowywania nośników z kopiami zapasowymi zawierających dane osobowe oraz do przechowywania dokumentacji papierowej.

b. Środki sprzętowe, informatyczne i telekomunikacyjne

Stosuje się niszczarki dokumentów.
Urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania.
Serwer oraz stacje robocze zabezpieczone są programem antywirusowym NOD32 firmy ESET.
Kopie zapasowe wykonywane są raz dziennie na nośnikach DVD.

c. Środki ochrony w ramach oprogramowania systemu:

Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników.
System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika.
Zastosowano działający w tle program antywirusowy na komputerach użytkowników.
W systemie sieciowym stosuje się mechanizm wymuszający okresową zmianę haseł dostępu.

d. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator.
Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

e. Środki ochrony w ramach systemu użytkowego.

Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.

Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika.

f. Środki organizacyjne.

Wyznaczono **Administratora Bezpieczeństwa Informacji**.

Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone.

Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych (**załącznik nr 2** do Polityki Bezpieczeństwa).

Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy. Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym. Oświadczenie– zobowiązanie pracownika stanowi załącznik nr 4 do Polityki Bezpieczeństwa.

Personel pomocniczy może przebywać w pomieszczeniach gdzie przetwarzane są dane osobowe tylko w towarzystwie osób upoważnionych do przetwarzania danych osobowych, chyba że ABI wystawi indywidualne upoważnienie do przebywania w takim pomieszczeniu bez asysty (wzór upoważnienia stanowi **załącznik nr 3** do Polityki Bezpieczeństwa).

Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

7. Postanowienia końcowe.

a. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

b. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych (**załącznik nr 5** do Polityki Bezpieczeństwa).

c. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926).

8. Struktura baz danych osobowych

a Baza danych dłużników MZK
nazwisko, imię (może być drugie imię), imię ojca i matki
data i miejsce urodzenia (rok, miesiąc, dzień)
PESEL
seria i numer dowodu osobistego lub innego dokumentu
miejsce aktualnego pobytu (stałego lub czasowego ponad 2 miesiące) – miasto, ulica, numer domu i mieszkania
data, godzina i miejsce wystawienia protokołu-wezwania
sygnatura postępowania sądowego

sygnatura postępowania odwoławczego
miejsce pracy
uwagi

b. Rejestr skarg i wniosków.
data wpływu
imię i nazwisko petenta, nazwa instytucji, redakcji
adres petenta instytucji
przedmiot skargi, zażalenia i odwołania
data zlecenia załatwienia
komu zlecono załatwienie
data wysłania do załatwienia
sposób załatwienia
data wysłania zawiadomienia
kogo zawiadomiono
uwagi

c. Kadry
PESEL
imię i nazwisko
nazwisko rodowe
data i miejsce urodzenia
płeć
adres stały(miejscowość, ulica, nr domu, nr mieszkania)
dowód osobisty(seria, nr i rodzaj, wydany przez, data wydania)
imię ojca, imię matki
stan cywilny
obowiązek wojskowy(dokument wojskowy, seria i numer, stopień wojskowy, specjalność, ewidencja, przydział mobilizacyjny)
nr legitymacji służbowej
posiada gospodarstwo rolne
emeryt/rencista
obywatelstwo obce
telefon, osoba kontaktowa
wykształcenie, nazwa szkoły i rok
staż pracy
tytuł zawodowy
zawód wyuczony zasadniczy
zawód wykonywany
ukończone kursy
uzyskane kwalifikacje
warunki zatrudnienia
nieobecności w pracy
historia pracy, kary, nagrody

d. Płace
imię i nazwisko
dane płacowe
numer konta
ubezpieczenia ZUS

PRZEWODNICZĄCY
ZARZĄDU MZK
Krzysztof Baradziej

Załącznik nr 1
do Polityki Bezpieczeństwa
Danych Osobowych w MZK
z siedzibą w Jastrzębiu -Zdroju

U P O W Ż N I E N I E

Zgodnie a art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 Nr 101 poz. 926 z późn. zm.),

Upoważniam Firmę/Panią/Pana.....

do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych oraz do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych w Międzygminnym Związku Komunikacyjnym w Jastrzębiu-Zdroju. Ww. firmę/osobę wyznaczam na **Administratora Bezpieczeństwa Informacji (ABI).**

Przyjmuję do wiadomości i wykonania:

.....

Jastrzębie-Zdrój dnia.....

Załącznik nr 2
do Polityki Bezpieczeństwa
Danych Osobowych w MZK
z siedzibą w Jastrzębiu -Zdroju

U P O W Ż N I E N I E

Zgodnie a art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 Nr 101 poz. 926 z późn. zm.),

Upoważniam Panią/Pana.....

do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych zatrudnionych pracowników, stosując przepisy wykonawcze do Kodeksu Pracy w sprawach wynikających za stosunku pracy oraz przepisy i instrukcje o ochronie danych osobowych i sposobie zarządzania systemem informatycznym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

1. Upoważnienie wydaje się na czas nieokreślony.
2. Upoważnienie wygasa z dniem rozwiązania stosunku pracy lub jego wcześniejszego cofnięcia przez Administratora Danych.

Jastrzębie-Zdrój dnia.....

.....
podpis pracodawcy

Załącznik nr 3
do Polityki Bezpieczeństwa
Danych Osobowych w MZK
z siedzibą w Jastrzębiu –Zdroju

U P O W Ż N I E N I E

Zgodnie a art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 Nr 101 poz. 926 z późn. zm.),

Upoważniam Panią/Pana.....

do przebywania na terenie pomieszczeń biurowych Międzygminnego Związku Komunikacyjnego z siedzibą w Jastrzębiu-Zdroju, w których przetwarzane są dane osobowe podczas nieobecności osób upoważnionych do ich przetwarzania w ramach wykonywanych obowiązków służbowych.

3. Upoważnienie wydaje się na czas nieokreślony.
4. Upoważnienie wygasa z dniem rozwiązania stosunku pracy lub jego wcześniejszego cofnięcia przez Administratora Danych.

Jastrzębie-Zdrój dnia.....

.....
podpis pracodawcy

Załącznik nr 4
do Polityki Bezpieczeństwa
Danych Osobowych w MZK
z siedzibą w Jastrzębiu –Zdroju

OŚWIADCZENIE – ZOBOWIĄZANIE

Oświadcza, że zapoznałem/łam się z:

- ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 Nr 101 poz. 926 z późn. zm.);
- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
- instrukcją określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji;
- instrukcją postępowania w sytuacji naruszenia danych osobowych przeznaczonych dla osób przy przetwarzaniu danych.

Powyższe akty prawne i normatywne przyjmuję do wiadomości i przestrzegania. Jednocześnie zobowiązuję się do ochrony danych osobowych przed niepożądanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem informacji.

.....
(podpis osoby przyjmującej oświadczenie)

.....
(data i podpis pracownika)

Załącznik nr 5
do Polityki Bezpieczeństwa
Danych Osobowych w MZK
z siedzibą w Jastrzębiu –Zdroju

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W MIĘDZYGMINNYM ZWIĄZKU KOMUNIKACYJNYM Z SIEDZIBĄ W JASTRZĘBIU-ZDRUJU

lp	Nazwisko i imię	Stanowisko służbowe	Zakres upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator (jeżeli dane przetwarzane są w systemie informatycz.
1						
2						
3						
4						

Załącznik nr 2
do Uchwały Zarządu MZK
nr 36/X/2011 z dnia 05.10.2011r.

Instrukcja Zarządzania Systemem Informatycznym

1. Zbiory danych osobowych.

   W systemie informatycznym przechowywane są dane osobowe dotyczące osób, które nie posiadały ważnego biletu na korzystanie ze środków komunikacji miejskiej.
   System informatyczny służący do przetwarzania powyższych danych osobowych, zrealizowany jest w lokalnej sieci komputerowej opartej na serwerze i stacjach roboczych, nie posiadających dostępu do globalnej sieci internetowej.
   System ten funkcjonuje w Referacie KNR Międzygminnego Związku Komunikacyjnego w Jastrzębiu Zdroju.

2. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.

   Dla każdego użytkownika systemu informatycznego, przydziela się odrębny identyfikator i hasło oraz uprawnienia w systemie zgodnie z zakresem obowiązków.
   Przyznany użytkownikom identyfikator jest niezmienny, natomiast użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż raz na miesiąc.
   Za przydział i rejestrację identyfikatorów odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
   Administrator Bezpieczeństwa Informacji wyrejestrowuje z systemu sieciowego identyfikator i hasło pracownika, który utracił uprawnienia dostępu do danych osobowych. Identyfikator pracownika oraz hasło dostępu do systemu informatycznego stanowią tajemnicę służbową.
   Użytkownik po otrzymaniu indywidualnego identyfikatora oraz hasła powinien je zapamiętać. Nie wolno ich zapisywać w miejscach, które umożliwiałyby osobom trzecim zapoznanie się z nimi.

3. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

   Identyfikator i hasło przekazywane są użytkownikowi w formie ustnej przez Administratora Bezpieczeństwa Informacji. Hasło to powinno zostać przez użytkownika zmienione bezpośrednio po zalogowaniu się do systemu informatycznego. Hasło musi składać się min. z 8 znaków w tym przynajmniej jednej dużej litery, jednej małej litery, jednej cyfry oraz jednego znaku specjalnego takiego jak: !, @, #, $, %, ^, &, *, ?.
   Zmiana hasła powinna być realizowana przez użytkownika systemu nie rzadziej niż jeden raz na 30 dni.

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

   Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.

Użytkownicy uzyskują bezpośredni dostęp do danych w aplikacji po podaniu identyfikatora i właściwego hasła.

Kończąc pracę użytkownik powinien:

a. wykonać kopię awaryjną (zapasową),
b. zamknąć program oraz wyjść z systemu i wyłączyć komputer wraz z drukarką,
c. sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy są prawidłowo zabezpieczone przed uruchomieniem ich przez osoby postronne.

Wszystkie zauważone usterki i nieprawidłowości na stanowisku użytkownik winien natychmiast zgłosić bezpośredniemu przełożonemu, odpowiednim służbom konserwacyjnym oraz Administratorowi Bezpieczeństwa Informacji.

W przypadku stwierdzenia przez użytkownika danych osobowych naruszenia zabezpieczeń systemu informatycznego, na które mogą wskazywać:

a. stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),
b. różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych opcjach),
c. różnica w zawartości zbioru danych osobowych (np. brak lub nadmiar danych), jest on zobowiązany niezwłocznie powiadomić o tym bezpośrednio przełożonego oraz Administratora Bezpieczeństwa Informacji, a w przypadku ich nieobecności – bezpośrednio Administratora Danych Osobowych.

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:

a. zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
b. na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
c przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
d niezwłocznie podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji,
e przywrócić normalny stan działania systemu.

Po wyeliminowaniu bezpośredniego zagrożenia Administrator Bezpieczeństwa Informacji ma obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności sprawdzić:

a. stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
b. zawartość zbioru danych osobowych,
c. sposób działania programu,
d. obecność wirusów komputerowych.

5. Procedury tworzenia kopii zapasowych zbiorów danych

Dane zgromadzone w pamięciach komputerów powinny być zabezpieczone przed ich utratą przez tworzenie ich kopii awaryjnych w cyklach:

- codziennym
- tygodniowym
- miesięcznym.

Za archiwizację danych przechowywanych w pamięci komputerów lokalnych odpowiedzialni są użytkownicy danych osobowych. Archiwizacji należy dokonywać w każdym dniu, w którym dokonywane były jakiekolwiek zmiany. Dane powinny być kopiowane na wyznaczony dysk sieciowy lub płyty DVD, a następnie przechowywane w pomieszczeniu wskazanym przez Administratora Bezpieczeństwa Informacji.

Za archiwizację danych przechowywanych w pamięci serwerów sieciowych odpowiedzialny jest kierownik działu, w którym dane są przetwarzane. W cyklu codziennym należy archiwizować zmiany, a w cyklu tygodniowym całą zawartość baz danych przechowywanych w pamięci serwerów sieciowych. Kopie wykonane na płytach DVD lub taśmach magnetycznych przechowywać należy w odpowiednio chronionym i zabezpieczonym pomieszczeniu.

Archiwizowanie danych z pamięci serwerów w cyklu miesięcznym dokonywać należy na płytach DVD lub taśmach magnetycznych. Kopie zapasowe danych z serwera należy przechowywać w odpowiednio zabezpieczonym pomieszczeniu poza pomieszczeniem, w którym znajduje się serwer. Za archiwizowanie danych z pamięci serwerów w cyklu miesięcznym odpowiedzialny jest Administrator bezpieczeństwa Informacji.

6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

Nośniki informatyczne, wydruki zawierające dane osobowe oraz kopie awaryjne, przechowywać należy w pomieszczeniu archiwum MZK, w zamkniętych szafach przez okres 30 dni.
Miesięczne kopie zapasowe, winny być przechowywane przynajmniej przez 6 miesięcy.

Za wydruki zawierające dane osobowe odpowiedzialni są użytkownicy danych osobowych, którzy je wykonali. Wydruki te winny być przechowywane zgodnie z terminami określonymi w instrukcji.

Każdy użytkownik ma obowiązek pozbawiania zapisu danych osobowych z nośników, które przeznaczone są do przekazywania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych oraz do pozbawiania zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji.

7. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w paragrafie 5 pkt 6 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2009r.

Serwer oraz stacje robocze zabezpieczone są programem antywirusowym NOD32 firmy ESET.
W celu zmniejszenia zagrożenia zabrania się użytkownikom korzystania z zewnętrznych pamięci USB.

Systemy do przetwarzania danych osobowych są zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskane nieuprawnionego dostępu, przez brak połączenia z siecią publiczną.

Zabrania się:

a. udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
b. wykorzystywania sieci komputerowej w celach w innych niż służbowych,
c. samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),
d. trwałego lub czasowego kopiowania programów komputerowych w całości lub części jakimikolwiek środkami i w jakiejkolwiek formie,
e. publicznego rozpowszechniania programów komputerowych lub ich kopii,
f. przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
g. udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej,
h. wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez wyraźnego upoważnienia Administratora Bezpieczeństwa Informacji,
i. używania prywatnych skrzynek mailowych działających na innych serwerach niż urzędowy,
j. uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści, kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody Administratora Danych Osobowych.

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

Raz na kwartał Administrator Bezpieczeństwa Informacji lub wyznaczona przez niego osoba, dokonuje przeglądu i konserwacji systemu informatycznego i zbioru danych osobowych.
W przypadku konieczności oddania sprzętu zawierającego dane osobowe do naprawy na zewnątrz, Administrator Bezpieczeństwa Informacji zobowiązany jest do usunięcia zapisanych danych w sposób uniemożliwiający ich odzyskanie. W przypadku gdy nie można tych danych usunąć, naprawa sprzętu winna być dokonywana pod nadzorem Administratora Bezpieczeństwa Informacji.

PRZEWODNICZĄCY
ZARZĄDU MZK
Krzysztof Baradziej