Polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Akademia Wychowania Fizycznego we Wrocławiu

al. Ignacego Jana Paderewskiego 35

51-612 Wrocław

SPIS TREŚCI

1. Wstęp

1.1. Informacje ogólne

1. Niniejsza Polityka bezpieczeństwa została opracowana w celu zapewnienia prawidłowości wdrożenia i zabezpieczenia procesu przetwarzania danych osobowych w Akademii Wychowania Fizycznego we Wrocławiu oraz kompleksowości rozwiązań w przedmiotowym obszarze.
2. Głównym celem wprowadzenia Polityki bezpieczeństwa jest zapewnienie zgodności działania Akademii z Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi.
3. Polityka Bezpieczeństwa została opracowana w oparciu o wytyczne zawarte w następujących aktach prawnych:
    - Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 992),
    - 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 nr 100, poz. 1024),
    - Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r. poz. 719),
    - Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r. poz. 745),

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Polityka Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Na Politykę Bezpieczeństwa składają się następujące informacje:
    - wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,

- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
2. **zbiór danych** — każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3. **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
5. **system informatyczny** — zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6. **zabezpieczenie danych w systemie informatycznym** — wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
7. **usuwanie danych** — rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
8. **dokumentacja przetwarzania danych** – dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określoną w przepisach wydanych na podstawie art. 39a ustawy,

9. **sprawdzenie** – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
10. **sprawozdanie** – dokument, o którym mowa w art. 36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia,
11. **Ustawa** - Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 992),
12. **GIODO –** Główny Inspektor Ochrony Danych Osobowych,
13. **ADO –** Administrator Danych Osobowych,
14. **ABI -** Administrator Bezpieczeństwa Informacji,
15. **ASI** - Administrator Systemów Informatycznych..

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH W AWF

2.1. INFORMACJE OGÓLNE

1. Administrator Danych Osobowych,
2. Administrator Bezpieczeństwa Informacji,
3. Administrator Systemów Informatycznych.

2.2. ADMINISTRATOR DANYCH OSOBOWYCH

Akademia Wychowania Fizycznego we Wrocławiu

al. Ignacego Jana Paderewskiego 35

51-612 Wrocław

Regon: 000327860

2.3. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

1. W AWF Wrocław zadania Administratora Danych Osobowych wykonuje Administrator Bezpieczeństwa Informacji i jego zastępca.
2. Do uprawnień i obowiązków Administratora Bezpieczeństwa Informacji należą m. in.:
    - stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym,
    - aktualizacja i modyfikacja ww. dokumentów,

- czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania,
- prowadzenie jawnego rejestru zbiorów danych osobowych,
- udział w kontrolach prowadzonych przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych,
- udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
- nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych,
- nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
- prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,
- nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,
- monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

2.4. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Administratorem Systemów Informatycznych jest osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).

   Do uprawnień i obowiązków Administratora Systemów Informatycznych należy m. in.:

   - nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
   - nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   - podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

- identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.

2.5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Akademia, jako Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej w oparciu o art. 31 ustawy.
2. Do umów zawieranych z podmiotami zewnętrznymi, przy realizacji których istnieje prawdopodobieństwo dostępu do pomieszczeń lub informacji i danych podlegających ochronie powinny zostać włączone klauzule:
    - dotyczące obowiązku ochrony tych informacji przez strony umowy zarówno w trakcie trwania umowy, jak i po jej ustaniu,
    - ograniczenia dostępu do informacji wyłącznie do osób związanych z realizacją umowy,
    - zakazu ujawniania danych,
    - odpowiedzialności w przypadku naruszenia bezpieczeństwa danych zarówno przez podmiot jak i zatrudnionych pracowników.
3. Projekty umów powierzenia przetwarzania danych osobowych innemu podmiotowi należy opiniować u Administratora Bezpieczeństwa Informacji.
4. Jednostki organizacyjne, w których zawierane są umowy powierzenia przetwarzania danych osobowych zobowiązane są do prowadzenia rejestru umów powierzenia.
5. Podmiot, któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie, ponosi również odpowiedzialność za zachowanie wszelkich wymogów wynikających z przepisów prawa w zakresie ochrony danych osobowych, w szczególności zastosowanie wymogów technicznych i organizacyjnych do zabezpieczenia przedmiotowych danych.

4. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi każdy pracownik mający dostęp do danych.
2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem odpowiednich niszczarek.
5. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
7. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

5. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji w przypadku stwierdzenia naruszenia:

- zabezpieczenia systemu informatycznego,
- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- ujawnienia metody pracy lub sposobu działania programu,
- jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).

2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

3. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

4. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych

- stosownie do objawów i komunikatów towarzyszących naruszeniu,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

5. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:

- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy AWF,
- może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych,
- nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza AWF.

6. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- cenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Raport, o którym mowa w pkt 6, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.

8. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

9. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo AWF, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.
10. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Wzór raportu z naruszenia bezpieczeństwa systemu informatycznego stanowi załącznik nr 8 do niniejszego opracowania.

6. TRYB I SPOSÓB SPRAWDZANIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH ORAZ OPRACOWANIA SPRAWOZDANIA

1. Sprawdzenie jest przeprowadzane w trybie:
   - sprawdzenia planowego – według planu sprawdzeń, o którym mowa w ust. 2-5;
   - sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;
   - art. 19b ust. 1 ustawy – w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.
2. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.
3. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych,
4. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje, co najmniej jedno sprawdzenie.
5. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem, co najmniej raz na pięć lat.

6. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
7. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie, o którym mowa w art. 19b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzenia.
8. Administrator bezpieczeństwa informacji dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
9.. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:
    - sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
    - odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
    - sporządzeniu kopii otrzymanego dokumentu;
    - sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
    - sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu..
10. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności administratora bezpieczeństwa informacji mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.
11. Materiały są sporządzane w postaci papierowej lub w postaci elektronicznej.
12. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności w toku sprawdzenia.

13. Administrator bezpieczeństwa informacji zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.
14. Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie.
15. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.
16. Administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie:
    - ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;
    - ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;
    - ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez Generalnego Inspektora zgodnie z art. 19b ust. 1 ustawy.

Wzór sprawozdania ze sprawdzenia stanowi załącznik nr 7 do niniejszego opracowania.

7. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Administrator Danych Osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych AWF, a w szczególności:

1. zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
2. zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
3. zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

7.1.ZABEZPIECZENIA ORGANIZACYJNE

1. Zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
2. Przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych. Szkolenia powinny dotyczyć :

a) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
b) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

3. Kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

Wykaz pomieszczeń, w których przetwarzane są dane osobowe zawiera załącznik nr 1 do niniejszego dokumentu.

Wzór upoważnienia dla pracownika zajmującego się przetwarzaniem danych osobowych zawiera załącznik nr 2 do niniejszego dokumentu.

7.2. ZABEZPIECZENIA TECHNICZNE

1. W pomieszczeniach, w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego.
2. W pomieszczeniach, w których znajdują się serwery zamontowane powinny być czujniki dymu.
3. W pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.
4. Wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

7.3. ZABEZPIECZENIA CHRONIĄCE PRZED UTRATĄ DANYCH

1. Odrębne zasilanie sprzętu komputerowego.
2. Ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.
3. Ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie do tego celu wyznaczona.
4. Ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.

7.4. ZABEZPIECZENIA PRZED NIEAUTORYZOWANYM DOSTĘPEM

1. Wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (skrosowanie) danego użytkownika do sieci komputerowej dokonuje

administrator systemu informatycznego w uzgodnieniu i po powiadomieniu Administratora Bezpieczeństwa Informacji.

2. Aby uzyskać dostęp do systemu, należy zwrócić się do Administratora Bezpieczeństwa Informacji z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.
3. W systemie informatycznym stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła:
   a) każdy użytkownik systemu przetwarzania posiada swój unikalny identyfikator;
   b) użytkownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami;
   c) każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa;
   d) hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik – zabronione jest przekazywania hasła innym osobom.

7.5. ZABEZPIECZENIA PRZED NIEAUTORYZOWANYM DOSTĘPEM PRZEZ INTERNET

W zakresie dostępu z sieci wewnętrznej do sieci rozległej Internet stosuje się firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. „Ściana ogniowa” składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

7.6. ZABEZPIECZENIA ANTYWIRUSOWE

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

1. Zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego.
2. Możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa” w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

8 - ARCHIWIZACJA DANYCH

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

8.1.WYKONYWANIE KOPII

1. Kopie wykonywane są na taśmę, płytę CD, DVD lub zewnętrzne nośniki pamięci.
2. Dane systemu wraz z bazą danych kopiowane są co najmniej raz w tygodniu – tzw. pełny backup bazy danych.
3. Kopie awaryjne danych zapisywanych w programie wykonywane są codziennie – tzw. dump schematu systemu.
4. Kopie awaryjne przechowywane są w miejscach zapewniających ich odpowiednią ochronę przed osobami niepowołanymi oraz czynnikami zewnętrznymi mogącymi je uszkodzić (np. kasa pancerna).
5. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
6. Administrator Bezpieczeństwa Informacji podejmuje odpowiednie czynności w celu okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

8.2. NISZCZENIE KOPII

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie.
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

ZAŁĄCZNIKI

Załącznik nr 1 – Wykaz pomieszczeń , w których przetwarzane są dane osobowe w AWF

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych

Załącznik nr 3 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 4 – Wykaz zbiorów danych osobowych w AWF

Załącznik nr 5 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 6 - Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Załącznik nr 7 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Załącznik nr 8 - Raport z naruszenia bezpieczeństwa systemu informatycznego

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: Miejsce:		

Załącznik nr 1 – Wykaz pomieszczeń, w których przetwarzane są dane osobowe w AWF

Dział/Stanowiska	Budynek i pokój	System komputerowy służący do przetwarzania danych osobowych
Archiwum	WOSS	Azak firmy Archicom S.C
Dziekanat wydziału WF	Budynek DS. Spartakus	eOrdo (system dziekanatowy firmy Unold Comp.),
Dziekanat wydziału Fizjoterapii	Budynek P4	eOrdo (system dziekanatowy firmy Unold Comp.),
Dziekanat Nauk o Sporcie	Hala Wielofunkcyjna	eOrdo (system dziekanatowy firmy Unold Comp.),
Dom studencki Spartakus	Budynek DS. Spartakus	eOrdo (system dziekanatowy firmy Unold Comp.),
Biblioteka	Biblioteka	Aleph (system biblioteczny firmy Aleph),
Kwestura	Hala Wielofunkcyjna	eOrdo (system dziekanatowy firmy Unold Comp.), F-K (system finansowo-księgowy firmy Yuma)
Dział Spraw Pracowniczych i Płac	Hala Wielofunkcyjna	Teta Constelation i Teta HRM (systemy kadrowo-płacowe firmy Unit4)
Rektorat	Budynek przy Banacha 11	eOrdo (system dziekanatowy firmy Unold Comp.)
Dział Organizacji Praktyk i Obozów	Budynek P 4	eOrdo (system dziekanatowy firmy Unold Comp.)
Centrum Doskonalenia Kadr, Dział Praktyk Pedagogicznych Studia Doktoranckie Wydziału WF	Budynek przy Witelona 25	eOrdo (system dziekanatowy firmy Unold Comp.)
Pracownicy dydaktyczni i administracyjni	INTRANET	Omnis (system dziekanatowy firmy Unold Comp.), Teta HRM (system kadrowo-płacowy firmy Teta)
Wydziałowe Komisje Rekrutacyjne	Budynkek P4	eOrdo (system dziekanatowy firmy Unold Comp.)

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji w Akademii Wychowania Fizycznego we Wrocławiu), na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182) upoważniam:

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r., poz. 1182), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Akademii Wychowania Fizycznego we Wrocławiu wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Akademii Wychowania Fizycznego we Wrocławiu (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 3 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

………………….., dnia …………….

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z ……………………………. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

……………………………………………….

Podpis

Załącznik nr 4 – Wykaz zbiorów danych osobowych w AWF

1. Dane gromadzone przez Dziekanaty.
2. Dane gromadzone przez Centrum Doskonalenia Kadr
3. Dane w Dziale Spraw Osobowych i Płac
4. Dane w systemie bibliotecznym
5. Dane do prac naukowych
6. Dane w systemie BHP
7. Dane w archiwum
8. Dane w księgowości
9. Dane w domu studenckim
10. Dane podręczne pracowników (naukowe i dydaktyczne)
11. Dane kandydatów na studia

Załącznik nr 5 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

Załącznik nr 6 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

ŚRODKI TECHNICZNE

Środek ochrony technicznej i fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).		
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**		
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**		
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**		
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**		
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**		
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**		
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**		

9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**		
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**		
11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie**.		
17. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**		
18. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**		

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych		
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych		
Wyznaczono Administratora Bezpieczeństwa Informacji		
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych		
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych		
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych		

Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego		
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy		
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym		
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco		

Załącznik nr 7 - Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/ czynności sprawdzających

.....

miejscowość, data

PROTOKÓŁ

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*

w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:.....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: .....
3. Data wykonania czynności kontrolnych:.....
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: .....
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:.....
6. Ustalenia dokonane w trakcie czynności kontrolnych:.....
7. Wnioski i zalecenia pokontrolne:

....

(data i podpis osoby wykonującej czynności kontrolne) (data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Administrator Bezpieczeństwa Informacji

* niepotrzebne skreślić

Załącznik nr 8 - Raport z naruszenia bezpieczeństwa systemu informatycznego

---

Akademia Wychowania Fizycznego Wrocław, dnia ……..

we Wrocławiu

Raport z naruszenia bezpieczeństwa systemu informatycznego

1. Data: ……. …… Godzina: ……

2. Osoba powiadamiająca o zaistniałym zdarzeniu:
……..
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:
……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……..
……..
……..

5. Przyczyny wystąpienia zdarzenia:
……..
……..
……..

6. Podjęte działania:
……..
……..
……..

7. Postępowanie wyjaśniające:
……..
……..
……..

……

data, podpis Administratora Bezpieczeństwa Informacji