

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

Akademia Wychowania Fizycznego we Wrocławiu

Luty 2022

1. WSTĘP

1.1. INFORMACJE OGÓLNE

Niniejszy dokument został opracowany w celu zapewnienia prawidłowości wdrożenia i zabezpieczenia procesu przetwarzania danych osobowych w Akademii Wychowania Fizycznego we Wrocławiu oraz kompleksowości rozwiązań w przedmiotowym obszarze. Głównym celem wprowadzenia „Polityki bezpieczeństwa” jest zapewnienie zgodności działania Akademii z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

1.2. CELE POLITYKI

Celami Polityki Bezpieczeństwa są:

- zapewnienie zgodności działalności Uczelni z przepisami powszechnie obowiązującego prawa, w zakresie bezpiecznego przetwarzania informacji i ich reprezentacji w postaci danych przetwarzanych w systemach informatycznych będących własnością lub utrzymywanych przez Uczelnię,
- zapewnienie wytycznych w celu właściwego bezpieczeństwa informacji w ramach realizowanych procesów administracyjnych, dydaktycznych oraz naukowych oraz bezpieczeństwa danych w ramach utrzymywanych systemów informatycznych.
- przeciwdziałanie incydentom bezpieczeństwa informacji,
- kształtowanie świadomości pracowników w zakresie konieczności przestrzegania zasad bezpieczeństwa informacji,
- wspieranie podstaw będących elementem budowy i stosowania w Uczelni dobrych praktyk w zakresie bezpieczeństwa informacji,
- dbanie o interes Uczelni w odniesieniu do przetwarzanych Informacji,
- zapewnienie w odniesieniu do przetwarzanych informacji chronionych odpowiedniego poziomu atrybutów bezpieczeństwa zgodnie z wymaganiami poufności, dostępności, integralności i rozliczalności.

1.3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZENSTWA ORAZ ZAKRES ZASTOSOWANIA

Polityka Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych oraz ich zabezpieczenia przed nieuprawnionym dostępem.

Na Politykę Bezpieczeństwa składają się następujące informacje:

- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
- Ewidencja osób upoważnionych do przetwarzania danych osobowych w Uczelni.
- Rejestr ryzyka.
- Rejestr czynności przetwarzania.

- 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.

1.4. WYJAŚNIENIE UŻYWANYCH TERMINÓW

- Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- 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.
- Przetwarzanie danych - jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
- Poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- Usuwanie danych - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
- 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.
- Polityka Bezpieczeństwa - „Polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”.
- ADO - Administrator Danych Osobowych,
- IOD - Inspektor Ochrony Danych.
- ASI - Administrator Systemów Informatycznych.
- RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. PODMIOTY ZAANGAŻOWANE W PROCES OCHRONY DANYCH OSOBOWYCH W UCZELNI

2.1. ADMINISTRATOR DANYCH OSOBOWYCH

Do obowiązków Administratora Danych Osobowych (ADO) należy m. in.:

- wdrożenie odpowiednich i skutecznych środków oraz wykazanie, że czynności przetwarzania są zgodne rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.
- współpraca z organem nadzorczym,
- udostępnianie organowi nadzorczemu rejestrów w celu monitorowania operacji przetwarzania,
- wdrożenie środków minimalizujące ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufności oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.

2.2. INSPEKTOR OCHRONY DANYCH

Do uprawnień i obowiązków Inspektora Ochrony Danych (IOD) należy m. in.:

- stały nadzór nad treścią Polityki Bezpieczeństwa,
- nadawanie poszczególnym pracownikom upoważnień do przetwarzania 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 przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych,
- szacowanie ryzyka właściwe dla przetwarzania,
- prowadzenie rejestru czynności lub rejestru kategorii czynności.

2.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

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

Do uprawnień i obowiązków ASI 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.

2.4. 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 RODO.
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.
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 IOD.
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 BEZPIECZENSTWA 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, jaki 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 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 IOD 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 IOD lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
4. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych IOD 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 IOD lub osoby upoważnionej.
5. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, IOD 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 powiadomienia o zaistniałym naruszeniu ADO,
 - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Uczelni.
6. IOD 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, IOD niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.
8. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu IOD 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 Uczelni, IOD, 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.

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

ADO jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Uczelni, a w szczególności:

- zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
- zapobiegać przetwarzaniu danych z naruszeniem RODO oraz zmianie, utracie, uszkodzeniu lub zapobiegać przed zabraniem danych przez osobę nieuprawnioną.

6.1. ZABEZPIECZENIA ORGANIZACYJNE

1. Zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych. IOD zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
2. 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.

6.2. 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 powinna znajdować się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.
4. Wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

6.3. 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 ASI lub osoba specjalnie do tego celu wyznaczona.
4. Ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.

6.4. ZABEZPIECZENIA PRZED NIEAUTORYZOWANYM DOSTĘPEM

1. Wszystkie gniazda lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie, (skrosowanie) danego użytkownika do sieci komputerowej dokonuje ASI w uzgodnieniu i po powiadomieniu IOD.

2. Aby uzyskać dostęp do systemu, należy zwrócić się do IOD 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:
 - każdy użytkownik systemu przetwarzania posiada swój unikalny identyfikator,
 - użytkownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami,
 - każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa,
 - hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik - zabronione jest przekazywanie hasła innym osobom.

6.5. 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.

6.6. ZABEZPIECZENIA ANTYWIRUSOWE

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.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania. Niezależnie od niniejszych zasad opisanych w „Polityce 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.

7. ARCHIWIZACJA DANYCH

Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii awaryjnych i kopii bezpieczeństwa. Za proces tworzenia kopii odpowiada ASI lub osoba specjalnie do tego celu wyznaczona.

7.1. WYKONYWANIE KOPII

1. Kopie wykonywane są na taśmie, płytę CD, DVD, zewnętrzne nośniki pamięci lub serwer kopii.
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 przechowywane są w miejscach zapewniających ich odpowiednią ochronę przed osobami niepowołanymi oraz czynnikami zewnętrznymi mogącymi je uszkodzić (np. kasa pancerna, serwerownia z kontrolą dostępu).
5. ASI odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
6. ASI podejmuje odpowiednie czynności w celu okresowej weryfikacji kopii zapasowych pod kątem ich przydatności.

7.2. 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 zniszczenia nośnika magnetycznego powinna być sprawdzona przez IOD.
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

Wzór upoważnienia do przetwarzania danych

Załącznik nr 2

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 3

Wzór raportu z naruszenia bezpieczeństwa systemu informatycznego

Załącznik nr 4

Rejestr czynności przetwarzania

Załącznik nr 5

Rejestr Ryzyka

Załącznik nr 6

Analiza Ryzyka

Inspektor Ochrony Danych

.....

Sporządził

Wrocław,

.....

Zatwierdził