OŚRODEK SPORTU i REKREACJI
w SUWAŁKACH
ul. Wojska Polskiego 2
16-400 SUWAŁKI
NIP 844-19-33-618

ZARZĄDZENIE NR 35/2018

Dyrektora Ośrodka Sportu i Rekreacji w Suwałkach
z dnia ...6. czerwca..... 2018 roku

w sprawie: **ustalenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Sportu i Rekreacji w Suwałkach**

Na podstawie artykułu 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) opublikowanego w Dzienniku Urzędowym Unii Europejskiej L119 4 maja 2016 r. i ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r., poz. 1000) zarządzam, co następuje:

§ 1.

1. Ustalam Politykę bezpieczeństwa Ośrodka Sportu i Rekreacji w Suwałkach w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. Ustalam Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Sportu i Rekreacji w Suwałkach w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§ 2.

Wykonanie niniejszego zarządzenia powierzam Zastępcy Dyrektora i kierownikom komórek organizacyjnych Ośrodka Sportu i Rekreacji w Suwałkach.

§ 3.

Traci moc zarządzenie nr 44/2013 Dyrektora Ośrodka Sportu i Rekreacji z dnia 12 sierpnia 2013 roku w sprawie ustalenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Sportu i Rekreacji.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz

OŚRODEK SPORTU i REKREACJI
w SUWAŁKACH
ul. Wojska Polskiego 2
16-400 SUWAŁKI
NIP 844-19-33-618

Załącznik Nr 1 do Zarządzenia nr 35/2018
Dyrektora Ośrodka Sportu i Rekreacji
z dnia 6 czerwca 2018 roku

POLITYKA BEZPIECZEŃSTWA
OŚRODKA SPORTU I REKREACJI W SUWAŁKACH

Realizując postanowienia **Ogólnego Rozporządzenia o Ochronie Danych Osobowych 2016/679 (RODO) oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. rok 2018 pozycja 1000)** ustalam reguły oraz zasady pozwalające na zapewnienie ochrony danych osobowych w Ośrodku Sportu i Rekreacji w Suwałkach.

§ 1

1. Celem polityki bezpieczeństwa jest takie postępowanie, aby osoby upoważnione do przetwarzania danych osobowych w pełni zabezpieczyły dostęp do nich przed osobami nieupoważnionymi i gromadziły w zbiorach dane zgodnie z wymogami ustawy.
2. Polityką bezpieczeństwa objęte są dane osobowe, którymi zgodnie z ustawą są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. Reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych obowiązują, także w przypadku przetwarzania danych poza zbiorem danych.
4. Całokształt działań w ramach polityki bezpieczeństwa jest wymogiem ustawowym i ma za zadanie ochronę prywatności osób, których dane są przetwarzane.
5. Niniejsza polityka bezpieczeństwa zawiera:

a) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

c) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

d) sposób przepływu danych pomiędzy poszczególnymi systemami,

e) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 2

Obszar, w którym przetwarzane są dane osobowe stanowią pomieszczenia budynków wchodzących w skład Ośrodka Sportu i Rekreacji w Suwałkach wymienione w ***Załączniku nr 1*** stanowiącym integralną część niniejszej polityki bezpieczeństwa.

§ 3

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opisem struktury zbiorów danych znajduje się w ***Załączniku nr 2*** stanowiącym integralną część niniejszej polityki bezpieczeństwa .

§ 4

Przepływ danych pomiędzy poszczególnymi systemami jest ustalony i kontrolowany przez Administratora Danych.

Udostępnianie danych osobowych poza Ośrodek Sportu i Rekreacji w Suwałkach jest kontrolowane przez Administratora Danych i zabezpieczone przed dostępem dla osób i jednostek nieupoważnionych.

Szczegóły przepływu danych pomiędzy systemami zawiera ***Załącznik nr 2*** do polityki bezpieczeństwa OSiR w Suwałkach (Opis struktury zbiorów danych i ich powiązań).

§ 5

Ośrodek Sportu i Rekreacji w Suwałkach posiada środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Funkcjonują zabezpieczenia:

1. dostępu do budynków i pomieszczeń:
   1) kontrola dostępu do budynku i pomieszczeń, w których przetwarza się i archiwizuje dane osobowe, zabezpieczenie okien w budynkach/pomieszczeniach przed nieuprawnionym dostępem,
   2) system alarmowy lub nadzór nad budynkami /pomieszczeniami w dniach/okresach wolnych od pracy,
   3) zamki w drzwiach wejściowych pomieszczeń, zamykane w okresach, gdy w pomieszczeniach nie pracują osoby upoważnione;
   4) odpowiednio bezpieczne ustawienie stacji roboczych – w taki sposób, aby osoby postronne nie widziały danych na wyświetlaczach;
   5) prowadzony jest nadzór nad budynkami przez wyznaczonych pracowników lub firmy, z którymi zawarte zostały odpowiednie porozumienia;

2. zasilania systemów informatycznych poprzez zastosowanie urządzeń podtrzymujących napięcie (UPS) w serwerowni i na stanowiskach komputerowych,

3. systemów informatycznych:

1) dostęp do systemu jedynie przez osoby upoważnione (system identyfikatorów i haseł),
2) poziomy uprawnień,
3) kopie awaryjne na nośniku zewnętrznym,
4) przechowywanie nośników z kopiami awaryjnymi w zabezpieczonych szafach lub sejfach.
5) wygaszacze ekranów i czasowe wylogowywanie się, blokowanie systemu, przymusowe ponowne logowanie się
6) wydruki składowane w miejscach niedostępnych dla osób postronnych;
7) systemowe zabezpieczenia stacji roboczych (firewall)
8) programowe zabezpieczenia przed dostępem osób nieupoważnionych oraz instalacją programów szpiegowskich;

§ 6

1. Wszystkie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych zobowiązane są do bezwzględnego przestrzegania podanych w niniejszym opracowaniu reguł i zasad tworzących politykę bezpieczeństwa.
2. Nadzór organizacyjny nad bezpieczeństwem i przestrzeganiem przepisów zapewniający poufność, integralność i rozliczalność przetwarzanych danych osobowych sprawują osoby wyznaczone przez Administratora Danych, w którego imieniu występuje Dyrektor Ośrodka Sportu i Rekreacji w Suwałkach.

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz

Załącznik Nr 1
do Polityki bezpieczeństwa Ośrodka Sportu i Rekreacji w Suwałkach

Obszar Ośrodka Sportu i Rekreacji w Suwałkach, w którym przetwarzane są dane osobowe:

Lp	Nazwa obiektu	Kod obiektu	Adres budynku	Obszar / Dział (komórka)	Oznaczenie pomieszczenia
1	Biuro	BI	Wojska Polskiego 2	**Dyrektor OSiR w Suwałkach**	207
2	Pływalnia	PŁ	Wojska Polskiego 2	Zastępca Dyrektora OSiR w Suwałkach (ZD)	-
3	Biuro	BI	Wojska Polskiego 2	Kierownik Działu Administracji i Kadr (DAiK)	26
4	Biuro	BI	Wojska Polskiego 2	Dział Administracji i Kadr (DAiK)	26, 27
5	Biuro	BI	Wojska Polskiego 2	Sekretariat (DAiK)	206
6	Biuro	BI	Wojska Polskiego 2	Komisja Socjalna (DAiK)	26
7	Biuro	BI	Wojska Polskiego 2	Główny Księgowy (DF)	29
8	Biuro	BI	Wojska Polskiego 2	Dział Finansowy (DF)	28,26
9	Biuro	BI	Wojska Polskiego 2	Kierownik Dz.Sportu, Rekr. i Marketingu (DS)	2
10	Biuro	BI	Wojska Polskiego 2	Dział Sportu Rekreacji i Marketingu (DS)	1
11	Biuro	BI	Wojska Polskiego 2	Serwerownia	-
12	Aquapark	AQ	Papieża Jana Pawła II 7	Kierownik Aquaparku (AQ)	1.6
13	Aquapark	AQ	Papieża Jana Pawła II 7	Sekretariat (AQ)	1.7
14	Aquapark	AQ	Papieża Jana Pawła II 7	Rozliczenia (AQ)	1.4
15	Aquapark	AQ	Papieża Jana Pawła II 7	Kasy strefa basenowa (AQ)	0.6
16	Aquapark	AQ	Papieża Jana Pawła II 7	Kasa strefa saunowa (AQ)	1.33
17	Aquapark	AQ	Papieża Jana Pawła II 7	Kierownik Utrzymania Ruchu (AQ)	1.3
18	Aquapark	AQ	Papieża Jana Pawła II 7	Główny specjalista ds. BHP (DAiK)	1.8
19	Aquapark	AQ	Papieża Jana Pawła II 7	Ochrona (AQ)	0.41
20	Aquapark	AQ	Papieża Jana Pawła II 7	Serwerownia (AQ)	0.41a
21	Aquapark	AQ	Papieża Jana Pawła II 7	Sala konferencyjna (AQ)	1.13
22	Aquapark	AQ	Papieża Jana Pawła II 7	Multimedia (AQ)	1.52
23	Aquapark	AQ	Papieża Jana Pawła II 7	Ratownicy (AQ)	0.17
24	Aquapark	AQ	Papieża Jana Pawła II 7	Technicy (AQ)	-1.15

25	Miejski Plac Zabaw	MPZ	Papieża Jana Pawła II 7	Miejski Plac Zabaw (AQ)	—
26	Biuro	BI	Wojska Polskiego 2	Kierownik ZO I	25
27	Biuro	BI	Wojska Polskiego 2	Hale sportowe obsługa (ZO I)	01
28	Pływalnia	PŁ	Wojska Polskiego 2	Recepcja i zaplecze administracyjno-sportowe (ZO I)	-
29	Stadion lekkoatletyczny	LA	Wojska Polskiego 17a	Recepcja i zaplecze administracyjno-sportowe (ZO I)	-
30	Stadion lekkoatletyczny	LA	Wojska Polskiego 17a	Modelarnia (DS.)	-
31	Hostel Wigry	HW	Zarzecze 26	Kierownik ZO II	-
32	Hostel Wigry	HW	Zarzecze 26	Recepcja (ZO II)	-
33	Eurocamping	EC	Zarzecze 26	Recepcja (ZO II)	-
34	Stadion piłkarski	SP	Zarzecze 26	Biura i kasy	-
35	Ośrodek Żeglarski	OŻ	Zastawie 38a	Kierownik ZO III	-
36	Ośrodek Żeglarski	OŻ	Zastawie 38a	Biuro (ZO III)	-
37	Ośrodek Wypoczynkowo-Żeglarski	OWŻ	Stary Folwark 55d	Recepcja (ZO III)	-
38	Zalew"Arkadia"	ZA	Wojska Polskiego 2	Teren Zalewu (ZOIII)	-

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz

Załącznik nr 2 do Polityki Bezpieczeństwa Ośrodka Sportu i Rekreacji w Suwałkach

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

lp	Nazwa zbioru danych	Sposób przetwarzania / nazwa systemu	Obszary / działy przetwarzania	Struktura przetwarzanych danych osobowych	Sposób pozyskania danych lub zbiór, z którego wpływają	Sposób wykorzystania, obszary i zbiory, do których dane przechodzą	Cel przetwarzania
1	Kadry i płace – pracownicy, byli pracownicy, zleceniobiorcy	PROGMAN – moduł Kadry, Płace, Zlecone	BI/DAiK, BI/DF	Imię, nazwisko, nazwisko rodowe, adres , PESEL, NIP,seria i nr dowodu os., data i miejsce urodz., imiona rodziców, telefon	akta osobowe, kartoteki, wykazy, skorowidze, umowy	wersja papierowa; po wykorzystaniu do składnicy akt;	w związku z zatrudnieniem
2	Dane kadrowe do rozliczeń z ZUS	PŁATNIK	BI/DAiK, BI/DF	Imię, nazwisko, adres , PESEL, NIP, data urodzenia, obywatelstwo	PROGMAN	na zewnątrz- ZUS; wersja papier. -Dział Finansowy, składnica akt	w związku z zatrudnieniem
3	Dokumentacja ZFŚS	wpisy ręczne, kopie el.	BI/DAiK/Komisja Socjalna	Imię, nazwisko, adres, seria i nr dowodu os., stan rodz., oświadczenia o dochodach	wnioski pracowników-wersja papierowa	wersja papierowa do składnicy akt;	w związku z zatrudnieniem
4	Dziennik korespondencji	wpisy ręczne, dok.wychodzące kopie el.	wszystkie komórki OSiR	Imię, Nazwisko,adres,telefon	dokumenty przychodzące i wychodzące	wersja papierowa do składnicy akt;	potwierdzenie przepływu dokumentów
5	Rejestr umów zamówień publicznych	Excel	BI/DAiK	Imię, nazwisko,adres,telefon	oferty,dokumenty zamówień, przetargów	na zewnątrz -Urząd Zamówień Publicznych	dokumentacja umów cywilnopr.
6	Kontrahenci OSiR	System PROGMAN	wszystkie komórki OSiR	Imię, nazwisko, NIP, PESEL, adres	okazane dokumenty, oświadczenia, zestawienia	ZUS,US,UM/Gminy Suwałki, UMWoj. Podl., firmy ubezp., banki, wersja pap. – skł. akt	fakturowanie, rozliczenia finansowe
7	Kontrahenci archiwalni	System WFGANG i SYMFONIA	BI/DF	Imię, nazwisko, NIP, PESEL, adres	nie aktualizuje się	tylko przeglądanie	rozliczenia finansowe
8	Bankowość elektroniczna	System PEKAO Biznes 24	BI/DF	Imię, nazwisko, adres	okazane dokumenty, oświadczenia	banki	rozliczenia finansowe
9	Rejestr umów OSIR	dok.papierowe, kopie elektron.	BI/DF-centralnie, pozostałe komórki-kopie(podzbiory)	Imię, nazwisko, NIP, PESEL, adres , data i m-ce urodz.	okazane dokumenty, oświadczenia	dane umów,Kontrahenci OSiR, Bankowość elektron.	System Eobiekt, system PROGMAN
10	PZU - eRU	zdalnie - przez Internet	BI/DF	Imię, nazwisko, adres , PESEL, NIP, data urodzenia, obywatelstwo	deklaracja złożona przez pracownika	zbiór w PZU - dane do ubezpieczenia gupowego pracownika	w związku z zatrudnieniem
11	ZUS - PUE (Platforma Usłu Elektronicznych)	zdalnie - przez Internet - przeglądanie	BI/DF	Imię, nazwisko, adres , PESEL, NIP, data urodzenia, obywatelstwo	dane z ZUS	zbiór w ZUS - dane pracowników do ubezpieczenia społecznego	w związku z zatrudnieniem

12	Lista uczestników zawodów sportowych	Edytor tekstowy lub lista ręczna	BI/DSRiM	Imię, nazwisko, płeć, telefon, data urodzenia, nazwa szkoły,nr klasy, adres zamieszkania	Od uczestników, opiekunów, głównego sędziego/organizatora	Archiwizacja OSiR : DSRiM lub Dział Finansowy, przekazywanie komunikatów sportowych do mediów	organizacja zawodów sportowych
13	Lista zawodników sekcji sportowych OSiR	Zestawienia papierowe i elektroniczne	BI/DSRiM	Imię i Nazwisko, adres, telefon, e-mail, Pesel	okazane dokumenty	Ewidencja zajęć	w związku z udziałem w zajęciach sport.
14	Ewidencja karnetów - nagród	wpisy ręczne	BI/DSRiM	Imię, nazwisko, adres	wg okazanych dokumentów	Ewidencja, rozliczenia,po wykorzystaniu do skł. akt	umowa cywilnoprawna
15	Ewidencja pobytów w obiektach OSiR	wpisy ręczne	ZOII/EC ZOII/HW ZOIII/OWŻ	Imię, nazwisko, adres, nr dowodu tożsamości, PESEL,	wg okazanych dokumentów	Usuwany po zakończeniu okresu wykorzystania	w związku z pobieraniem opłaty
16	Konta klientów Aquaparku	Eobiekt	AQ/ kasy, AQ/rozliczenia	Nazwisko i imię, telefon	Formularze kont klienta lub Bony-nagrody	Dział Finansowy	umowa cywilnoprawna
17	Kontrahenci Aquaparku	Eobiekt	AQ/ kasy, AQ/rozliczenia	Nazwisko i imię,firma, adres, NIP	Podaje klient	Dział Finansowy	wystawienie faktury
18	Kontakty e-mail	Programy pocztowe	wszystkie komórki OSiR	nazwy, podpisy, dane w treści	W poczcie elektronicznej wg listy adresów e-mail OSiR	Korespondencja - kasowane po wykorzystaniu	Załatwianie spraw
19	Ewidencja uczestników zajęć	Edytor tekstowy, kopia papier	AQ/ kasy, AQ/rozliczenia, AQ/sekretariat	Imię, nazwisko, adres, telefon,data i m-ce ur., pesel, osoba upow.	Formularze zgłoszeniowe	Po wykorzystaniu do składnicy akt	umowa cywilnoprawna
20	Dane kontaktowe pracowników	Edytor tekstowy, kopia papier	AQ/ sekretariat	Imię, nazwisko, numer telefonu	Od pracowników	usuwane po wykorzystaniu	w związku z zatrudnieniem, kontakt
21	Ewidencja wypadków pracowników	wpisy ręczne, edytor tekstowy	AQ/BHP	Nazwisko i imię, data urodz., adres, pesel, nr dow.os.	System kadrowy, dokumentacja wypadkowa	System płacowy	w związku z zatrudnieniem
22	Ewidencja wypadków klientów	wpisy ręczne, edytor tekstowy	AQ/BHP, AQ/Ratownicy ZOI/Pływalnia	Nazwisko i imię, data urodz., adres, pesel, nr dow.os.	Karty wypadków, Dziennik pracy punktu sanitarnego na pływalni	Firmy ubezpieczające, roszczenia	Dokumentacja powypadkowa
23	Skierowania kuratorów sądowych	wpisy ręczne, kopie elektroniczne	BI/DAiK	Nazwisko,imię, data ur. Adres,Pesel	Dokumenty wpływające	Kierownicy komórek org., kuratorzy sądowi	Decyzja
24	Szkolenia BHP pracowników OSiR	wpisy ręczne	AQ/BHP	Nazwisko,imię, data urodzenia	System kadrowy	System kadrowy, Firmy szkolące	w związku z zatrudnieniem

25	Pracownicy i zleceniobiorcy	wpisy ręczne, kopie elektroniczne	BI/DAiK, BI/DF	Nazwisko,imię oraz inne dane wg uznania piszącego pismo	Dokumenty i formularze wpływające - papierowe	dane wejściowe; wersja papierowa po wykorzystaniu do składnicy akt;	PROGMAN Kadry i Płace
26	OBRAZY Z MONITORINGU	ELEKTRONICZNIE - SYSTEM CCTV	AQ, ZOI, ZOII	OBRAZY W ZASIĘGU KAMER	NAGRANIA-FILMY	NADPISYWANE NOWYMI DANYMI-KOPIE NA ŻĄDANIE UPR.ORGANÓW	BEZPIECZEŃSTWO WEWN. I DLA SŁUŻB SPECJ.
27	Informacje medialne	Narzędzia www, edytory tekstów i obrazów	BI/DSRiM	Zdjęcia, nazwisko,imię, rok ur.	Podczas imprez, od uczestników i organizatorów imprez	Informacje publikowane sa stronach www i w ogłoszeniach	Działalność statutowa OSiR
28	Formularze kont klientów	ręcznie	AQ/Rozliczenia	Nazwisko, imię, nr telefonu	wypełnia klient	dane wejściowe	System Eobiekt
29	Rejestr rzeczy zgubionych	ręcznie	AQ/Rozliczenia	Nazwisko, imię,adres,telefon,Pesel/nrdo	dane od klienta	Potwierdzenie odbioru - do wglądu w razie potrzeby	Zarządzenie Dyrektora OSiR
30	Dokumenty rozliczeniowe kontrahentów OSiR	papierowe, kopie elektroniczne	BI/DF	Nazwisko, imię,adres, nazwa firmy, NIP, nr konta bank.	Dokumenty wpływające i wewnętrzne	dane wejściowe	System PROGMAN
31	Dokumentacja archiwalna pracowników	wydruki Kadry i Płace PROGMAN, dok. zewnętrzne	BI/DF	Imię i nazwisko, PESEL, adres, data urodzenia	Dane kadrowe, listy płac, dekl. PIT-11	przechowywane w celach archiwalnych	dane do US ZUS dla pracowników

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz

OŚRODEK SPORTU i REKREACJI
w SUWAŁKACH
ul. Wojska Polskiego 2
16-400 SUWAŁKI
NIP 844-19-33-618

Załącznik Nr 2 do Zarządzenia nr 35/2018
Dyrektora Ośrodka Sportu i Rekreacji
z dnia 6 grudnia 2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W OŚRODKU SPORTU I REKREACJI W SUWAŁKACH

Rozdział 1
Postanowienia ogólne

§ 1

Instrukcja reguluje zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Sportu i Rekreacji w Suwałkach.

§ 2

Przetwarzanie danych osobowych w Ośrodku Sportu i Rekreacji w Suwałkach odbywa się na zasadach określonych w **Ogólnym Rozporządzeniu o Ochronie Danych Osobowych 2016/679 (RODO) oraz w ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. rok 2018 pozycja 1000)**

§ 3

Celem wprowadzenia niniejszej instrukcji jest ochrona danych osobowych zawartych w systemach informatycznych eksploatowanych w lokalnych sieciach komputerowych Ośrodka. Instrukcja ta, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz postępowania w przypadku zaniku napięcia dla użytkowników systemu,
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych zbiorów danych,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
7) sposób realizacji wymogu odnotowania informacji o odbiorcach danych, którym zostały udostępnione dane zawarte w zbiorach niejawnych,
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Rozdział 2
Objaśnienia

§ 4

Przez użyte w instrukcji określenia należy rozumieć:

1) **dane osobowe** – wszelkie informacje o określonej lub dającej się określić osobie fizycznej,
2) **zbiór danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3) **Administrator Danych** – (zwany w dalszej części AD) rozumie się przez to Ośrodek Sportu i Rekreacji w Suwałkach, w imieniu którego działa Dyrektor Ośrodka Sportu i Rekreacji w Suwałkach, decydujący o celach i środkach przetwarzania danych osobowych,

4) **przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, przeglądanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zarówno w systemach informatycznych, jak i metodami tradycyjnymi(kartoteki, księgi, wykazy),
5) **system informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6) **Administrator Systemu Informatycznego** – (zwany w dalszej części ASI) informatyk lub inny pracownik, zajmujący się zarządzaniem całością lub wydzieloną częścią systemu informatycznego, odpowiadający za jej sprawne działanie. Do zadań ASI należy nadzorowanie pracy serwerów, dodawanie i kasowanie kont ich użytkowników, konfiguracja komputerów, instalowanie oprogramowania, dbanie o bezpieczeństwo systemu informatycznego, nadzorowanie, eliminowanie nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalatorskich, konfiguracyjnych i naprawczych,
7) **użytkownik systemu informatycznego** – pracownik Ośrodka Sportu i Rekreacji w Suwałkach posiadający upoważnienie do pracy w tym systemie,
8) **OSiR** – Ośrodek Sportu i Rekreacji w Suwałkach,
9) **kierownik komórki organizacyjnej** – kierownik wyodrębnionej komórki organizacyjnej zgodnie z Regulaminem Organizacyjnym OSiR,
10) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) podmiotu mającego zawartą umowę na piśmie, w zakresie i celu przewidzianym w umowie,
    d) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
11) **Inspektor Ochrony Danych Osobowych** - (zwany w dalszej części IODO) osoba wyznaczona przez Dyrektora Ośrodka Sportu i Rekreacji w Suwałkach. Jest ona odpowiedzialna za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemach informatycznych Ośrodka. Do jej obowiązków należy w szczególności:

- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- przeprowadzanie okresowych kontroli poprawności funkcjonowania zabezpieczeń systemów informatycznych,
- podejmowanie stosownych działań zgodnie z niniejszą instrukcją w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczeń systemu informatycznego.

12) **identyfikator użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
13) **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
14) **karta mikroprocesorowa** – uniwersalny nośnik w postaci karty plastikowej z umieszczonym na niej mikroprocesorem, który pozwala na ochronę procesu logowania użytkownika, podpisywanie dokumentów i poczty elektronicznej oraz szyfrowanie,
15) **pin** – kod, przyznawany do każdej karty mikroprocesorowej, umożliwiający autoryzację użytkownika przy użyciu karty mikroprocesorowej,
16) **autoryzacja** – proces, w którym sprawdzane jest czy dana osoba ma prawo dostępu do systemu informatycznego. Odpowiednie uprawnienia są przypisane do konkretnej, zidentyfikowanej osoby. Autoryzacja jest zwykle poprzedzona uwierzytelnieniem (zidentyfikowaniem) podmiotu,
17) **uwierzytelnienie** – proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby. Uwierzytelnienie zwykle odbywa się przez podanie odpowiedniego loginu i hasła, można też użyć do tego celu karty mikroprocesorowej,

18) **UPS**–zasilacz awaryjny podtrzymujący pracę komputera po zaniku napięcia zasilającego,
19) **sieć LAN** – lokalna sieć komputerowa,
20) **sieć publiczna** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późniejszymi zmianami),
21) **zapora ogniowa** – (ang. firewall – "ściana ogniowa"), jeden ze sposobów zabezpieczania sieci i systemów informatycznych przed intruzami. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz,
22) **urządzenia klasy UTM** – (ang. unified threat management / zunifikowane zarządzanie zagrożeniami), oferujące kompletną wielowarstwową ochronę przed zagrożeniami z Internetu, takimi jak oprogramowanie szpiegowskie, wirusy, ataki sieciowe i inne.

Rozdział 3
Obowiązki pracownicze wynikające z ochrony danych osobowych
§ 5

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.
3. Kierownicy komórek organizacyjnych Ośrodka są zobowiązani do:

a) zastosowania niezbędnych środków technicznych i organizacyjnych, określonych w przepisach powszechnie obowiązujących w celu zapewnienia ochrony przetwarzania danych osobowych,
b) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników,
c) sygnalizowania niezgodności aktów prawnych oraz aktów wewnętrznych Ośrodka z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej.

4. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez AD, w zakresie indywidualnych obowiązków pracowniczych.
5. Osoba upoważniona przez AD jest zobowiązana do:

a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
b) stosowania określonych procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
c) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą,
d) podporządkowania się poleceniom kierownika komórki organizacyjnej i przestrzegania ustalonych przez niego szczegółowych zasad i procedur.

Rozdział 4
Postępowanie przy upoważnianiu osób do przetwarzania danych osobowych
§ 6

1. W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, kierownik komórki organizacyjnej obowiązany jest sporządzić dla niego i odpowiednio wypełnić Upoważnienie do przetwarzania danych osobowych, którego treść stanowi ***załącznik nr 1.***
2. W przypadku przyjęcia do pracy kierownika komórki organizacyjnej lub pracownika na samodzielnym stanowisku pracy, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Dyrektor Ośrodka Sportu i Rekreacji w Suwałkach obowiązany jest wydać takiemu pracownikowi upoważnienie do przetwarzania danych osobowych.

3. Pracownik, któremu AD udzieli upoważnienia, którego treść stanowi ***załącznik nr 1*** jest zobowiązany do jego podpisania, czym przyjmuje je do wiadomości i stosowania.
4. Przepisy ustępu 1, 5, 9 i 10 stosuje się odpowiednio do praktykantów i stażystów odbywających praktykę lub staż w Ośrodku.
5. W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, kierownik komórki organizacyjnej obowiązany jest bezzwłocznie skierować wniosek o wydanie bądź cofnięcie upoważnienia do przetwarzania danych osobowych do AD.
6. W przypadku zmiany stanowiska, bądź zakresu obowiązków kierownika komórki organizacyjnej lub pracownika na samodzielnym stanowisku pracy, Dyrektor Ośrodka Sportu i Rekreacji w Suwałkach obowiązany jest bezzwłocznie wydać bądź cofnąć upoważnienie do przetwarzania danych osobowych.
7. Wypowiedzenie umowy o pracę przez pracodawcę jest równocześnie cofnięciem upoważnienia do przetwarzania danych osobowych.
8. W sytuacji wypowiedzenia umowy o pracę przez pracownika, upoważnienie traci moc z datą rozwiązania umowy o pracę.
9. Ewidencję pracowników upoważnionych do przetwarzania danych osobowych prowadzi IODO – wzór ewidencji stanowi ***załącznik nr 2.***
10. Wnioski o nadanie lub cofnięcie uprawnień przechowywane są w aktach IODO.
11. Upoważnienia do przetwarzania danych osobowych sporządzane są w 4 egzemplarzach, z których pierwszy otrzymuje osoba upoważniana, drugi przechowuje IODO, trzeci przechowuje kierownik komórki organizacyjnej osoby upoważnianej a czwarty przekazuje się do Działu Kadr do akt osobowych upoważnionego pracownika.

Rozdział 5
Postępowanie w przypadku naruszenia bezpieczeństwa danych osobowych
§ 7

1. Za kontrolę, przeglądy i nadzór nad konserwacją systemów informatycznych służących do przetwarzania danych osobowych odpowiedzialny jest IODO, a w szczególności:
- na wniosek AD dokonuje kontroli oraz oceny stanu bezpieczeństwa danych osobowych,
- dokonuje kontroli systemu informatycznego po uzyskaniu informacji o próbie nieautoryzowanego dostępu, wystąpieniu zagrożenia wirusem komputerowym lub innym złośliwym programem,
2. W przypadku uzasadnionego podejrzenia naruszenia zasad ochrony danych osobowych w Ośrodku, pracownik zobowiązany jest do niezwłocznego poinformowania o tym kierownika komórki organizacyjnej.
3. Kierownik komórki organizacyjnej, po dokonaniu oceny stanu faktycznego i stwierdzeniu naruszenia, jest zobowiązany poinformować o tym fakcie IODO.
4. W przypadku powtarzającego się naruszenia zasad ochrony danych osobowych, pracownik jest zobowiązany do niezwłocznego poinformowania o tym fakcie IODO.
5. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym jest IODO, którego zadaniem jest w szczególności przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

Rozdział 6
Ogólne zasady eksploatacji systemów komputerowych i systemów przetwarzania danych osobowych
§ 8

1. W obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby których dane dotyczą, ASI oraz inne osoby indywidualnie upoważnione przez Dyrektora Ośrodka Sportu i Rekreacji w Suwałkach.

2. Pomieszczenia w obszarze przetwarzania danych osobowych muszą być zamykane na zamek w czasie nieobecności pracowników.
3. Monitory komputerów na których odbywa się przetwarzanie danych osobowych muszą być zlokalizowane w sposób uniemożliwiający wgląd osobom trzecim.
4. Ekrany monitorów komputerów na których odbywa się przetwarzanie danych osobowych muszą być automatycznie wyłączane po upływie 15 minut nieaktywności użytkownika.
5. Dyski i taśmy magnetyczne zawierające dane osobowe, a przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do otrzymania danych, przed oddaniem są pozbawiane zapisu.
6. Wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji, są w ciągu dnia gromadzone na stanowiskach pracy i na koniec dnia niszczone w niszczarce dokumentów.
7. Zabronione jest wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem, a w szczególności instalowania gier, komunikatorów internetowych oraz oprogramowania innego niż niezbędne do realizacji przetwarzania danych i/lub realizacji innych zadań służbowych oraz instalowania oprogramowania przez osoby do tego nieuprawnione i bez wiedzy IODO.
8. Zabronione jest wykonywanie kopii danych osobowych oraz wydruków danych osobowych w celach innych niż wynikające z zasad przetwarzania danych, archiwizacji i/lub przekazania danych podmiotowi uprawnionemu.
9. Nośniki danych zawierające dane osobowe muszą być przechowywane w zamkniętych szafach.

Rozdział 7
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 9

1. Rejestrowanie użytkownika systemu informatycznego oraz nadawanie mu uprawnień do przetwarzania danych osobowych odbywa się na podstawie upoważnienia wydanego przez AD.
2. Osobą odpowiedzialną za przekazanie administratorowi właściwego systemu informatycznego zlecenia założenia konta użytkownika zgodnie z przyznanym upoważnieniem jest IODO.
3. ASI tworzy konto nowego użytkownika zgodnie z identyfikatorem podanym w upoważnieniu do przetwarzania danych i nadaje użytkownikowi uprawnienia zgodnie z zakresem podanym w tym upoważnieniu.
4. Hasło dostępu użytkownik zmienia bezpośrednio po uzyskaniu dostępu do systemu oraz co najmniej raz na miesiąc lub raz na rok w przypadku stosowania kart mikroprocesorowych służących do uwierzytelnienia hasła.
5. Użytkownik zmienia hasło w przypadku kompromitacji hasła.
6. Użytkownik zmienia pin w przypadku kompromitacji pinu.
7. Użytkownicy zobowiązani są do utrzymania w tajemnicy haseł dostępu i pinów, również po upływie ich ważności.
8. Przy stwierdzeniu próby włamania do systemu informatycznego lub podejrzeniu o kompromitację hasła, ASI blokuje konto i powiadamia IODO.
9. W przypadku rozwiązania lub ustania stosunku pracy konto jest blokowane w systemie informatycznym. Odpowiada za to IODO. Fakt ten musi być odnotowany w ewidencji osób przetwarzających dane osobowe.

§ 10

W przypadku gdy użytkownik systemu informatycznego zmienił stanowisko pracy stosuje się zasady z § 9.

Rozdział 8
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 11

1. Przydziału identyfikatora i hasła dokonuje IODO.
2. Użytkownik przy pierwszym dostępie do systemu informatycznego jest zobowiązany do zmiany hasła. Użytkownik zmienia hasło standardowo nie rzadziej niż co 30 dni oraz w każdym przepadku podejrzenia, że jego hasło mogło zostać upublicznione.
3. Hasło musi składać się z co najmniej 8 znaków, zawierać duże i małe litery, cyfry i co najmniej jeden znak specjalny.
4. Pin do karty mikroprocesorowej musi składać się z co najmniej 4 znaków.
5. Hasła są przechowywane w systemach bazodanowych w postaci zaszyfrowanej.
6. Piny są przechowywane na karcie mikroprocesorowej w postaci zaszyfrowanej.
7. Konto użytkownika jest blokowane w przypadku trzech nieudanych prób dostępu.
8. Pin użytkownika na karcie mikroprocesorowej jest blokowany w przypadku trzech nieudanych prób dostępu.
9. Karty mikroprocesorowe nie mogą być udostępniane innym osobom.
10. Hasło i pin nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób niepowołanych.

Rozdział 9
Procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz postępowania w przypadku zaniku napięcia dla użytkowników systemu informatycznego

§ 12

1. Przed rozpoczęciem pracy użytkownik zobowiązany jest do sprawdzenia stanu stacji komputerowej, w szczególności uszkodzeń lub ingerencji osób trzecich.
2. Rozpoczynając pracę na komputerze użytkownik wprowadza wszystkie wymagane identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.
3. W przypadku niemożliwości dostępu do systemu informatycznego z powodu zablokowania konta poprzez nieudane próby dostępu użytkownik powiadamia o tym fakcie IODO.
4. W przypadku dłuższej przerwy w korzystaniu z systemu informatycznego użytkownik obowiązany jest zawiesić pracę w systemie poprzez zaktywizowanie wygaszacza ekranu zabezpieczonego hasłem, wyrejestrować się z systemu informatycznego lub w inny sposób zablokować stację roboczą.
5. W przypadku braku aktywności użytkownika w systemie informatycznym trwającej dłużej niż 15 minut automatycznie włącza się wygaszacz ekranowy. Ponowny dostęp do systemu informatycznego następuje po poprawnym uwierzytelnieniu.
6. Po zakończeniu pracy użytkownik powinien, prawidłowo wylogować się z systemu informatycznego, wyłączyć komputer oraz UPS, wybrać kartę mikroprocesorową z czytnika.
7. W przypadku zaniku napięcia, które ma charakter trwały, użytkownik powinien:

a) jeśli otrzymał komunikat, o braku napięcia, wyłączeniu serwera po określonym czasie natychmiast zapisać dane, wylogować się z systemu informatycznego i bezpiecznie wyłączyć komputer,
b) jeśli nie otrzymał komunikatu lub nie korzysta z sieci LAN powinien zapisać dane i bezpiecznie wyłączyć komputer.

8. Ponowna praca jest możliwa po przywróceniu napięcia w sieci energetycznej.
9. W przypadku serii krótkich zaników napięcia (sygnalizowane dźwiękiem przez zasilacz awaryjny lub komunikatami na ekranie monitora) należy zakończyć pracę oraz powiadomić IODO o niestabilności sieci energetycznej oraz powiadomić Informatyka, który określi czy UPS jest sprawny.
10. Ustawienie monitora powinno uniemożliwiać podgląd osobom nieuprawnionym szczególnie w procesie obsługi klienta.
11. Wydruki po wykorzystaniu niszczy się w niszczarkach dokumentów.
12. Pomieszczenia w których są przetwarzane dane osobowe zamyka się na czas nieobecności osób zatrudnionych przy przetwarzaniu danych osobowych.

13. Osoby nieuprawnione mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe tylko w obecności osoby uprawnionej.
14. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

a) ujawniania danych osobowych,
b) kopiowania bazy danych lub jej części poza przewidzianymi kopiami bezpieczeństwa,
c) przetwarzania danych w sposób inny niż opisany instrukcją,
d) instalacji nielegalnego oprogramowania mogącego naruszyć bezpieczeństwo danych osobowych.

Rozdział 10
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 13

1. Kopie bezpieczeństwa wykonywane są w trybie dziennym.
2. Kopie bezpieczeństwa są sporządzane automatycznie przez specjalizowane urządzenia lub wykonuje je ASI.
3. Raz na kwartał są wykonywane przez ASI kopie zapasowe na nośnikach jednorazowego zapisu i prowadzona jest ewidencja wykonywania kopii zapasowych.
4. Wszystkie nośniki są opisane.
5. Tworzone są kopie bezpieczeństwa nowych i aktualizowanych programów oraz narzędzi programistycznych do przetwarzania zbiorów danych. Przechowuje się je w szafie pancernej.
6. Kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione, chyba że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
7. Wykorzystywanie nośników informacji lub wydruków w celu innym niż wskazany jest zabronione.

Rozdział 11
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych zbiorów danych

§ 14

1. Elektroniczne nośniki danych i kopie bezpieczeństwa na nośnikach zewnętrznych przechowuje się poza miejscem przetwarzania danych osobowych w zabezpieczonej szafie w zabezpieczonych opakowaniach chroniących przed kurzem i wilgocią.
2. Dostęp do nośników zawierających dane osobowe jest zabezpieczony poprzez:
   a) całodobowy monitoring,
   b) system alarmowy,
   c) szafę pancerną,
3. Kopie dzienne są przechowywane przez okres tygodnia
4. Kopie kwartalne są przechowywane przez okres 3 lat.
5. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy fizycznie w stopniu uniemożliwiającym ich odczytanie. Sporządza się protokół zniszczenia nośnika.
6. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać zarysować itp.).

Rozdział 12
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 15

1. Wszystkie stacje na których przetwarzane są dane osobowe posiadają wysoki poziom zabezpieczeń.
2. W celu ochrony dostępu do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej w systemie operacyjnym oraz sprzętowe rozwiązania np. Firewall lub urządzenia klasy UTM.

3. Na każdej stacji komputerowej na której przetwarzane są dane osobowe stosuje się aktywną ochronę antywirusową, działającą w czasie rzeczywistym.
4. Aktualizacja programu antywirusowego przeprowadzana jest codziennie, automatycznie bez udziału użytkownika.
5. Pełne sprawdzenie systemu operacyjnego odbywa się raz w tygodniu.
6. Wszystkie nośniki, których zawartość jest wczytywana do komputera muszą być każdorazowo sprawdzane programem antywirusowym. Odpowiedzialnym za te czynności jest pracownik obsługujący komputer.
7. Każdy użytkownik w przypadku stwierdzenia wystąpienia komunikatu ostrzegającego lub podejrzenia działalności wirusa komputerowego lub szkodliwego oprogramowania ma obowiązek zgłosić ten fakt IODO.
8. W przypadku naruszenia bezpieczeństwa danych użytkownik jest zobowiązany zgłosić ten fakt IODO.
9. Do obowiązków IODO należy okresowe sprawdzenie funkcjonowania i aktualność programu antywirusowego na wszystkich stacjach komputerowych przetwarzających dane osobowe.

Rozdział 13
Sposób realizacji wymogu odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione
§ 16

1. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
2. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym należy odnotować w systemie informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Rozdział 14
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych
§ 17

1. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane pod nadzorem ASI, bez możliwości dostępu do danych osobowych.
2. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych w sposób trwały lub naprawia się je pod nadzorem ASI.
3. Okresową weryfikację kopii bezpieczeństwa pod kontem ich przydatności do odtworzenia danych przeprowadza ASI.
4. Nośniki informacji przekazywane na zewnątrz są pozbawiane zapisów zawierających dane osobowe. Niszczenie zapisów odbywa się poprzez usunięcie danych w sposób uniemożliwiający ich odzyskanie.

Rozdział 15
Zasady postępowania z komputerami przenośnymi
§ 18

Komputery przenośne, używane do przetwarzania danych osobowych, zabezpiecza się podczas transportu oraz użytkowania przed dostępem do tych danych osób nieuprawnionych, w szczególności należy:

a) zabezpieczyć dostęp do komputera hasłem,
b) zabezpieczyć dostęp do systemu operacyjnego poprzez obligatoryjne wprowadzenie nazwy użytkownika i hasła,
c) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych,

d) nie przechowywać lokalnie zbiorów z danymi osobowymi - możliwa tylko praca zdalna w systemie przetwarzania danych osobowych.
e) wszelkie dane mające związek z danymi osobowymi przechowywać w plikach zabezpieczonych hasłem.

Rozdział 16
Przepisy końcowe
§ 19

1. Niniejsza instrukcja przeznaczona jest dla użytkowników systemu informatycznego i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.
2. Wykonanie postanowień instrukcji ma na celu ujednolicenie zarządzania systemem informatycznym w Ośrodku Sportu i Rekreacji w Suwałkach.
3. Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń AD.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym IODO.
6. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia IODO nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz.U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. **W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie stosowne przepisy wykonawcze.**

§ 20

Niniejsza instrukcja ma odpowiednie zastosowanie do podmiotów , które w oparciu o zawartą umowę wykonują w imieniu lub na rzecz OSiR czynności lub usługi, wymagające dostępu do danych osobowych AD.

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz

Załącznik Nr 1 do Instrukcji zarządzania systemem informatycznym ...
w Ośrodku Sportu i Rekreacji w Suwałkach

Suwałki, ... r.

Ośrodek Sportu i Rekreacji w Suwałkach
ul. Wojska Polskiego 2, 16-400 Suwałki

Pani/Pan*

.....

.....

UPOWAŻNIENIE NR .....
DO PRZETWARZANIA DANYCH OSOBOWYCH

I.

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dniem ..... r. udzielam polecenia i upoważniam Panią/ Pana*:

..... zatrudnioną/nego w Ośrodku Sportu i Rekreacji w Suwałkach
(imię i nazwisko)
do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku:

..... polegającego w szczególności na*):
(zajmowane stanowisko)

1. przeglądaniu, przechowywaniu, wykorzystywaniu,
2. pozyskiwaniu, dodawaniu, wpisywaniu,
3. modyfikacji, aktualizacji, zmianie,
4. usuwaniu, kasowaniu, niszczeniu,
5. udostępnianiu,
6. innym czynnościom ..... (wpisać)

II.

Upoważniam Panią/Pana*) do przetwarzania kategorii danych osobowych/zbiorów danych osobowych, w szczególności:

1. nazwisko i imię,
2. data urodzenia,
3. PESEL, numer dokumentu tożsamości,
4. NIP, REGON,
5. adres zamieszkania lub siedziby firmy,
6. telefon kontaktowy, adres e-mail,
7. inne: ..... (wpisać)

III.

Upoważnienie jest ważne do odwołania oraz wygasa z chwilą ustania Pani/Pana*) zatrudnienia w Ośrodku Sportu i Rekreacji w Suwałkach na podanym w p.I stanowisku.

IV.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w każdej formie, w tym tradycyjnej i elektronicznej lub innej prawnie dopuszczalnej.

V.

Obowiązek zachowania powyższych informacji w tajemnicy, w tym w szczególności danych osobowych powierzonych do przetwarzania, istnieje od chwili udzielenia niniejszego upoważnienia, przez okres zatrudnienia, jak również po ustaniu zatrudnienia.

VI.

1. Osoba upoważniona obowiązana jest przetwarzać dane osobowe przekazane Jej do przetwarzania w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administartora Danych - Ośrodka Sportu i Rekreacji w Suwałkach.
2. Osoba upoważniona zobowiazuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem, przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, przepisami obowiązującej na terenie RP ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Ośrodku Sportu i Rekreacji w Suwałkach wewnętrznymi regulacjami w sprawie ochrony danych osobowych.
3. Naruszenie obowiązków o których mowa w niniejszym upoważnieniu może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów obowiązującej na terenie RP ustawy o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

.....
data i podpis Upoważnionej/go

.....
data i podpis osoby upoważnionej
do reprezentowania Administratora (Dyrektor)

*) *niepotrzebne skreślić*

OŚWIADCZENIE

1. Oświadczam, że zapoznałam/łem się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Ośrodku Sportu i Rekreacji w Suwałkach. Przyjmuję do wiadomości obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.
2. Jestem świadoma/my obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposóbów ich zabezpieczenia, również po odwołaniu upoważnienia lub po ustaniu zatrudnienia.

.....
data i podpis Upoważnionej/go

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz

rozdzielnik: 4 egzemplarze w oryginale (dokumentacja kadrowa, IODO, kierownik komórki, osoba upoważniona).

Załącznik Nr 2 do Instrukcji zarządzania systemem informatycznym
w Ośrodku Sportu i Rekreacji w Suwałkach

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

w Ośrodku Sportu i Rekreacji w Suwałkach

L.p.	Data upoważnienia	Numer upoważnienia	Imię i nazwisko osoby upoważnionej	Stanowisko	komórka OSiR	zakres czynności	rodzaj danych	uwagi
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								

DYREKTOR
Ośrodka Sportu i Rekreacji w Suwałkach
mgr Waldemar Borysewicz