POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ SPORTOWYCH IM. SPORTOWCÓW ZIEMI SZCZECIŃSKIEJ W SZCZECINIE

Załącznik Nr 1 do Zarządzenia Nr 18
Dyrektora ZSS z dnia 02.11.2015 r.
zm.Zarządzeniem Nr 6 z 7.03.2017

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ SPORTOWYCH W SZCZECINIE

I. POSTANOWIENIA WSTĘPNE.

1. „Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w Zespole Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie, jest dokumentem zwanym dalej polityką bezpieczeństwa, który określa zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym ujawnieniem.

2. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

3. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zawiera:
1) identyfikację zasobów systemu tradycyjnego i informatycznego;
2) wykaz pomieszczeń, tworzący obszar, w którym przetwarzane są dane osobowe;
3) wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych;
4) opis struktury zbiorów danych i sposoby ich przepływu;
5) środki techniczne i organizacyjne, służące zapewnieniu poufności przetwarzanych danych.

4. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w Zespole Szkół Sportowych jak i innych, np. studentów, odbywających w nim praktyki pedagogiczne.

II. DEFINICJE.

1. Definicje

Ilekroć w instrukcji jest mowa o:

1) **administratorze danych osobowych** – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Zespole Szkół Sportowych funkcję administratora danych pełni dyrektor szkoły;
2) **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji (ABI);
3) **administratorze systemu** – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagane specjalnych uprawnień;
4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) **zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;
6) **przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych,

np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie;

7) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

9) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

10) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika szkoły, która upoważniona została do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;

11) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

12) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

13) **rozporządzeniu MSWiA** – rozumie się przez to 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.);

14) **serwisancie** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;

15) **sieci publicznej** – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

16) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

17) **szkole** – rozumie się przez to Zespół Szkół Sportowych w Szczecinie

18) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

19) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ~~(t.j. Dz. U. z 2014 r., poz. 1182. z późn. zm.~~); (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.); [1]

20) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

21) **użytkowniku** – rozumie się przez to pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło.

[1] Zarządzenie Nr 6 Dyrektora ZSS z dnia 7.03.2017 r.

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH.

1. Administrator danych osobowych.

Funkcję administratora danych osobowych sprawuje dyrektor szkoły. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,

2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,

3) wyznacza administratora bezpieczeństwa informacji oraz administratora sieci oraz określa zakres ich zadań i czynności,

4) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych, o ile jako właściwą do jej prowadzenia nie wskaże inną osobę,

5) zapewnia we współpracy z administratorem bezpieczeństwa informacji i systemu użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,

6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

2. Administrator bezpieczeństwa informacji.

Administrator bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem stosowanych środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych;

2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;

3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych;

4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;

5) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych;

6) zawiera wzory dokumentów (odpowiednie klauzule w dokumentach), dotyczących ochrony danych osobowych;

7) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych;

8) prowadzi oraz aktualizuje dokumentację, opisującą sposób przetwarzanych danych osobowych oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych;

9) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;

10) przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków

osób upoważnionych do przetwarzania danych osobowych;

11) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych;

12) w porozumieniu z administratorem danych osobowych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

Administrator bezpieczeństwa informacji ma prawo:

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji;
2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzanie niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

3. Administrator systemu.

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym są przetwarzane dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

3) na wniosek dyrektora szkoły przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;

6) wyrejestrowuje użytkowników na polecenie administratora danych;

7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych;

8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora bezpieczeństwa informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii

zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod katem ich dalszej przydatności do odtwarzania danych w przypadki awarii systemu informatycznego;

11) podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

Funkcję administratora systemu pełni pracownik firmy p. Grzegorz Rynkiewicz

4. Osoba upoważniona do przetwarzania danych.

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;

4) stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. IDENTYFIKACJA ZASOBÓW SYSTEMU INFORMATYCZNEGO.

1. Struktura informatyczna Zespołu Szkół Sportowych składa się z sieci wewnętrznej, mieszczącej się w pomieszczeniach szkoły i jest połączona siecią zbudowaną w oparciu o łącza dzierżawione w własne. Informacje przetwarzane w tej strukturze są jawne, ale podlegają ochronie zgodnie z przepisami ustawy.

2. W ramach tej struktury funkcjonuje oddzielnie system finansowy, za który odpowiada główny księgowy, oraz system zainstalowany w sekretariacie szkoły, które pracują oddzielnie.

2. Wszystkie aplikacje w których przetwarza się dane osobowe są on-linowe a ich archiwizacja odbywa się automatycznie na serwerach zewnętrznych firmy „PROGMAN”.

V. WYKAZ POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na

danych osobowych, takich , jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.

2. Dane osobowe przetwarzane są tylko i wyłącznie na terenie szkoły przy ul. Małopolskiej 22

3. Pomieszczenia w których przetwarzane są dane osobowe, nazwa, nr sali, kondygnacja, inne informacje.

a) sekretariat szkoły, I piętro, sala nr 107
b) pokój nauczycielski I piętro, sala 114
c) gabinet Dyrektora Szkoły, I piętro 107
d) gabinet wicedyrektora szkoły ds. sportowych, I piętro, sala nr 106
e) gabinet wicedyrektorów szkoły ds. dydaktycznych i wychowawczych, I piętro, sala nr 105
f) pomieszczenie pracowników księgowości – główna księgowa, parter, sala nr 12
g) pomieszczenie pracowników księgowości – starsza księgowa-kasjer, parter, sala nr 12
h) pomieszczenie kierownika administracyjno-gospodarczego, parter, sala nr 20
i) pomieszczenie na serwer szkoły i serwer archiwizujący, wysoki parter, sala nr 013
j) gabinet pielęgniarki szkolnej, partner, sala nr 5
k) gabinet pedagoga szkolnego, parter, sala nr 8

VI. WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW STOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Rejestr zbioru danych

L.p.	Nazwa zbioru (kadrowy, płacowy, itp.)	Nazwa programu (programów) informatycznego stosowanego do przetwarzania danych osobowych
1.	Akta osobowe pracowników	Progman – Kadry-rejestr elektroniczny
2.	Listy płac pracowników	Progman – Płace-rejestr elektroniczny
3.	Ewidencja umów – zleceń	Progman – Zlecone-rejestr elektroniczny
4.	Ewidencja przelewów bankowych	Progman – Przelewy-rejestr elektroniczny
5.	Ewidencja osób korzystających z ZFŚS	Progman – ZFŚŚ-rejestr elektroniczny
6.	Ewidencja zadań gospodarczych szkoły	Progman – Finanse-rejestr elektroniczny
7.	Ewidencja wpływów i wypływów gotówkowych	Progman – Kasa-rejestr elektroniczny
8.	Ewidencja uczniów	Progman - Sekretariat-rejestr elektroniczny
9.	Arkusz organizacyjny szkoły	Progman – iArkusz-rejestr elektroniczny
10.	Organizacja obligatoryjnych zajęć szkolnych	Librus – Plan lekcji-rejestr elektroniczny
11.	Ewidencja danych przekazywanych do ZUS	Płatnik – rejestr elektroniczny
12.	Ewidencja deklaracji	PFRON – rejestr elektroniczny
13.	Ewidencja danych statystycznych	GUS – rejestr elektroniczny
14.	Ewidencja danych osobowych kandydatów do szkoły	Progman - Nabór-rejestr elektroniczny
15.	Dzienniki lekcyjne	Progman - IDziennik
16.	Ewidencja członków pracowniczej kasy zapomogowo-pożyczkowej	Progman – Kasa Zapomogowo-Pożyczkowa
17.	System Informacji Oświatowej	SIO- rejestr elektroniczny

18.	Okręgowa Komisja Egzaminacyjna	OKE – rejestr elektroniczny
18a.[2]	Rejestr korespondencji przychodzącej i wychodzącej	MDB Sekretariat – rejestr elektroniczny
18b.[3]	Monitoring wizyjny	CCTV-VIVOTEK
19.	**Nazwa zbioru (ewidencja, wykaz, rejestr, itp.) w formie papierowej**	**Miejsce przechowywania zbioru**
20.	Księgi druków ścisłego zarachowania : legitymacje szkolne,duplikaty legitymacji szkolnych, świadectwa szkolne, duplikaty świadectw, indeksy Gimnazjum dla Dorosłych, karty rowerowe, legitymacje służbowe nauczycieli	Sekretariat szkoły pok. 107
21.	Księga druków ścisłego zarachowania - czeki	Księgowość pok. 12,
22.	Akta osobowe pracowników administracji i obsługi	Księgowość pok. 12,
23.	Akta osobowe nauczycieli	Sekretariat szkoły pok. 107
24.	Lista wypłat	Księgowość pok. 12,
25.	Rejestr nieobecności w pracy	Sekretariat szkoły pok. 107, Wicedyrektor pok. 105
26.	Księga zastępstw nauczycieli	Wicedyrektor szkoły pok. 105
27.	Księga protokołów Rady Pedagogicznej	Wicedyrektor szkoły pok. 106
28.	Rejestr wydanych zaświadczeń	Sekretariat szkoły pok. 107
29.	Ewidencja urlopów pracowników niepedagogicznych	Księgowość pok. 12,
30.	Rejestr delegacji służbowych	Sekretariat szkoły pok. 107
31.	Ewidencja osób zatrudnionych do przetwarzania danych osobowych	Sekretariat szkoły pok. 107
32.	Księga uczniów	Sekretariat szkoły pok. 107
33.	Księga absolwenta	Sekretariat szkoły pok. 107
34.	Dzienniki: nauczanie indywidualne,wychowawców, zajęć pozalekcyjnych, zajęć z art. nr 42 KN, świetlicy, lekcyjne nauczycieli wychowania fizycznego	Pokój nauczycielski pok. 114
35.	Zbiór arkuszy ocen uczniów	Wicedyrektor szkoły pok. 106
36.	Rejestr opinii psychologiczno-pedagogicznych uczniów	Sekretariat szkoły pok. 107, Pedagog szkolny pok. 8
37.	Rejestr wniosków i decyzji o przyznaniu nauczycielom pomocy zdrowotnej	Sekretariat szkoły pok. 107
38.	Rejestr wydawnych aktów nadania stopnia awansu zawodowego nauczycieli	Sekretariat szkoły pok. 107
39.	Protokół przekazania darowizny	Sekretariat szkoły pok. 107
40.	Rejestr zwolnień z zajęć z wychowania fizycznego	Sekretariat szkoły pok. 107
41.	Rejestr wypadków uczniów	Wicedyrektor szkoły pok. 105
42.	Rejestr wypadków przy pracy	Księgowość pok. 12
43.	Rejestr wypadków w drodze do lub z pracy	Księgowość pok. 12
44.	Rejestr chorób zawodowych	Księgowość pok. 12
45.	Akta postępowań powypadkowych	Księgowość pok. 12
46.	Rejestr upoważnień	Sekretariat szkoły pok. 107
47.	Składnica	Pokój 311
48.	Karta rozliczeń godzin ponadwymiarowych i zastępstw	Wicedyrektor szkoły pok. 105

49.	Rejestr nieobecności nauczycieli	Sekretariat szkoły pok. 107, Wicedyrektor szkoły pok. 105
50.	Rejestr zarządzeń Dyrektora Szkoły	Sekretariat szkoły pok. 107
51.	Zbiór kartotek PKZP	Księgowość pok. 12
52.	Ewidencja dzieci z obwodu Gimnazjum nr 11	Sekretariat szkoły pok. 107
53.	Dokumentacja związana z organizacją obozów i zawodów sportowych, organizacją badań lekarskich uczniów klas sportowych,zgłoszeniami zawodników do Polskich Związków Sportowych	Wicedyrektor szkoły pok. 105
54.	Karty zdrowia uczniów	Pielęgniarka szkolna pok. 5

VII. STRUKTURA ZBIORÓW DANYCH, SPOSÓB PRZEPŁYWU DANYCH I ZAKRES ICH PRZETWARZANIA.

1. Zbiór danych „Kandydaci do szkoły".

Zbiór ten obejmuje dane osobowe kandydatów szkół, ubiegających się o przyjęcie do szkoły.

1) Zakres pierwszych danych tego zbioru, tzn. imię (imiona) i nazwisko kandydata, data i miejsce urodzenia, PESEL, adres zamieszkania, numer gimnazjum, do którego uczęszcza, imię i nazwisko rodziców (prawnych opiekunów) , ich adres zamieszkania , numer telefonu, dostępny jest członkom szkolnej komisji rekrutacyjno-kwalifikacyjnej, dyrektorowi szkoły i jego zastępcy oraz sekretarce, która wspiera komisję w pracach związanych z naborem kandydatów – przygotowaniem list przyjętych i ich uaktualnieniem oraz zbieraniem dokumentacji od kandydatów.

Dane osobowe kandydatów i ich rodziców znane są członkom komisji rekrutacyjno-kwalifikacyjnej i pozostałym osobom, uczestniczącym w procedurze naboru, w dniu ogłoszenia wyników naboru.

Wykazy kandydatów, przyjętych do szkoły, są upubliczniane wraz z ich danymi: imionami i nazwiskami oraz punktacją na tablicy informacyjnej w dniu ogłoszenia wyników.

Dane tego zakresu przetwarzane są za pomocą programu „Progman – Nabór", który wprowadził do użytku organ prowadzący szkołę. Dostęp do niego ma sekretarka. Mogą być udostępniane zarówno organowi prowadzącemu szkołę (Wydziałowi Oświaty Urzędu Miasta Szczecin), jak i organowi nadzorującemu szkołę, (Zachodniopomorskiemu Kuratorowi Oświaty) w celu opracowywania raportów o wynikach naboru kandydatów do szkół ponadgimnazjalnych, do gimnazjum i szkoły podstawowej

2) Zakresu drugi danych tego zbioru obejmuje wizerunek kandydatów przyjętych do szkoły i ich rodziców, którzy w dniu ogłoszenia wyników naboru i kilku następnych dniach, tj.: do dnia ostatecznego zamknięcia list przyjętych, pojawiają się w szkole. Ich wizerunek rejestruje program CCTV- monitoring wizyjny, do którego dostęp ma dyrektor szkoły. Może być udostępniony policji i straży miejskiej w sytuacji zaistnienia wydarzenia, będącego przedmiotem prowadzonego postępowania.

[2,3] Zarządzenie Nr 6 Dyrektora ZSS z dnia 07.03.2017 r

2. Zbiór danych „Uczniowie szkoły”.

Zbiór ten obejmuje dane osobowe uczniów i ich rodziców: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, PESEL oraz imiona i nazwisko rodziców (prawnych opiekunów), adres zamieszkania, numer telefonu domowego lub do pracy.

1) Zakres pierwszy danych tego zbioru: numer ewidencyjny ucznia, imię (imiona) i nazwisko, data i miejsce urodzenia, adres zamieszkania oraz imiona i nazwiska rodziców (prawnych opiekunów) ucznia – obejmuje „Księgę uczniów szkoły” i jest dostępny wychowawcom klasowym, dyrektorowi i jego zastępcy oraz sekretarce. Dane tego zakresu są udostępniane organowi prowadzącemu szkołę i organowi nadzorującemu szkołę w celu przeprowadzenia kontroli. Dane tego zakresu mogą być udostępnione pracownikom NIK, GIODO, MEN na podstawie pisemnych upoważnień do przeprowadzenia kontroli, a także policji i straży miejskiej w sytuacji popełnienia przez ucznia wykroczenia przeciw prawu.

2) Zakres drugi danych tego zbioru: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres ich zamieszkania odnosi się do arkuszy ocen ucznia. Dane w nich zawarte przetwarzają wychowawcy klas, a dostęp do nich mają również dyrektor szkoły i jego zastępca oraz sekretarka, która po zakończonym cyklu kształcenia gromadzi je w specjalnych teczkach i przechowuje w archiwum szkolnym.

Dane z zakresu trzeciego mogą być udostępniane tylko przedstawicielom organu prowadzącemu i nadzorującego szkołę w celach kontrolnych.

3) Zakres trzeci danych osobowych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres zamieszkania i numery telefonów do domu lub do pracy obejmuje dzienniki lekcyjne i jest dostępny wszystkim nauczycielom zatrudnionym w szkole oraz praktykantom, odbywającym w niej praktyki pedagogiczne. Dane te są przechowywane w aplikacji IDziennik. Dane osobowe z tego zakresu mogą być udostępnione jedynie przedstawicielom organu prowadzącego szkołę oraz organu nadzorującego w czasie wizytacji lub w sytuacjach interwencyjnych, a także NIK i MEN w celu przeprowadzenia odpowiednich kontroli.

4) Zakres czwarty danych zbioru „Uczniowie szkoły”: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, PESEL, informacje o przebytych chorobach, wzroście, wadze, ostrości wzroku itp., a także imiona i nazwisko rodziców (prawnych opiekunów) i ich adres zamieszkania – odnosi się do dokumentacji medycznej ucznia, na którą składają się karta zdrowia ucznia, karta bilansu zdrowia 18-latka oraz wykazy ewidencyjne uczniów.

Dane z tego zakresu są przetwarzane w sposób tradycyjny przez pielęgniarkę szkolną, a dostęp do nich ma oprócz niej mają lekarz, prowadzący badania uczniów, oraz dyrektor szkoły. Wykazy ewidencyjne uczniów, w których są podane ich imiona, nazwiska oraz PESEL są przekazywane do NFZ, natomiast pozostałą dokumentację wydaje się uczniowi po zakończeniu nauki.

Dane z tego zakresu mogą być udostępnione NFZ, NIK, MZiOS na podstawie pisemnego upoważnienia w celu przeprowadzenia kontroli.

5) Zakres piaty danych tego zbioru obejmuje dane uczniów (w tym dane wrażliwe), tj. imiona i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, a także ostatnie dane o stanie zdrowia (w tym również zdrowia psychicznego), przedstawione w zaświadczeniach i opiniach, poradni psychologiczno-pedagogicznej, która wnioskuje do dyrektora szkoły o nauczanie indywidualne, indywidualny tok nauki, obniżenie progu wymagań albo

dostosowanie warunków egzaminu maturalnego/ gimnazjalnego/ sprawdzianu do formy niepełnosprawności ucznia.

Dostęp do tych danych, które są przetwarzane wyłącznie ręcznie, mają wyłącznie dyrektor szkoły, jego zastępcy, wybrani nauczyciele i pedagog szkolny. Mogą być udostępnione organom, prowadzącym kontrolę, w tym zwłaszcza Kuratorium Oświaty Okręgowej Komisji Egzaminacyjnej w Poznaniu.

6) Zakres szósty danych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, PESEL, adres zamieszkania, numer telefonu oraz imiona i nazwisko rodziców, dostępny jest dyrektorowi szkoły, jego zastępcą i sekretarce.

Dane te przedstawione są w wersji papierowej w postaci deklaracji maturalnej, składanej przez ucznia, które następnie wprowadzane i wysyłane są do systemu Okręgowej Komisji Egzaminacyjnej w Poznaniu w celu przetwarzania ich dla potrzeb egzaminu maturalnego, gimnazjalnego i sprawdzianu Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła użytkownika, nadanych przez OKE w Poznaniu.

7) Zakres siódmy danych tego zbioru dotyczy wizerunku ucznia, który rejestrują kamery, działające w programie CCTV. Dostęp do tych danych ma bezpośrednioi dyrektor szkoły, a także policja i służba miejska, ale tylko wtedy, jeśli prowadzi postępowanie.

3. Zbiór danych „Pracownicy szkoły".

Zbiór ten obejmuje dane osobowe byłych i obecnych pracowników szkoły, tj.: nauczycieli, pracowników administracji i obsługi. Dane te przetwarzane są zarówno ręcznie, jak i w systemie informatycznym.

1) zakres pierwszy danych tego zbioru, tzn. imię i nazwisko nauczyciela oraz ich numery telefonów, dostępne są prawie wszystkim pracownikom szkoły, a także uczniom i ich rodzicom, jeżeli nauczyciele wyrażą na to zgodę.

2) Zakres drugi tego zbioru, tzn. imię i nazwisko pracownika szkoły, data i miejsce urodzenia imiona i nazwisko rodziców, adres zamieszkania, wysokość wynagrodzenia, dane dotyczące wynagrodzenia, kwalifikacji zawodowych, wynagrodzenia, przeszeregowań, urlopów i zwolnień lekarskich, numer dowodu osobistego, numer NIP i PESEL, a także dane wrażliwe – informacje o odbytych szkoleniach, o posiadanych dzieciach, zawartym związku małżeńskim, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych na podstawie przeprowadzonych badań profilaktycznych (wstępnych, okresowych i kontrolnych) oraz w związku z ubieganiem się nauczyciela o przyznanie urlopu dla podratowania zdrowia. Dane te zamieszczone są w dokumentach teczek akt osobowych pracownika, a dostęp do nich mają:

- dyrektor szkoły,
- sekretarka, prowadząca sprawy kadrowe nauczycieli,
- pracownik księgowości prowadzący sprawy kadrowe pracowników administracji i obsługi.

Dane z zakresu drugiego mogą być udostępniane organowi prowadzącemu szkołę i organowi nadzorującemu szkołę, a także innym organom prowadzącym kontrolę, w tym zwłaszcza PIP, RIO i sądom powszechnym w związku z prowadzonym postępowaniem.

W systemie informatycznym funkcjonującym w szkole,dane zbioru „Pracownicy szkoły" są przetwarzane tylko w drugim zakresie. Na polecenie dyrektora szkoły pracownicy, zajmujący się sprawami kadrowymi, przygotowują w programie „Edytor tekstu „MS WORD" umowy o pracę, porozumienia, przeszeregowania, wypowiedzenia, w tym wypowiedzenia zmieniające, informacje o warunkach zatrudnienia, zakresy obowiązków, korespondencję w sprawie zatrudnienia i wysokości zarobków lub rozwiązania stosunku pracy i świadectwa pracy. Dane te są niezwłocznie wprowadzane do bazy danych komputera , na którym

pracują te osoby. Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła pracownika, zajmującego się sprawami kadrowymi.

Z teczek akt osobowych pracowników szkoły dane są przekazywane przez osoby zajmujące się sprawami kadrowymi w sposób tradycyjny do programów SIO – system informacji oświatowej i Arkusza Progman – arkusza organizacyjnego i uaktualniane dwa razy do roku -31 marca i 30 września. Wprowadzanie danych do SIO jest możliwe po wprowadzeniu identyfikatora i hasła.

Dostęp do tych danych mają organ prowadzący i nadzorujący szkołę, w przypadku SIO do danych osobowych ma dostęp również MEN.

4. Zbiór danych „Księgowość-finanse szkoły".

Zakres danych tego zbioru, tzn. imię i nazwisko pracownika szkoły, jego adres zamieszkania, data i miejsce urodzenia, imiona i nazwiska rodziców, dane, dotyczące wykształcenia i stopnia awansu zawodowego, stażu pracy, wynagrodzenia, urlopów i zwolnień lekarskich, numeru dowodu osobistego, numeru konta bankowego, numer PESEL i NIP, dostępny jest tylko dyrektorowi szkoły i pracownikom księgowości.

Dane tego zakresu są udostępniane przez głównego księgowego ZUS-owi, urzędom skarbowym, a także firmom ubezpieczeniowym AVIVA Towarzystwo Ubezpieczeń na Życie S.A.; PZU S.A. w zakresie wymaganym przez nie w tradycyjnym systemie przetwarzania danych.

Dane tego zbioru są też przetwarzane za pomocą programu „Progman Finanse DDJ", z którego niektóre z nich są importowane półautomatycznie do programu „Płatnik", który służy do korespondencji z ZUS-em. Kontakt z ZUS-em odbywa się za pomocą poczty elektronicznej i jest uwierzytelniany co roku zmienianymi certyfikatem dostępu z przypisanym mu hasłem.

Na tym samym komputerze przetwarzane są dane: imię i nazwisko pracownika, staż pracy, a także informacje dotyczące wynagrodzenia, w tym wynagrodzenia zasadniczego, dodatku stażowego i dodatku motywacyjnego oraz kwot odciąganych na poczet podatku od osób fizycznych, składek na ZUS, fundusz zdrowotny i związki zawodowe, a także kwot spłaty z tytułu pożyczek w programie płacowym Progman Płace.

Na tym samym komputerze są przetwarzane również dane: imię i nazwisko pracownika, adres, numer rachunku bankowego, w systemie bankowości elektronicznej za pomocą programu „Przeglądarka" i aplikacji „iPKO Biznes", dostępnej po połączeniu z siecią internet (on-line), w którym tworzy się przelewy wynagrodzeń. Każdorazowy przelew opatrzony jest bezpiecznym podpisem elektronicznym, składanym przez dyrektora szkoły lub jego zastępcę oraz głównego księgowego.

5) Ze względu na fakt, że system informatyczny szkoły połączony jest z siecią publiczną poprzez internet, zgodnie z §6. ust. 4. rozporządzenia MSWiA należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

VIII. ŚRODKI TECHNICZNE I ORGANIZACYJNE, SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI PRZETWARZANYCH DANYCH.

1. Bezpieczeństwo osobowe.

Zachowanie poufności.

1. Dyrektor szkoły danych przeprowadza nabór na wolne stanowiska w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych przetwarzanych w szkole, pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest

minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia szkolne), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

4. Ryzyko ze strony osób, które dokonują bieżących napraw komputera, minimalizowane jest obecnością użytkownika systemu.

Szkolenia w zakresie ochrony danych osobowych.

1. Administrator bezpieczeństwa informacji uwzględnia następujący plan szkoleń:
   a) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
   b) Szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
   c) Przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
2. Tematyka szkoleń obejmuje:
   a) Przepisy i procedury, dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   b) Sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
   c) Obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
   d) Odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
   e) Zasady i procedury określone w polityce bezpieczeństwa.

2. Strefy bezpieczeństwa.

W szkole wydzielono dwie strefy bezpieczeństwa. Do strefy I wchodzą:

1) gabinet księgowej, w którym może przebywać główny księgowy i starszy księgowy; inni użytkownicy danych (sekretarka, kierownik gospodarczy, intendent i nauczyciele) tylko w towarzystwie głównej księgowej lub starszej księgowej, a osoby postronne w ogóle nie mają dostępu.

2) sekretariat z kasą pancerną, gabinet dyrektora szkoły oraz pokój kierownika gospodarczego, w których mogą przebywać inni użytkownicy danych tylko w obecności; to samo dotyczy uczniów, ich rodziców oraz interesantów; nikt z osób postronnych nie może przebywać w części sekretariatu, odgrodzonej barierką; kluczem do gabinetu dyrektora i sekretariatu może dysponować na stałe dyrektor i pracownicy sekretariatu.

W strefie II do danych osobowych mają dostęp wszystkie osoby upoważnione do ich przetwarzania, a osoby postronne (uczniowie, ich rodzice i praktykanci) tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje pokój nauczycielski, pokój zastępcy dyrektora, gabinet medyczny i pokój pedagoga szkolnego.

3. Zabezpieczenie sprzętu.

1. Strategiczne urządzenia systemu informacyjnego w szkole powinny być zasilane za pośrednictwem zasilaczy awaryjnych (UPS) (sekretariat szkoły i główny księgowy).

2. W celu zapewnienia większego bezpieczeństwa i ochrony danych powinno wykorzystać się system operacyjny Microsoft Windows XP i młodsze wersje, posiadające rozbudowane mechanizmy nadawania uprawnień i praw dostępu. Dla pełnego wykorzystania mechanizmów należy stosować system plików NTFS, który zapewnia wsparcie mechanizmu ochrony plików i katalogów oraz mechanizmów odzyskiwania na wypadek uszkodzenia dysku lub awarii komputerów.

3.Administrator bezpieczeństwa informatycznego przy udziale administratora sieci informatycznej jest jedyną osoba uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustalonych i statutowych zadań szkoły i posiadających ważną licencję użytkownika.

4. Bieżąca konserwacja sprzętu wykorzystywanego w szkole do przetwarzania danych prowadzona jest przez jej pracowników, przede wszystkim przez administratora sieci.

5. Poważne naprawy wykonywane przez pracowników firm zewnętrznych realizowane są w budynku szkoły po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszanie bezpieczeństwa danych.

6. Dopuszcza się konserwowanie i naprawę sprzętu poza szkołą jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych, można zbyć dopiero po usunięciu danych osobowych, a urządzenia uszkodzone mogą być przekazywane do utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony szkoły) właściwym podmiotom, z którymi także zawiera się umowy powierzania przetwarzanych danych.

7. Wszystkie awarie i konserwacje systemu informatycznego mogące prowadzić do wycieku danych osobowychsą opisywane są w stosownych protokołach, które podpisują osoby uczestniczące w naprawie lub konserwacji.

4. Zabezpieczenia we własnym zakresie.

W celu podniesienia bezpieczeństwa danych każda osoba upoważniona do przetwarzania danych lub użytkownik systemu informatycznego zobowiązani są do:

1) ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
2) niepozostawienia bez kontroli dokumentów i nośników danych w klasach i innych miejscach publicznych oraz w samochodach;
3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
4) niepodłączania do listew, podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
5) pilnego strzeżenia akt;
6) kasowania po wykorzystaniu danych na dyskach przenośnych;
7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
16) kończenia pracy stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy;
18) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
19) zachowania tajemnicy danych, w tym także wobec najbliższych;
20) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
21) umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
22) zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
23) zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

5. Wykorzystywanie akt i dokumentów szkolnych do pracy w domu.

1. Wykorzystywanie akt i dokumentów, zawierających dane osobowe (arkusze ocen i inne), do pracy w domu jest możliwe tylko po uzyskaniu upoważnienia na piśmie, udzielanego przez dyrektora szkoły lub jego zastępcę.
2. Administrator bezpieczeństwa informatycznego lub upoważniona przez niego osoba prowadzi ewidencję akt spraw i dokumentów szkolnych, wynoszonych przez uprawnionych pracowników.
3. Niedopuszczalne jest pozostawienie akt lub dokumentów bez dozoru w czasie ich przenoszenia do domu np. w samochodzie.
4. Z wynoszonych dokumentów może korzystać wyłącznie upoważniony pracownik, który powinien dołożyć wszelkich starań, aby osoby postronne, w tym domownicy, nie mogły mieć do nich dostępu. Dokumenty przechowywane w domu, w czasie, w którym nie są

konieczne do wykonywania pracy, powinny być zamykane w sposób uniemożliwiający dostęp osób innych niż upoważniony pracownik.

5. Upoważniony pracownik po zakończeniu wykonywania pracy w domu powinien niezwłocznie zwrócić dokumenty dyrektorowi szkoły lub jego zastępcy.
6. Pracownicy, wynoszący dokumenty i akta spraw do domu, są obowiązani do ochrony danych w nich zawartych i w razie ich udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym podlegają grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 zgodnie z art. 51 ustawy.

6. Postępowanie z nośnikami danych i ich bezpieczeństwo.

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

7. Wymiana danych i ich bezpieczeństwo.

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w pkt. 9. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora bezpieczeństwa informacji oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

3. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami” na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

4. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa informacji oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

5. Administrator bezpieczeństwa informacji dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojan, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu

informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

6. Należy stosować następujące sposoby kryptograficznej ochrony danych:

- przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – tunelowanie, szyfrowanie połączenia,

- przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.

8. Kontrola dostępu do systemu.

1. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator bezpieczeństwa informacji po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek dyrektora szkoły, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. Następnie użytkownik jest zobowiązany do zmiany hasła przy pierwszym logowaniu.

2. Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora bezpieczeństwa informacji po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia, zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł.

3. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji i pracowników działu informatyki.

9. Kontrola dostępu do sieci.

1. System informatyczny posiada szerokopasmowe połączenie z Internetem.

2. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

3. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie główny księgowy i wyznaczony przez dyrektora szkoły starszy księgowy z jednej strony i dyrektor szkoły oraz wyznaczony przez dyrektora szkoły jego zastępca po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

10. Komputery przenośne i praca na odległość.

W szkole używa się komputerów przenośnych (komputer dyrektora szkoły i jego zastępców) do przetwarzania danych osobowych, które uruchamia się po wprowadzeniu hasła.

11. Monitorowanie dostępu do systemu i jego użycia.

1. Odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest administrator bezpieczeństwa informacji lub upoważniona przez niego osoba, a administrator danych osobowych kontroluje jego przebieg i rezultaty.

2. System informatyczny, działający w szkole, powinien zapewnić odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,

3) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,

4) informacji o odbiorcach w rozumieniu art. 7. pkt 6. ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,

5) sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. 1. pkt. 8. ustawy.

Odnotowanie informacji, o których mowa w pkt. 1. i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt. 1-5.

3. System informatyczny administratora danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:

1) Identyfikator użytkownika,

2) Datę i czas zalogowania i wylogowania się z systemu,

3) Tożsamość stacji roboczej,

4) Zapisy udanych i nieudanych prób dostępu do systemu,

5) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych

12. Przeglądy okresowe, zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy).

1.Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza osoby przetwarzające dane osobowe, są obowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

1. Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.

3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i administratora danych, w której usunięto dane osobowe.

13. Udostępnianie danych osobowych.

1. Udostępnianie danych osobowych policji, służbie miejskiej i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem .
2. Udostępnianie informacji policji odbywa się według następującej procedury:

1) udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:

- oznaczenie wnioskodawcy,

- wskazanie przepisów uprawniających do dostępu do informacji,

- określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub

Udostępnienia,

- wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

2) udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

3) osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.

4), jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

5), jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępniania informacji.

3. Innym podmiotom dane osobowe, dotyczące pracowników i uczniów szkoły, nie mogą być udostępniane.

14. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
Niezależnie od rozwiązania stosunku pracy osoby, popełniające przestępstwo, będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51 i 52. ustawy oraz art. 266. Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1) Stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo

Osobie nieupoważnionej,

2) Niezabezpieczenia nośnika lub komputera przenośnego,

3) Zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych

Operacji w systemie informatycznym administratora danych.

XI. Przeglądy polityki bezpieczeństwa i audyty systemu.

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) Zmian w budowie systemu informatycznego,
2) Zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3) Zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji po uzgodnieniu z dyrektorem szkoły może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i dyrektora.

Dyrektor szkoły, biorąc pod uwagę wnioski administratora bezpieczeństwa informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

X. POSTANOWIENIA KOŃCOWE.

1. Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązania jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur ochrony danych jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi włącznie z rozwiązaniem stosunku pracy na podstawie art. 52. Kodeksu pracy.

3. Polityka bezpieczeństwa, wchodzi w życie z dniem 2 listopada 2015 roku.

4. Traci moc polityka bezpieczeństwa stanowiąca załącznik Nr 1 do Zarządzenia Nr 7 Dyrektora Zezpołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie z dnia 01.09.2011 r

ZAŁĄCZNIKI :

Załącznik Nr 1. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Zespole Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie – forma elektroniczna.

Załącznik Nr 2. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Zespole Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie – rejestr papierowy.

Załącznik Nr 3. Wzór oświadczenia

Załącznik Nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik Nr 5. Wzór Odwołania upoważnienia

Załącznik Nr 6. Wzór druku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych

Załącznik Nr 7. Wzór sprawozdania ze sprawdzenia zgodności przetwarzanych danych osobowych z przepisami o ochronie danych osobowych nr ...../20 .....

Dyrektor
(-) mgr Jarosław Duda

Zmiany do Zarządzenia Nr 18 z dnia 02.11.2015 r. zostały wprowadzone Zarządzeniem Nr 6 Dyrektora ZSS z dnia 7.03.2017

Załącznik Nr 3 do Polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZSS wprowadz. Zarz.Nr 6 Dyrektora ZSS z 7.03.2017 r.

.....
(imię i nazwisko pracownika)

.....
(stanowisko służbowe)

OŚWIADCZENIE

Oświadczam, że zapoznałam(-em) się z przepisami *ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych* (tekst jedn.: tekst jedn. : Dz . U. z 2016 r., poz. 922 ze zm.) oraz Polityką bezpieczeństwa i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i zobowiązuję się do ich przestrzegania w trakcie pracy w

Zespół Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie
.....
(*nazwa szkoły)*

oraz zachowania w tajemnicy wszystkich danych osobowych, do których miałam(em) dostęp w związku z zatrudnieniem – także po ustaniu stosunku zatrudnienia.

Zespół Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie
.....
(nazwa szkoły)

.....
(data i podpis pracownika)

Załącznik Nr 4 do Polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZSS wprowadz.Zarz.Nr 6 Dyrektora ZSS z 7.03.2017

Szczecin,……

UPOWAŻNIENIE NR ……../20

Działając zgodnie z art. 37 *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (tekst jedn. : Dz . U. z 2016 r., poz. 922 ze zm.)

Upoważniam Pana/Panią……
(imię i nazwisko)

do przetworzenia danych osobowych w ……
(nazwa jednostki)

w zakresie
……
……
……
……
……
(wymienić ew. czynności oraz zawartość zbioru)

Równocześnie zobowiązuję Pana/Panią do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia.

Informuję, że udostępnienie danych osobowych lub umożliwienie dostępu do nich osobie nieupoważnionej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art.51 ustawy o ochronie danych osobowych).

Upoważnienie jest ważne od dnia …… r do …….. r.

…….. ……
(data i podpis upoważnionego) (podpis administratora danych)

Załącznik Nr 5 do Polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZSS
wprowadz. Zarz.Nr 6 Dyrektora ZSS z 07.03.2017

Szczecinie, dnia ..... r.

.....
(pieczęć Szkoły)

ODWOŁANIE UPOWAŻNIENIA Nr …
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. : Dz . U. z 2016 r., poz. 922 ze zm.)

odwołuję z dniem …….. upoważnienie do przetwarzania danych

osobowych wystawione dla Pani/Pana …….

Administrator Danych Osobowych

……
(pieczątka i podpis)

Załącznik Nr 6 do Polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZSS

WZÓR DRUKU EWIDENCJI OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Ewidencja osób zatrudnionych w Zespole Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie przy przetwarzaniu danych osobowych :

Lp.	Imię i nazwisko	Stanowisko	Nr upoważnienia	Indentyfikator	Data nadania upoważnienia	Data ustania upoważnienia

Załącznik Nr 7 do Polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZSS
wprowadz. Zarz.Nr 6 Dyrektora ZSS z 07.03.2017

Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

nr …/20…

Sprawozdanie sporządzone zgodnie z art. 36c *Ustawy o ochronie danych osobowych* (t.j. Dz.U. z 2016 r. poz. 922 ze zm.).

Data rozpoczęcia sprawdzenia: dd/mm/rrrr

Data zakończenia sprawdzenia: dd/mm/rrrr

Tryb: sprawdzenie planowe / doraźne / dla GIODO

(niepotrzebne skreślić)

1. Administrator danych

……...

……...

(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania oraz REGON)

2. Administrator bezpieczeństwa informacji

……

(imię, nazwisko)

3. Wykaz czynności podjętych w toku sprawdzenia, w tym imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach

……

……

4. **Przedmiot i zakres sprawdzenia**

……

……..……...

5. **Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych**

……

……

6. **Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem**

Naruszenie	**Podjęte / planowane działania**

7. **Załączniki**

…….

(data, miejsce, podpis ABI)

Uwaga! W przypadku wersji papierowej, na każdej stronie parafa ABI.

Załącznik Nr 2 Do zarządzenia Nr 18
Dyrektora ZSS z dnia 02.11.2015
zm. Zarządzeniem Nr 6 z 07.03.2017 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ SPORTOWYCH W SZCZECINIE

I. CELE WPROWADZENIA I ZAKRES ZASTOSOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.

1. „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Zespole Szkół Sportowych, zwana dalej instrukcją, została wprowadzona w celu spełnienia wymagań, o których jest mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (~~t.j. Dz. U. 2014 r., poz. 1182. z późn. zm.~~) (t.j. Dz.U. z 2016 r. poz.922 z późn.zm.) [4] oraz 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. 2004 r., nr 100, poz. 1024), tj. zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem".

2. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Zespole Szkół Sportowych i wraz z nim składa się na dokumentację wymaganą przez art. 36. ust. 2. ustawy o ochronie danych osobowych.

3. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w szkole, w których są przetwarzane dane osobowe.

4. Instrukcja podlega monitorowaniu i w razie potrzeby uaktualnianiu co roku, do końca stycznia, przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.

5. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

[4] *Zarządzenie Nr 6 Dyrektora ZSS z dnia 07.03.2017 r.*

II. DEFINICJE.

1. Definicje

Ilekroć w instrukcji jest mowa o:

1) **administratorze danych osobowych** – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Zespole Szkół …. funkcję administratora danych pełni dyrektor szkoły;
2) **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji (ABI);
3) **administratorze systemu** – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagane specjalnych uprawnień;
4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) **zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;
6) **przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie;
7) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
9) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
10) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika szkoły, która upoważniona została do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;
11) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
12) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
13) **rozporządzeniu MSWiA** – rozumie się przez to 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.);
14) **serwisancie** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;
15) **sieci publicznej** – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną

głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

16) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

17) **szkole** – rozumie się przez to Zespół Szkół Sportowych w Szczecinie,

18) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

19) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ~~(t.j. Dz. U. z 2014 r., , poz.1182. z późn. zm.);~~ (t.j. Dz. U. z 2016 r., , poz.922 z późn. zm.[5]);

20) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

21) **użytkowniku** – rozumie się przez to pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło.

III. NADAWANIE I REJESTROWANIE (WYREJESTROWANIE) UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM.

1. Nadawanie i rejestrowanie uprawnień.

1) Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez dyrektora szkoły lub uprawnioną przez niego osobę.

2) Rejestracja użytkownika, o którym jest mowa w pkt. 1., polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. Wyrejestrowanie uprawnień.

1) Wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor szkoły lub upoważniona przez niego osoba.

2) Wyrejestrowanie, o którym jest mowa w pkt. 1., może mieć charakter czasowy lub trwały.

3) Wyrejestrowanie następuje przez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

[5] Zarządzenie Nr 6 Dyrektora ZSS z dnia 7.03.2017 r.

4) Czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:
   a) zawieszenia w pełnieniu obowiązków służbowych.

5) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   a) wypowiedzenie umowy o pracę,
   b) wszczęcie postępowania dyscyplinarnego.

6) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

IV. METODY I ŚRODKI UWIERZYTELNIENIA.

1. Każdy użytkownik systemu informatycznego otrzymuje od administratora bezpieczeństwa informacji identyfikator i hasło.

2. Identyfikator składa się z sześciu znaków, z których dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a cztery kolejne- czterem pierwszym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne./ wpisać własne/
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika systemu administrator bezpieczeństwa informacji nadaje inny identyfikator, odstępując od zasady określonej w pkt. 1.
4. Hasło użytkownika powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

6.Zmiana haseł w systemie następuje nie rzadziej niż co 30 dni. Pierwsze hasło jest przekazywane urzytkownikom ustnie przez ABI a następnie urzytkownicy są zobowiązani do zmiany haseł samodzielnie.

V. PROCEDURY ZWIĄZANE Z GROMADZENIEM, PRZECHOWYWANIEM, PRZETWARZANIEM, USUWANIEM DANYCH OSOBOWYCH.

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informacyjnym oraz wskazanie osoby odpowiedzialnej za te czynności.

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych (wzór tego upoważnienia stanowi załącznik do zarządzenia dyrektora szkoły). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego, przetwarzającego dane osobowe, następuje na wniosek dyrektora szkoły.

2) Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia upoważnienia zostaje dołączona do akt osobowych pracownika.

3) Identyfikator i hasło do systemu informatycznego, przetwarzającego dane osobowe, są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator bezpieczeństwa informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek administratora danych osobowych.

4) Administrator jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Zespole Szkół Sportowych w Szczecinie.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła
.
2) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.

3) Identyfikator i hasło użytkownika powinny odpowiadać wymaganiom, określonym w rozdziale IV.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych.

2) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3) Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji. Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu do zbioru danych.

4) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączony jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

5) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.

6) W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje, oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

7) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

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

1) Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie w tym celu wyznaczona.

2) Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe, tworzone są w następujący sposób:

a) kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie w sposób automatyczny na serwerze lokalnym szkoły,

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

1) Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku, gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2) Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek szkoły powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.

3) W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 4. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny,należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

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

1) W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.

2) Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania

danych z wykorzystaniem ogólnodostępnej sieci internet,

- przechwycenie danych z aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy, zakłócający pracę aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3) W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

4) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje, pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.

5) W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego, przetwarzający dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem, wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor, zapewniający ochronę przed wirusami w dokumentach MS Office, powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

6) Systemy antywirusowe, zainstalowane na stacjach roboczych, powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

7) System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

8) Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- skanowania zawartości dysków stacji roboczej, pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej, pracującej w systemie informatycznym, pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

9) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania, zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowefunkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1. pkt. 4. rozporządzenia MSWiA.

1) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy, pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

2) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizmy, pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu,

- nieudane próby dostępu do systemu informatycznego, przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3) Zapis działań użytkownika uwzględnia:
- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4) Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

2) Prace serwisowe na terenie szkoły, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jego pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych, znajdujących się w towarzystwie pracowników szkoły.

3) Przed rozpoczęciem prac serwisowych przez osoby spoza szkoły konieczne jest potwierdzenie tożsamości serwisantów.

4) Urządzenia, dyski lub inne elektroniczne nośniki informacji, 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;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VI. POZIOM BEZPIECZEŃSTWA.

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6. rozporządzenia.

VII. STOSOWANE ŚRODKI BEZPIECZEŃSTWA.

1. Zgodnie z treścią § 6. ust. 4 rozporządzenia o którym jest mowa w pkt. 1.1. niniejszej instrukcji stosuje się w szkole środki bezpieczeństwa na poziomie wysokim.

2. W szkole stosuje się następujące środki bezpieczeństwa:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3) Stosowane są mechanizmy kontroli dostępu do danych.
4) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

5) W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków.

6) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych.

7) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.

8) Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

9) 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 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.

10) W przypadku, gdy do uwierzytelnienia użytkowników używa się haseł, hasło to składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

11) Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

VIII. POSTANOWIENIA KOŃCOWE.

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest administrator bezpieczeństwa informacji lub inna osoba upoważniona przez administratora danych.

2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie (załącznik nr 3), potwierdzające znajomość jej treści.

4. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52. kodeksu pracy.

5. Niniejsza instrukcja wchodzi w życie z dniem 2 listopada 2015 r.

6. Traci moc instrukcja zarządzania systemem informatycznym stanowiąca załącznik Nr 2 do Zarządzenia Nr 7 Dyrektora Zezpołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie z dnia 01.09.2011 r.

Dyrektor
(-) mgr Jarosław Duda

…….
(Administrator danych osobowych)

Zmiany do Zarządzenia Nr 18 z dnia 02.11.2015 r. zostały wprowadzone Zarządzeniem Nr 6 Dyrektora ZSS z dnia 7.03.2017 r.

Tabela form naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych

Formy naruszeń	Sposoby postępowania
ZAKRESIE WIEDZY	
Ujawnienie sposobu działania aplikacji i systemu oraz zabezpieczeń osobom nieupoważnionym.	1. Przerwać czynność prowadzącą do ujawnienia informacji. 2. Sporządzić raport z opisem, jaka informacja została ujawniona. 3. Powiadomić Administratora Bezpieczeństwa Informacji.
Ujawnienie danych dotyczących infrastruktury informatycznej.	
Dopuszczanie do sytuacji lub stwarzanie warunków, w których osoba nieupoważniona pozyskuje wyżej wymienione informacje.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy z aktywną aplikacją umożliwiającą dostęp do bazy danych osobowych.	1. Zakończyć działanie aplikacji. 2. Sporządzić raport.
Dopuszczenie innej osoby do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych.	1. Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. 2. Sporządzić raport.
Pozostawienie w niezabezpieczonym i widocznym miejscu hasła dostępu do bazy danych osobowych lub sieci.	1. Zabezpieczyć informację z hasłami w sposób uniemożliwiający odczytanie. 2. Powiadomić Administratora Bezpieczeństwa Informacji. 3. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania z dostępem do bazy danych osobowych osobom nieupoważnionym.	1. Wezwać osobę nieupoważnioną do opuszczenia stanowiska. 2. Ustalić czynności, których dokonały osoby nieupoważnione. 3. Przerwać działanie programów. 4. Powiadomić Administratora Bezpieczeństwa Informacji. 5. Sporządzić raport.
Samodzielne instalowanie oprogramowania.	1. Pouczyć osobę, która zainstalowała oprogramowanie o bezprawności jej działania. 2. Wezwać służby informatyczne. 3. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	1. Wezwać osobę modyfikującą, aby tego zaniechała.

	2. Sporządzić raport.
Odczytywanie nośników informacji przed sprawdzeniem ich działania poprzez program antywirusowy.	1. Pouczyć osobę o szkodliwości takiego działania. 2. Wezwać służby informatyczne. 3. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW, KTÓRE ZAWIERAJĄ DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	1. Zabezpieczyć dokumenty. 2. Sporządzić raport.
Przechowywanie dokumentów niezabezpieczonych przed osobami nieupoważnionymi.	1. Powiadomić Administratora Bezpieczeństwa Informacji. 2. Poprawić zabezpieczenia. 3. Sporządzić raport.
Wyrzucanie dokumentów niewłaściwie zniszczonych, co umożliwia ich odczytanie.	1. Zabezpieczyć dokumenty. 2. Powiadomić przełożonych. 3. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów bez kontroli nad ich kopią.	1. Zaprzestać kopiowania. 2. Odzyskać kopię. 3. Powiadomić Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport.
Sporządzanie kopii danych na nośnikach danych niezgodnie z procedurą.	1. Zaprzestać kopiowania. 2. Odzyskać kopię. 3. Powiadomić Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez nadzoru niezamkniętego pomieszczenia z dostępem do danych osobowych.	1. Zabezpieczyć pomieszczenie. 2. Powiadomić Administratora Bezpieczeństwa Informacji. 3. Sporządzić raport.
Dopuszczanie do kontaktu ze sprzętem komputerowym osobom nieznanym.	1. Wezwać osoby opuszczenia pomieszczeń. 2. Ustalić tożsamość osób. 3. Powiadomić Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport.
Dopuszczanie do podłączania urządzeń do sieci komputerowej, demontażu gniazd i torów kablowych przez osoby nienależne do służb informatycznych i telekomunikacyjnych.	1. Wezwać osoby do zaprzestania bezprawnych działań. 2. Ustalić tożsamość osób. 3. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczanie do podłączania urządzeń do sieci komputerowej, demontażu gniazd i torów kablowych przez osoby nienależne do służb informatycznych i telekomunikacyjnych.	1. Wezwać osoby do zaprzestania bezprawnych działań. 2. Ustalić tożsamość osób. 3. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. 4. Sporządzić raport.
Dopuszczanie osób spoza służb	1. Wezwać osoby do zaprzestania

informatycznych i telekomunikacyjnych do przebywania w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej.	bezprawnych działań. 2. Ustalić tożsamość osób. 3. Wezwać do opuszczenia chronionych pomieszczeń. 4. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. 5. Sporządzić raport.

Załącznik Nr 3 Zarządzenia Nr 18 Dyrektora Zespołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie z dnia 02.11.2015 r. (wprowadzony Zarz. Nr 6 z 7.03.2017 r.)

PROCEDURA OBSŁUGI I KORZYSTANIA Z MONITORINGU WIZYJNEGO W ZESPOLE SZKÓL SPORTOWYCH W SZCZECINIE

I. Podstawa prawna:

1.Konwencja Praw Dziecka (Dz. U z 1991 r. Nr 120, poz. 526 ze zm.)
2.Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2016 r. poz. 1432)
3.Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922)
4.Rozporządzenie MENiS z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz. U. z 2003 r. Nr 6, poz. 69 ze zm.)

II.PROCEDURA

1.Zespół Szkół Sportowych w Szczecinie posiada monitoring wizyjny.

2.Celem zainstalowania monitoringu wizyjnego jest:

1) poprawa bezpieczeństwa osób przebywających na terenie szkoły oraz na terenie do niej przyległym
2) ograniczenie liczby sytuacji niepokojących w szkole i w jej bezpośrednim otoczeniu
3) rozwijanie świadomości społecznej i umiejętności podejmowania działań na rzecz poprawy bezpieczeństwa
4) aktywizacja i wspieranie organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w publicznych szkołach i placówkach
3.W szkole nie ma zainstalowanych kamer-atrap. Ciągłej obserwacji monitoringu dokonują pracownicy obsługi w dyżurce. Ekrany monitorów zamontowane w miejscach oglądu obrazów z kamer nie mogą być widoczne dla innych osób wchodzących do tych pomieszczeń.

4.W skład zestawu do monitoringu wizyjnego wchodzą:

Dwa rejestratory, dwa monitory komputerowe, kamery wewnętrzne (16 sztuk) i zewnętrzne (2 sztuki).

5.Zabezpieczone rejestratory oraz monitor znajduje się w serwerowni, a jeden monitor w dyżurce.

6.Kamery są rozmieszczone według dołączonego,, Planu rozmieszczenia kamer’’

7.Plik z materiałem archiwalnym może być przekazany upoważnionym organom – na ich pisemny wniosek.

7a. Zasady obowiązujące przy przekazywaniu pliku z materiałem archiwalnym upoważnionym organom:

1) przedstawiciel organów pisemnie kwituje odbiór materiału – protokół przekazania,
2) w pokwitowaniu odbioru zaznacza znaki szczególne materiału: nr kamery- określenie, miejsca zdarzenia nagranie z dn. – dzień, miesiąc, rok,
3) protokół przekazania przechowywany jest w sejfie w serwerowni,
4) do przegrywania materiału archiwalnego z rejestratora upoważniony jest informatyk lub osoba wskazana przez dyrektora.

8. Osobami uprawnionymi do ciągłej obserwacji monitoringu są pracownicy obsługi lub osoba powołana przez dyrektora szkoły.

9.Bieżący zapis monitoringu w ciągu dnia jest obserwowany przez osobę uprawnioną w dyżurce i w przypadku zaobserwowania przez nią sytuacji niepokojących ma ona obowiązek zgłosić niezwłocznie ten fakt dyrektorowi szkoły lub wicedyrektorom.

10.W przypadku zaistnienia niepokojących sytuacji w szkole lub otoczeniu szkoły osoby uprawnione przeglądają zapisy monitoringu i zgłaszają dyrektorowi zajście.

11.Zapisy z monitoringu będą wykorzystywane między innymi w sytuacjach:

1) zagrażających bezpieczeństwu uczniów, nauczycieli, pracowników szkoły,
2) niszczenia mienia szkoły,
3) przywłaszczenia,
4) konfliktowych, np. bójek
5) kryzysowych,
6) podejrzenia o palenie papierosów i korzystanie z używek,
7) jako przykłady dobrej praktyki i promowania właściwych zachowań.

12.Obrazy z monitoringu rejestrujące niepokojące sytuacje zapisywane są na trwałym nośniku informacji przez dyrektora i przechowywane do wyjaśnienia sprawy lub do końca danego roku szkolnego.

13.Pełny obraz z monitoringu przechowywany jest na dysku twardym przez minimum 30 dni a następnie ulega automatycznemu trwałemu usunięciu.

14.Elementy monitoringu wizyjnego będą w miarę konieczności i możliwości finansowych udoskonalane, wymieniane, rozszerzane.

15.Monitorowanie wizyjne stanowi środek wspierający wobec realizowanego w szkole planu dyżurów nauczycielskich, pracy woźnych i dozorców. Zainstalowany monitoring nie zwalnia wyżej wymienionych osób od wypełniania swoich obowiązków.

16.Osoby obserwujące bieżące zapisy i osoby przeglądające zapisy zobowiązane są do nieujawniania danych zarejestrowanych przez monitoring.

17.Prawo do ustalenia bądź zmiany hasła dostępu ma tylko dyrektor i administrator szkolnej sieci informatycznej.

18.W sprawach nieuregulowanych niniejszą procedurą ostateczną decyzję podejmuje dyrektor szkoły.

Załączniki :

1) Protokół przekazania na nośniku elektronicznym danych z systemu monitoringu Zespołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie – zał. Nr 1

2) Wniosek o udostepnienie danych z monitoringu Zespołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie – zał. Nr 2

Załącznik Nr 1 do procedury

Protokół przekazania na nośniku elektronicznym danych z systemu monitoringu Zespołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie

sporządzony w dniu ……r.

Dyrektor Zespołu Szkół Sportowych w Szczecinie, zwany dalej *przekazującym dane,*

przekazuje……
……
……
……

zwanym dalej *przyjmującym dane,*

na podstawie pisemnego wniosku z dnia……..dane z sytemu monitoringu szkoły.

1.Przekazujący przekazuje, a przyjmujący przyjmuje następujące dane (zapis z kamer):

Data	Numer kamery	Czas nagrania

2.Przyjmujący dane oświadcza, że wykorzystane zostaną one wyłącznie do celów określonych w pisemnym wniosku, stanowiącym załącznik do niniejszego protokołu.

Protokół sporządzono w dwóch jednakowych egzemplarzach, po jednym dla każdej ze stron.

……. ……..

Przekazujący Przyjmujący

Załącznik Nr 2 do procedury

Imię i nazwisko wnioskodawcy Szczecin, dnia…….

……..

……..

……..

Wniosek o udostepnienie danych z monitoringu

Zespołu Szkół Sportowych im. Sportowców Ziemi Szczecińskiej w Szczecinie

Zwracam się z prośbą o udostepnienie materiału z monitoringu wizyjnego szkoły z dnia…….

Uzasadnienie :

……
……
……
……
……
……
……
……
…….

……

Podpis wnioskodawcy

Decyzja dyrektora:

Wyrażam zgodę/nie wyrażam zgody

Data i podpis dyrektora