Instrukcja Zarządzania Systemem Informatycznym

DEFINICJE - ilekroć w niniejszym dokumencie jest mowa o:

1) **OSiR** – należy przez to rozumieć Ośrodek Sportu i Rekreacji w Łukowie
2) **Administratorze Danych Osobowych** – zwanym dalej ADO należy przez to rozumieć Dyrektora OSiR
3) **Administratorze Systemu Informatycznego** – zwanym dalej ASI należy przez to rozumieć osobę wyznaczoną przez ADO odpowiedzialną za funkcjonowanie systemu informatycznego OSiR.
4) **Użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym OSiR. Użytkownikiem może być pracownik OSiR, osoba wykonująca pracę na podstawie umowy o pracę, umowy–zlecenia, osoba odbywająca staż oraz osoba odbywająca praktyki w OSiR.
5) **Sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych OSiR wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej.

I. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r., Nr 101, poz.926 z późn.zm.)
   - Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym przetwarzania danych osobowych systemu informatycznego obowiązujących w OSiR
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik Nr 5 do Zarządzenia 64/2015 z dnia 30.12.2015 r.
3. Po spełnieniu wymogów określonych w pkt. I.1. i w pkt I.2. ADO pisemnie upoważnia osoby do przetwarzania danych osobowych (Załącznik Nr 4 do niniejszego Zarządzenia).
4. ASI po wydaniu upoważnienia przez ADO nadaje uprawnienia dostępu do systemu informatycznego i dokonuje rejestracji w rejestrze osób upoważnionych do przetwarzania danych osobowych Załącznik Nr 3 do niniejszego Zarządzenia.
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

9. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje również po ustaniu zatrudnienia.
10. Odebranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego, któremu pracownik podlega z podaniem daty oraz przyczyny odebranych uprawnień lub z zakończeniem okresu zatrudnienia.
11. Identyfikatory osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
12. ASI zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym
13. Rejestr powinien zawierać:
    - Imię i nazwisko użytkownika systemów informatycznych,
    - Datę nadania upoważnienia,
    - Datę ustania upoważnienia,
    - Zakres upoważnienia,
    - Login/identyfikator w systemie informatycznym,
    - podpis osoby upoważnionej,
    - Podpis ASI,
    - Podpis ADO.
14. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwić przeglądanie historii zmian uprawnień użytkowników.

II. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz na 30 dni.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej 0przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowego poinformowania ASI oraz zmiany hasła.
6. Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła – 8 znaków,
   b) zakazuje się stosować:
      - haseł, które użytkownik stosował uprzednio,
      - swojej nazwy użytkownika,
      - swojego imienia, drugiego imienia, nazwiska, pseudonimu, itp.,
      - imion, w szczególności imion osób z najbliższej rodziny,
      - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, nazwa ulicy przy której mieszka, itp.
      - przewidywalnych sekwencji znaków z klawiatury np. QWERTY, 1234567890, itp.
   i) należy stosować hasła zawierające kombinacje liter i cyfr.

7. Hasło użytkownika o prawach administratora posiada ADO.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu (zablokowania dostępu).
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcje wylogowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogowania się.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania.

IV. Procedury tworzenia zabezpieczeń

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada ASI, a w przypadku jego nieobecności ADO.
2. Kopie bezpieczeństwa wykonywane są na dyskach zewnętrznych bądź płytach DVD nie rzadziej niż raz na 2 tygodnie.
3. Kopie bezpieczeństwa zawierają dane służące do ich przetwarzania
4. ADO zleca okresowe kontrole kopii bezpieczeństwa pod kątem ich dalszej przydatności, a w przypadku ich uszkodzenia zleca ich likwidację.

V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

A. Elektroniczne nośniki informacji

1. Dane osobowe w postaci elektronicznej zapisane na dyskach CD, DVD czy dyskach twardych nie mogą być wynoszone poza siedzibę OSIR.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

B. Kopie zapasowe

1. Kopie zapasowe zbioru danych osobowych do przetwarzania danych są przechowywane w zamykanym sejfie zamykanej szafy pancernej znajdującej się w pomieszczeniu zamykanego magazynu podręcznego w biurze OSiR.
2. Dostęp do sejfu szafy pancernej ma ADO i ASI.

VI. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe.
2. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który zamierza używać nośnika.

3. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
4. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach – minimum raz w miesiącu.
5. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa.

VII. Połączenie do sieci Internet

Połączenie lokalnej sieci komputerowej OSiR z Internetem jest dopuszczalne wyłącznie po zainstalowaniu kompleksowego oprogramowania antywirusowego.

DYREKTOR

Zbigniew Biadun

Załącznik Nr 3 do Zarządzenia Nr 64/2015 z dnia 30.12.2015 r.

Rejestr osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Data nadania upoważnienia/ Numer upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login/ identyfikator w systemie informatycznym	Podpis osoby upoważnionej	Podpis ASI	Podpis ADO

Załącznik Nr 4 do zarządzenia Nr 64/2015 z dnia 30.12.2015 r.

Upoważnienie nr .....

z dnia .....

Działając na podstawie uprawnień nadanych mi w Ośrodku Sportu i Rekreacji w Łukowie w sprawie ochrony danych osobowych oraz w oparciu o art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2014 r., poz. 1182 z późn.zm.)

Upoważniam

Panią/Pana .....

do przetwarzania danych systemu informatycznego/nieinformatycznego oraz urządzeń wchodzących w jego skład zlokalizowanych w Ośrodku Sportu i Rekreacji w Łukowie służących do przetwarzania danych osobowych zawartych w zbiorze noszącym nazwę:

.....

.....

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w obowiązkach służbowych oraz Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r. , poz. 1182 z późn.zm.) i wydanych do niej przepisach oraz Zarządzeniu **Nr 64/2015 z dnia 30.12.2015 r. w sprawie ochrony przetwarzanych danych osobowych w Ośrodku Sportu i Rekreacji w Łukowie.**

Wymieniona osoba została wpisana do Rejestru osób upoważnionych do przetwarzania danych osobowych w Ośrodku Sportu i Rekreacji w Łukowie.

.....
podpis osoby upoważnionej

.....
podpis osoby wydającej upoważnienia

Załącznik Nr 5 do Zarządzenia Nr 64/2015 z dnia 30.12.2015 r.

.....
imię i nazwisko

.....
stanowisko

OŚWIADCZENIE

o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w **Ośrodku Sportu i Rekreacji w Łukowie** zasadach dotyczących przetwarzania danych osobowych, określonych w **„Polityce Bezpieczeństwa"** i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w **Ośrodku Sportu i Rekreacji w Łukowie.**

Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn.zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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). Poinformowano mnie również o grożącej, stosowanie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w **Ośrodku Sportu i Rekreacji w Łukowie** może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Łuków, dn.....r.
data złożenia oświadczenia

... ...
podpis pracownika

Załącznik Nr 6 do zarządzenia Nr 64/2015 z dnia 30.12.2015 r.

Ustanie/Cofnięcie*

Upoważnienia nr .....

z dnia .....

dot: przetwarzania danych systemu informatycznego/nieinformatycznego oraz urządzeń wchodzących w jego skład zlokalizowanych w Ośrodku Sportu i Rekreacji w Łukowie służących do przetwarzania danych osobowych przetwarzania danych osobowych w Ośrodku Sportu i Rekreacji w Łukowie

wydanego dla Pani/Pana

.....

.....
podpis pracownika

.....
podpis ADO

* *Niepotrzebne skreślić*

SZKOLENIA
Z ZAKRESU OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH

Temat: Zapoznanie się z dokumentami przetwarzania danych osobowych obowiązującymi w Ośrodku Sportu i Rekreacji w Łukowie.

Program szkolenia:

1. **Przedstawienie aktów prawnych**
   a) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r., poz. 1182 z późn.zm.)
   b) 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)
2. **Zapoznanie z Polityką Bezpieczeństwa w Ośrodku Sportu i Rekreacji w Łukowie.**
3. **Zapoznanie z Instrukcją Zarządzania Systemem Informatycznym w Ośrodku Sportu i Rekreacji w Łukowie.**
4. **Omówienie sposobu wypełnienia dokumentów**

- upoważnienia dla osób zatrudnionych przy przetwarzaniu danych osobowych
- oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami.

Wykaz osób uczestniczących w szkoleniu w dniu ..... r.

L.p.	Nazwisko i imię	Stanowisko	Podpis

.....

Podpis osoby przeprowadzającej szkolenie

REJESTR PROFILAKTYCZNYCH SKANOWAŃ ANTYWIRUSOWYCH

Lp.	Data skanowania	Stanowisko Komputerowe (nazwa komputera)	Uwagi	Podpis ASI

(Instrukcja Zarządzania Systemem Informatycznym stanowiąca Załącznik Nr 2 do Zarządzenia Nr 64/2015 Dyrektora Ośrodka Sportu i Rekreacji w Łukowie z dnia 30 grudnia 2015 r. roz. VI pkt 7)

REJESTR KOPII BEZPIECZEŃSTWA

Lp.	Data utworzenia kopii	Stanowisko Komputerowe (nazwa komputera)	Nośniki kopii	Uwagi	Podpis ASI

(Instrukcja Zarządzania Systemem Informatycznym stanowiąca Załącznik Nr 2 do Zarządzenia Nr 65/2015 Dyrektora Ośrodka Sportu i Rekreacji w Łukowie z dnia 30 grudnia 2015 r. roz. IV pkt 1-3)