Załącznik Nr 3 do
zarządzenia Nr 5/2012
Dyrektora Ośrodka Kultury w Drawsku Pomorskim
z dnia 1 marca 2012 r.

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W OŚRODKU KULTURY W DRAWSKU POMORSKIM

§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 wyznaczony 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)** – informatyk, czyli osoba odpowiedzialna za funkcjonowanie systemu informatycznego ośrodka kultury oraz stosowanie technicznych i organizacyjnych środków ochrony;

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

6) **identyfikator użytkownika (login)** – 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) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

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

§2. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym, zwanym dalej „systemem" oraz wskazanie osoby odpowiedzialnej za te czynności:

1) uprawnienia do przetwarzania danych osobowych nadawane są za zgodą administratora danych na wniosek kierownika właściwej komórki organizacyjnej. Uprawnienia dotyczą zarówno danych osobowych gromadzonych w systemie informatycznym, jak również w tradycyjnych zbiorach papierowych;

2) zgoda na pracę w systemie informatycznym jest wymagana także dla użytkowników, którzy nie przetwarzają danych osobowych;

3) wprowadza się rejestr osób zatrudnionych przy przetwarzaniu danych osobowych oraz osób pracujących w systemie;

4) rejestr prowadzony jest przez administratora bezpieczeństwa informacji w postaci elektronicznej oraz papierowej;

5) uprawnienia o których mowa w pkt 2 odbierane są w przypadku ustania stosunku pracy lub na wniosek kierownika właściwej komórki organizacyjnej;

6) użytkowników systemu tworzy oraz usuwa za zgodą administratora danych, administratora bezpieczeństwa informacji lub osoby przez niego upoważnionej;

7) osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia;

8) każdy pracownik ośrodka kultury podpisze oświadczenie, którego wzór stanowi załącznik Nr 2 do niniejszej instrukcji.

§3. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem:

1) każdy użytkownik systemu dopuszczony do pracy przy przetwarzaniu danych osobowych powinien posiadać odrębny, jednoznacznie identyfikujący pracownika login;

2) wprowadza się obowiązek uwierzytelnienia własnego loginu poprzez podanie hasła;

3) zmianę hasła należy dokonywać nie rzadziej niż co 30 dni;

4) hasło składa się co najmniej z 8 znaków, musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
5) początkowe hasło dostępu ustala się z administratorem bezpieczeństwa informacji, a następnie użytkownik systemu samodzielnie zmienia je przy użyciu odpowiednich narzędzi informatycznych;
6) dane osobowe gromadzone są wyłącznie na serwerach. Zabrania się gromadzenia danych osobowych na innych nośnikach danych;

7) w uzasadnionych przypadkach, za zgodą administratora bezpieczeństwa informacji, dane osobowe można przetwarzać poza serwerem;

8) tworzy się rejestr zewnętrznych nośników informacji, na których przetwarzane są dane osobowe;

9) rejestr o którym mowa w pkt 8 prowadzi administrator bezpieczeństwa informacji;

10) za zabezpieczenie danych osobowych przechowywanych w tradycyjnych rejestrach papierowych odpowiadają kierownicy właściwych komórek organizacyjnych.

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

1) logowanie do systemu następuje po podaniu identyfikatora oraz hasła dostępu;

2) użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień;

3) zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu;

4) zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3;

5) zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera;

6) administrator bezpieczeństwa informacji lub osoba przez niego upoważniona monitoruje logowanie oraz wylogowanie się użytkowników, a także nadzoruje zakres przetwarzanych przez nich zbiorów danych.

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

1) archiwizacja zbiorów danych osobowych znajdujących się na serwerze wykonywana jest co najmniej jeden raz w tygodniu i zapisywana na zewnętrzne elektroniczne nośniki informacji;

2) kopie danych, o których mowa w ust.1, wykonuje administrator systemu informatycznego lub osoba przez niego upoważniona.

§6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz kopii zapasowych:

1) dane, o których mowa w § 5 ust. 1, zapisywane są na macierze dyskowe;

2) nośniki z danymi przechowywane są w ognioodpornej kasie metalowej, w pomieszczeniu do którego wyłączny dostęp ma administrator bezpieczeństwa informacji, administrator systemu informatycznego lub osoba przez niego upoważniona;

3) kopie danych, o których mowa w §5 ust.1, nadpisuje się w przypadku kończącej się wolnej przestrzeni dyskowej na macierzy;

4) 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 mechanicznie 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 przez administratora danych osobowych;

5) urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

§7. Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:

1) system obejmuje się ochroną antywirusową polegającą na skanowaniu serwerów oraz stacji roboczych programem antywirusowym;

2) skanowanie serwerów wykonywane jest co najmniej raz w tygodniu przez administratora systemu informatycznego lub osobę przez niego upoważnioną;

3) skanowanie stacji roboczych wykonują ich użytkownicy;

4) użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, a także plików danych pobieranych z zasobów sieci Internet oraz otrzymanych w poczcie elektronicznej;

5) w celu zabezpieczenia systemu przed ingerencją z zewnątrz, systemy posiadają włączone ściany ogniowe;

6) przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej system jest chroniony zasilaczami awaryjnymi (UPS);

7) każda jednostka komputerowa jest zabezpieczona hasłem do BIOS-a;

8) administrator bezpieczeństwa informacji lub osoba przez niego upoważniona monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

§8. Informacje o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia:

1) tworzy się centralną ewidencję udostępniania danych prowadzoną w formie elektronicznej oraz papierowej, która w szczególności powinna zawierać co najmniej następujące pola: nazwa odbiorcy, data udostępnienia, zakres udostępnienia;

2) ewidencję, o której mowa w pkt 1 prowadzi administrator bezpieczeństwa informacji;

3) kierownicy komórek organizacyjnych są zobowiązani do tego, aby o fakcie udostępniania danych informować administratora bezpieczeństwa informacji, który dokonuje odpowiednich zapisów w ewidencji o której mowa w pkt 1.

§9. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1) przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez administratora danych;

2) czynności określone w pkt 1 mogą być wykonywane w obecności osoby upoważnionej do przetwarzania danych osobowych;

3) tworzy się ewidencję osób upoważnionych do wykonywania prac o których mowa w pkt 1;

4) ewidencję o której mowa w pkt 3 prowadzi w formie elektronicznej i papierowej administrator bezpieczeństwa informacji. Ewidencja ta zawiera następujące pola: imię i nazwisko, data, zakres wykonywanej czynności.

§10. Szczegółowe zasady korzystania ze sprzętu komputerowego i systemów informatycznych, poczty elektronicznej oraz Internetu określa Regulamin Użytkownika Systemów Teleinformatycznych Ośrodka Kultury w Drawsku Pomorskim, który stanowi załącznik Nr 1 do niniejszej Instrukcji.

.