INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W MIEJSKIM OŚRODKU SPORTU I REKREACJI W JASTRZĘBIU-ZDROJU

INSTRUKCJA ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

w Miejskim Ośrodku Sportu i Rekreacji w Jastrzębiu-Zdroju

wydana dnia ....20.03.2015.....

przez ..Dyrektora Miejskiego Ośrodka Sportu i Rekreacji

Postanowienia Ogólne

§ 1

Niniejsza instrukcja dotyczy każdego zbioru danych osobowych przetwarzanego w Miejskim Ośrodku Sportu i Rekreacji w Jastrzębiu-Zdroju zarówno w formie elektronicznej jak i papierowej. Aktualny wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, ich lokalizacją i sposobem dostępu.

Użyte w Instrukcji określenia oznaczają:

§ 2

1. **zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
2. **administrator danych osobowych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w § 3, decydujące o celach i środkach przetwarzania danych osobowych.
3. **administrator bezpieczeństwa informacji** - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych
   we wskazanych systemach informatycznych.
4. **administrator systemu informatycznego** - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
5. **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **stacja robocza** - stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
7. **bezpieczeństwo systemu informatycznego** - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
8. **przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych

osobowych takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie

9. **osoba upoważniona** - osoba posiadająca upoważnienie wydane przez ADO (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji).
10. **użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych
w systemie informatycznym,
11. **osoba uprawniona** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
12. **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182; z późniejszymi zmianami) z uwzględnieniem przepisów ustawy z dnia 7.11.2014r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r., poz. 1662), która weszła w życie dnia 1 stycznia 2015 roku nowelizującej przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych.
13. **rozporządzenie** - 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 2004 r. Nr. 100 , poz. 1024)

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 3

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik do Polityki bezpieczeństwa). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego użytkownika lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych. W formie pisemnej składa on wniosek do Administratora danych osobowych odpowiedniego dla zakresu danych o wydanie upoważnienia do przetwarzania danych osobowych. Wniosek ten powinien zawierać:

   a) imię i nazwisko pracownika, któremu upoważnienie zostanie nadane,
   b) nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
   c) zakres upoważnienia do przetwarzania danych osobowych,
   d) datę, z jaką upoważnienie ma być nadane,
   e) okres ważności upoważnienia.

2. Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika oraz przekazana do

wiadomości przełożonego pracownika.

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub osobę przez niego uprawnioną.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego odpowiada administrator danych osobowych lub powołany przez niego Administrator Bezpieczeństwa Informacji.

Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek Administratora Danych Osobowych, lub powołanego przez niego Administratora Bezpieczeństwa Informacji, przełożonego użytkownika lub koordynatora zadania, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych.

3. Administrator danych osobowych jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych . Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych taka ewidencja zawiera :

   A) Imię i nazwisko osoby upoważnionej
   B) Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych ,
   C) Nazwa systemu informatycznego , którego dotyczy upoważnienie,
   D) Identyfikator nadany w systemie informatycznym , w którym przetwarzane są dane osobowe

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

§ 4

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
2. Identyfikator składa się minimalnie z pięciu znaków- znaki identyfikatora nie są rozdzielone spacjami ani znakami interpunkcyjnymi, identyfikator nie zawiera polskich liter.
3. Identyfikator wpisuje się do ewidencji prowadzonej przez administratora danych osobowych wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez administratorów systemów informatycznych do właściwych systemów.

4. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika

z systemu informatycznego nie może być przydzielany innej osobie. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników.

5. Hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe.
6. Hasła są zmieniane przez użytkownika.
7. System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie
   30 dni od dnia ostatniej zmiany hasła.
8. System informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, w szczególności hasło powinno składać się z co najmniej 8 znaków. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 5

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym
   oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.
2. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa i ochrony przetwarzania danych osobowych" w Miejskim Ośrodku Sportu i Rekreacji w Jastrzębiu-Zdroju .
3. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora
   i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
4. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy.
   Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem danych osobowych. Użytkownik informuje administratora danych osobowych o zablokowaniu dostępu do zbioru danych. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

5. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni.

6. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne monitory stanowisk dostępu do danych powinny być ustawione w taki sposób żeby uniemożliwić tym osobom wgląd w dane.
7. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

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

§ 6

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie do tego celu wyznaczona. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegrywanie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. W przypadku, gdy z przyczyn technicznych jest to niemożliwe użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych baz danych na nośniku wymiennym i centralne ich przechowywanie w miejscu wskazanym przez administratora danych osobowych.

2. Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

   a) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie,
   b) kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku lokalnym komputera wybranego przez administratora systemu informatycznego (komputerem tym nie może być serwer baz danych),

   c) raz w tygodniu, na nośniku wymiennym, tworzona jest kopia zawierająca kopie zapasową danych osobowych z każdego dnia ostatniego tygodnia, kopia ta przechowywana jest w zamkniętej szafie w innym pomieszczeniu niż w którym znajdują się serwery danych,

d) zbiorcze (tygodniowe) kopie przechowywane są przez okres dwóch tygodni- po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne,
e) raz w miesiącu, pomiędzy 1 a 5 dniem każdego miesiąca tworzona jest kopia zapasowa danych osobowych, która przekazywana jest do przechowywania przy zachowaniu odpowiednich zabezpieczeń w innym budynku niż ten, w którym znajdują się serwery- przechowywane są tam kopie z 3 ostatnich miesięcy,
f) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz na miesiąc, która przechowywana jest w zamkniętej szafie. Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.

3. W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego. Z przeprowadzonego testu administrator systemu sporządza krótką notatkę uwzględniającą datę testu oraz jego rezultat (kopię notatki przekazuje administratorowi danych osobowych).

4. Nośniki kopii zapasowych, które zostały wycofane z użycia (jeżeli jest to możliwe) należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku nośniki podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

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

§ 7

1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.

2. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu.

§ 8

1. W związku z tym, że system informatyczny narażony jest na działanie oprogramowania,
którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.

   Można wyróżnić następujące rodzaje występujących tu zagrożeń:
   a) nieuprawniony dostęp bezpośrednio do bazy danych,
   b) uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób,
      że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
   c) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
   d) przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
   e) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych. W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia polegające na fizycznym odseparowaniu serwera bazy danych od sieci zewnętrznej:
      - autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
      - stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
      - stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
      - stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
      - stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

2. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów

komputerowych na stacje robocze są :

a) załączniki do poczty elektronicznej,
b) przeglądane strony internetowe,
c) pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

3. W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego przetwarzającego dane osobowe lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
b) antywirusowy skaner ruchu internetowego powinien być stale włączony,
c) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,
d) skaner poczty elektronicznej powinien być stale włączony.

4. Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane
w sposób następujący:

a) zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
b) możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

5. Użytkownicy systemu informatycznego zobowiązani są do następujących działań :

a) skanowanie zawartości dysków stacji roboczej pracującej w systemie informatycznym
pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu,
b) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
c) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować :

1. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

2. odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu czy dane zapisane
na kopiach nie są zainfekowane,
3. samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji
lub po skonsultowaniu się z zewnętrznymi ekspertami.

System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające
na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej.

W związku z tym system informatyczny powinien być wyposażony w co najmniej:

1) filtry zabezpieczające stacje robocze przed skutkami przepięcia,
2) zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamknięcie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

Sposób realizacji wymogów

§ 9

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).
2. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające
na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
b) operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu,
d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe
oraz nieudane próby wykonania operacji na danych osobowych,
e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3. Zapis działania użytkownika uwzględnia:

a) identyfikator użytkownika,
b) datę i czas kiedy zdarzenie miało miejsce,
c) rodzaj zdarzenia, określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów). W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie administratora danych osobowych lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

4. Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych
z uwzględnieniem:

a) identyfikatora osoby, której dane dotyczą,
b) osoby przesyłającej dane,
c) odbiorcy danych,
d) zakresu przekazanych danych osobowych,
e) daty operacji,
f) sposobu przekazania danych.

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

§ 10

1. Wszelkie prace związane z naprawami i konserwacją systemów informatycznych przetwarzających dane osobowe muszą uwzględniać zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe na terenie firmy prowadzone w tym zakresie mogą być wykonywane wyłącznie przez upoważnionych pracowników firmy lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie upoważnionych pracowników firmy.

2. Przed rozpoczęciem prac serwisowych przez osoby postronne konieczne jest potwierdzenie tożsamości serwisantów. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.

DYREKTOR
Miejskiego Ośrodka Sportu
i Rekreacji
mgr Zofia Florek

INSPEKTOR OCHRONY DANYCH
Jarosław Wacławek