Zarządzenie nr 7 /2013
Dyrektora Miejskiego Ośrodka Kultury
z dnia 5 lipca 2013 roku
w sprawie wprowadzenia Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (tekst jedn. Dz. U. z 16 kwietnia 2012 r. poz. 406), ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 101 z 2002 r., poz. 926 z późn. zm.), § 3 i § 4 Rozporządzenia 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 ze zm.) zarządzam, co następuje:

§ 1

Wprowadza się do stosowania z dniem 5 lipca 2013 „Politykę bezpieczeństwa Informacji Miejskiego Ośrodka Kultury w Pelplinie oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

1. Polityka bezpieczeństwa stanowi załącznik nr 1 do niniejszego Zarządzenia.
2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszego Zarządzenia

§ 2

Polityka bezpieczeństwa określa zbiór zasad obowiązujących przy zbieraniu, przetwarzaniu danych osobowych we wszystkich zbiorach administrowanych przez Miejski Ośrodek Kultury w Pelplinie

§ 3

Zarządzenie wchodzi w życie z dniem 5 lipca 2013 roku.

Załączniki:

1. Zał. Nr 1 Polityka bezpieczeństwa informacji Miejskiego Ośrodka Kultury w Pelplinie
2. Zał. Nr 2 Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Załącznik nr 1
do Zarządzenia dyrektora
Miejskiego Ośrodka Kultury w Pelplinie
Nr 7 z dnia 5 lipca 2013

Polityka bezpieczeństwa informacji

Rozdział 1
Postanowienia ogólne

1. *Polityka bezpieczeństwa informacji w Miejskim Ośrodku Kultury w Pelplinie, zwana dalej „Polityką", jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych, w szczególności w wykazach, dziennikach zajęć, listach wycieczek i w innych zbiorach ewidencyjnych.*
2. *Miejski Ośrodek Kultury w Pelplinie zwany dalej „Ośrodkiem" realizując politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:*
   1) *przetwarzane zgodnie z prawem;*
   2) *zbierane dla oznaczonych, zgodnych z planem pracy celów;*
   3) *przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.*

Rozdział 2
Ewidencja zasobów

1. *Wyjaśnienia używanych pojęć:*
   1) *Dane osobowe – wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,*
   2) *Baza danych osobowych – każdy zbiór danych o charakterze osobowym,*
   3) *Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, a zwłaszcza te, które wykonuje się w systemach informatycznych,*
   4) *Administrator bezpieczeństwa informacji – osoba nadzorująca przestrzeganie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych,*
   5) *Bezpieczeństwo systemu informatycznego – wdrożenie przez administratora danych osobowych lub inną osobę przez niego wyznaczoną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed dostępem, modyfikacją, ujawnieniem, pozyskiwaniem lub zniszczeniem,*
   6) *Nośniki danych osobowych – dyski twarde komputerów, płyty CD lub DVD, pamięć flash, itp.,*
   7) *Pracownicy – osoby zatrudnione w Ośrodku na umowę o pracę oraz instruktorzy zajęć.*
2. *Dane osobowe w Ośrodku Kultury przetwarzane są w budynku znajdującym się przy ul. Kościuszki 2A w Pelplinie.*
3. *Polityka zawiera:*
   1) *wykaz zbiorów danych osobowych przetwarzanych w Ośrodku wraz z opisami struktury zbiorów* ***(załącznik nr 1 do Polityki bezpieczeństwa informacji)***

2) *wykaz pomieszczeń, w których przetwarzane są dane osobowe w sposób tradycyjny i z użyciem stacjonarnego sprzętu komputerowego (**załącznik nr 2 do Polityki bezpieczeństwa informacji**)*

Rozdział 3
Opis zagrożeń naruszających ochronę danych osobowych

1. *Rodzaje zagrożeń naruszających ochronę danych osobowych:*
   1) *Zagrożenia losowe:*
      - *zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu prądu) – ich wystąpienie może prowadzić do utraty danych lub ich zniszczenia lub uszkodzenia,*
      - *wewnętrzne (np., awarie sprzętowe) – w wyniku ich wystąpienia może dojść do zniszczenia danych.*
   2) *Zagrożenie zamierzone (świadome i celowe naruszenie poufności danych).*

Rozdział 4
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności przetwarzanych danych osobowych.

1. *Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:*
   1) *wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatnią upoważnioną do przetwarzania danych osobę - także w godzinach pracy,*
   2) *w Ośrodku funkcjonuje system alarmowy, który zostaje włączony przez pracownika, który opuszcza Ośrodek jako ostatni.*
2. *Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:*
   1) *ochrona przed utratą zgromadzonych danych poprzez cykliczne (co pół roku) wykonywanie kopii zapasowych, z których w przypadku awarii, odtwarzane są dane i system operacyjny*
   2) *zastosowanie ochrony przeciwpożarowej poprzez umieszczenie gaśnic*
   3) *organizacyjną ochronę danych osobowych i ich przetwarzania realizuje się poprzez:*
      - *zapoznanie każdego pracownika z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem do pracy przy ich przetwarzaniu*
      - *przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych osobowych oraz form zabezpieczenia pomieszczeń i budynku, sprzętu*
   2) *upoważnienie osób do przetwarzania danych osobowych (**załącznik nr 3 do Polityki bezpieczeństwa informacji**)*
   3) *prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (**załącznik nr 4 do Polityki bezpieczeństwa informacji**)*

Rozdział 5
Postanowienia końcowe

1. *W sprawach nieuregulowanych niniejszym dokumentem maja zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), rozporządzenia 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. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).*
2. *Niniejsza „Polityka bezpieczeństwa" służąca do przetwarzania danych osobowych w Miejskim Ośrodku Kultury w Pelplinie wchodzi w życie z dniem podpisania.*

Załącznik nr 1
do Polityki bezpieczeństwa informacji

Wykaz zbiorów danych osobowych przetwarzanych w Miejskim Ośrodku Kultury w Pelplinie z podaniem formy i programów zastosowanych do przetwarzania danych.

L.p.	*Nazwa zbioru danych osobowych*	*Program/technika przetwarzania danych*	*Uwagi*
1.	*Uczestnicy zajęć artystycznych i wycieczek*	*Pakiet Microsoft Word*	
2.	*Newsletter*		

Załącznik nr 2
do Polityki bezpieczeństwa informacji

Wykaz pomieszczeń, w których przetwarzane są dane osobowe w Miejskim Ośrodku Kultury w Pelplinie

L.p.	*Adres*	*Pomieszczenie/ nazwa*	*Uwagi*
1.	*Pelplin, ul. Kościuszki 2a*	*Wszystkie pomieszczenia wchodzące skład trwałego zarządu Ośrodka Kultury*	

Załącznik nr 3
do Polityki bezpieczeństwa informacji

Nr ewidencyjny: ……..
……..
(miejscowość) (data)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Upoważniam

Panią/Pana……

zatrudnioną/zatrudnionego w …….

……

.

do przetwarzania danych osobowych, oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, rejestry, spisy, dzienniki zajęć, listy, itp.) i elektronicznej.

Do załącznika nr 3
Polityki bezpieczeństwa informacji

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisana (ny) oświadczam, iż:

1. *Zostałam (łem) przeszkolona (ny) w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm. oraz „Polityką bezpieczeństwa informacji w Miejskim Ośrodku Kultury w Pelplinie.*
2. *Znana jest mi odpowiedzialność karna za naruszenie ww. ustawy (art. 49-54)*

……

(data i podpis)

Niniejsze upoważnienie sporządzono w dwóch jednobrzmiących egz.- każdy na prawach oryginału, które otrzymują:
1.osoba upoważniona
2.a/a

Załącznik nr 4
do Polityki bezpieczeństwa informacji

Ewidencja osób upoważnionych do dostępu i przetwarzania danych osobowych

Nr ewidencyjny upoważnienia	***Nazwisko i imię***	***Zatrudnienie stałe (zakład macierzysty)***	***Umowa/ zlecenie***	***Uwagi***
1.2013	***Głazik-Szulc Grażyna***	***MOK Pelplin***	***-***	
2.2013	***Szweda Izabela***	***MOK Pelplin***	***-***	
3.2013	***Pielecka Anna***	***MOK Pelplin***	***-***	
4.2013	***Freda Ewa***	***MOK Pelplin***	***-***	
5.2013	***Sakowski Piotr***	***MOK Pelplin***	***-***	
6.2013	***Świtała Wiesław***	***MOK Pelplin***	***-***	

Załącznik nr 2
do Zarządzenia dyrektora
Miejskiego Ośrodka Kultury w Pelplinie
Nr 7 z dnia 5 lipca 2013

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Rozdział I
Postanowienia ogólne

1. *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania*

administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Miejskim Ośrodku Kultury w Pelplinie zwanym dalej „Ośrodkiem".

2. *Instrukcja została opracowana zgodnie z ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zwana dalej „ustawą o ochronie danych osobowych" oraz rozporządzeniem 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. Nr 100, póz. 1024).*
3. *Dyrektor Ośrodka wykonuje obowiązki administratora danych osobowych i administratora systemów informatycznych, a funkcję administratora bezpieczeństwa informacji sprawują wyznaczeni pracownicy w odniesieniu do prowadzonych w Ośrodku zbiorów danych.*
4. *W systemach informatycznych służących do przetwarzania danych osobowych w Ośrodku stosuje się środki bezpieczeństwa na poziomie podstawowym.*

Rozdział 2
Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. *Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez administratora bezpieczeństwa informacji z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Ośrodku wewnętrznymi regulacjami w tym zakresie.*
2. *Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych.*
3. *Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na przekazaniu dostępu do hasła oraz ustalenia zakresu dostępnych danych.*
4. *Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.*

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

1. *Użytkownik uzyskuje dostęp do danych osobowych wyłącznie po podaniu hasła zaraz po włączeniu komputera.*
2. *Hasło składa się co najmniej z 4 znaków.*
3. *Hasło powinno zawierać małe litery, może też zawierać inne znaki.*
4. *Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy.*
5. *Hasło należy zmieniać co najmniej raz w roku.*

6. *Użytkownik nie może udostępniać osobom nieuprawnionym hasła dostępu oraz osobom nieuprawnionym do swojego stanowiska pracy.*
7. *W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło.*

Rozdział 4
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. *Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego.*
2. *Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane. Kończąc pracę użytkownik obowiązany jest wyłączyć sprzęt komputerowy.*

Rozdział 5
Korzystanie z bankowości internetowej

1. *Do dokonywania operacji związanych z obsługą bankowości internetowej, dostępu do konta Ośrodka i wykonywania jakichkolwiek operacji, upoważnieni są wyłącznie główny księgowy i dyrektor.*
2. *Zabrania się przechowywania haseł dostępu do konta na biurku, w dokumentacji, razem z osobistym kluczem do konta (pen-drivem), zapisywania w notatkach, w pamięci komputera na dyskach. Hasła i login należy zapamiętać.*
3. *Osobisty klucz do konta (pen-drive) każda z osób, główny księgowy i dyrektor, przechowują w sposób należycie zabezpieczony, zapewniający nieużycie przez osoby trzecie. Po wylogowaniu się z banku, w czasie godzin pracy, pen-drive zamykany jest na klucz w kontenerach przy biurkach, a na zakończenie dnia pracy, w szafie pancernej.*
4. *Główny księgowy wprowadza wszelkie dane, które następnie zatwierdzają główny księgowy i dyrektor.*
5. *Zabrania się korzystania z bankowości internetowej na komputerze, na którym stwierdzono źle działającą ochronę, oprogramowanie lub inne problemy.*
6. *W czasie wykonywania operacji bankowych, zabrania się odchodzenia od komputera, przyjmowania rozmów telefonicznych i załatwiania innych spraw.*

Rozdział 6
Tworzenie kopii zapasowych zbiorów danych

1. *Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie raz na pół roku kopii zapasowych.*
2. *Kopie zapasowe przechowywane są na dysku zewnętrznym w szafie pancernej.*
3. *Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.*
4. *Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.*

5. *Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii.*

Rozdział 7
Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego

1. *Za ochronę antywirusową systemu informatycznego odpowiada administrator danych osobowych.*
2. *System antywirusowy zainstalowany jest w każdym komputerze.*
3. *Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym.*
4. *Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.*
5. *W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora bezpieczeństwa informacji.*

Rozdział 8
Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. *Dane osobowe przetwarzane w Ośrodku mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.*
2. *Dane osobowe udostępnia się na pisemny, umotywowany wniosek chyba, że przepisy odrębne stanowią inaczej.*
3. *Dane udostępnione Ośrodkowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.*
4. *Dokładna kopia danych osobowych przesłanych do Zakładu Ubezpieczeń Społecznych przechowywana jest w bazie danych programu Płatnik w postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia dokumentu, datą wysłania zestawu,*
5. *Dokładna kopia danych osobowych przesłanych do banku przechowywana jest w bazie danych systemu bankowości elektronicznej do wejścia, której konieczne jest wprowadzenie loginu i hasła.*

Rozdział 9
Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1. *Wszelkie prace związane z naprawami sprzętu komputerowego wykonywane są przez firmę zatrudnioną przez administratora bezpieczeństwa informacji.*
2. *Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora danych osobowych.*