Załącznik Nr 1 do
zarządzenia Nr 5/2012
Dyrektora Ośrodka Kultury w Drawsku Pomorskim
z dnia 1 marca 2012r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W OŚRODKU KULTURY W DRAWSKU POMORSKIM

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Ośrodku Kultury w Drawsku Pomorskim oraz jego systemie informatycznym, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady bezpieczeństwa.

§1. Definicje

1) **ośrodek kultury** – należy przez to rozumieć Ośrodek Kultury w Drawsku Pomorskim;

2) **administrator danych** – Dyrektor Ośrodka Kultury w Drawsku Pomorskim;

3) **administrator bezpieczeństwa informacji (ABI)** – pracownik ośrodka kultury lub inna osoba wyznaczona przez administratora danych do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

4) **administrator systemu informatycznego (ASI)** – to osoba odpowiedzialna za nadzorowanie i utrzymanie systemu informatycznego ośrodka kultury oraz stosowanie technicznych i organizacyjnych środków ochrony;

5) **użytkownik systemu** – to osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym ośrodka kultury. Użytkownikiem może być pracownik ośrodka kultury, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno prawnej, osoba odbywająca staż w ośrodku kultury, wolontariusz;

6) **identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

7) **hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

8) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

9) **rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

10) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

11) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.

§2. Polityka bezpieczeństwa określa:

1) wykaz budynków oraz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujących zawartości poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i rozliczalności przetwarzanych danych.

§3. Obszar przetwarzania danych osobowych.

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych ośrodka kultury znajdujące się w budynku ośrodka kultury w Drawsku Pomorskim przy ul. Piłsudskiego 12 oraz w filiach biblioteki w Rydzewie, Suliszewie i Gudowie.

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

1. Za zbiór danych osobowych przetwarzanych w ośrodku kultury uważa się:

1) dokumentację papierową (korespondencja, wnioski, deklaracje, itd.),

2) systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji,

3) wydruki komputerowe.

2. Wykaz zbiorów danych osobowych przetwarzanych w ośrodku kultury wraz z programami służącymi do przetwarzania ww. zbiorów stanowi ***załącznik*** do Polityki bezpieczeństwa przetwarzania danych osobowych Ośrodka Kultury w Drawsku Pomorskim.

§5. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opis struktury przetwarzanych danych osobowych oraz relacje pomiędzy danymi, procesy przetwarzania oraz struktura danych zostały zawarte w dokumentacji technicznej systemów informatycznych dostępnej u dostawców oprogramowania informatycznego. Licencje

oprogramowania nie obejmują listingu danych źródłowych, lecz jedynie prawo korzystania z rozwiązań.

§6. Sposób przepływu danych pomiędzy poszczególnymi systemami.

1.Systemy, w których przetwarza się dane osobowe nie są ze sobą połączone, co uniemożliwia przepływ danych pomiędzy nimi. Wyjątek stanowi baza danych z aplikacji „Gratyfikant", z której dane są eksportowane do aplikacji „Płatnik" i „Rewizor". Przekazywane są następujące dane: imiona i nazwiska, data urodzenia, adres zamieszkania lub pobytu, numery PESEL i NIP, przynależność do NFZ oraz dane wynagrodzenia pracownika. Pozostałe programy są niezależne i posiadają samodzielne bazy danych.

2. Sposób przepływu danych – z programu „Gratyfikant" generowany jest plik o strukturze akceptowanej przez programy „Płatnik" oraz „Rewizor. Następnie programy „Płatnik" i „Rewizor" importują dane z przygotowanego pliku. Przepływ danych odbywa się w lokalnej sieci LAN pomiędzy serwerem, a stacją roboczą.

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

1. Dane w postaci elektronicznej.

Dane przetwarzane są przy użyciu komputerów pracujących wyłącznie w wewnętrznej sieci komputerowej odseparowanej od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall oraz programowe firewalle na stacjach roboczych, dodatkowo zabezpieczonych oprogramowaniem antywirusowym.

Dostęp do danych następuje po autoryzacji. Autoryzacja polega na podaniu identyfikatora oraz hasła przydzielonego przez administratora bezpieczeństwa informacji na podstawie zgody administratora danych.

Uwzględniając kategorie przetwarzanych danych wprowadza się wysoki poziom bezpieczeństwa. Środki bezpieczeństwa na poziomie wysokim określa Instrukcja zarządzania systemem informatycznym, stanowiąca załącznik Nr 2 do zarządzenia Nr 4 Dyrektora Ośrodka Kultury w Drawsku Pomorskim z dnia 1 marca 2012r.

2. Dane w rejestrach papierowych.

Dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach oraz kasach pancernych.

3. Środki organizacyjne

Administrator danych powołuje administratora bezpieczeństwa informacji (ABI), który nadzoruje przestrzeganie zasady ochrony danych określonych w instrukcji zarządzania systemem informatycznym z uwzględnieniem spraw dotyczących ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach oraz administratora systemów informatycznych (ASI), który jest odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie.

4. Środki ochrony fizycznej:

1) wejście do budynku ośrodka zabezpieczone jest zamkami drzwiowymi oraz alarmem. Poszczególne pokoje, w których odbywa się przetwarzanie danych osobowych i ich składowanie muszą być wyposażone w niezależne zamki i muszą być

zamykane podczas nieobecności pracownika. Odpowiedzialność za właściwą ochronę pomieszczeń ponosi pracownik oraz kierownik komórki organizacyjnej;

2) przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności administratora bezpieczeństwa informacji;

3) pomieszczenia, o których mowa wyżej, zamykane są na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych w sposób uniemożliwiający dostęp do nich osób trzecich. Klucze do pomieszczeń służbowych znajdują się w budynku ośrodka kultury – w miejscu wyznaczonym przez dyrektora ośrodka kultury. Pozostawienie kluczy w zamkach pomieszczeń, gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju);

4) w pomieszczeniach, w których przewiduje się przyjmowanie interesantów, monitory stanowisk komputerowych ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane;

5) pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy. Przed rozpoczęciem pracy klucze pobierane zostają z „szafki" pod nadzorem dyrektora przez pracownika ośrodka kultury i tam też składowane po zakończeniu pracy.

5.Środki sprzętowe, informatyczne i telekomunikacyjne:

1) urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej urządzeniem UPS,

2) dostęp fizyczny do sieci lokalnej jest ograniczony, centralny punkt dystrybucyjny sieci umieszczony jest w serwerowni,

3) dostęp logiczny do sieci lokalnej zabezpieczony jest adresem IP,

4) dostęp do sieci WAN zabezpieczony jest firewall – em wraz z oprogramowaniem antywirusowym,

5) kopie awaryjne wykonywane są w cyklach: dzienna na dysku twardym, tygodniowa na macierzy dyskowej,

6) każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki,

7) inne środki przetwarzania: drukarki, skanery, niszczarki dokumentów.