Polityka bezpieczeństwa

systemu zarządzania bezpieczeństwem informacji

SPIS TREŚCI

Metryka dokumentu

Data	Wersja	Opis	Autor
01.07.2016	1.00	Utworzenie dokumentu	Piotr Welenc

Definicje

Administrator Danych Osobowych *(ADO)* – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Rektor, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji.

Administrator Bezpieczeństwa Informacji *(ABI)* – należy przez to rozumieć pracownika UMFC lub podmiot zewnętrzny powołany przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony danych osobowych i informacji, wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 poz. 1182 z późn. zm.)

Administrator Systemów Informatycznych *(ASI)* – należy przez to rozumieć pracownika lub pracowników Informatyki (również firm zewnętrznych, na podstawie zawartych umów) odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych.

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji oraz jej ochrona przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania i minimalizacji ryzyka przy zachowaniu atrybutów takich jak autentyczność, rozliczalność, niezaprzeczalność, niezawodność.

Bezpieczeństwo systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Dane osobowe mogą mieć formę: alfabetyczną, cyfrową, zdjęcia, video, dźwięku, danych biometrycznych *(odciski palców, obraz tęczówki),* danych medycznych.

Dane osobowe wrażliwe – kategoria danych osobowych objętych szczególną ochroną, których przetwarzanie jest poddane zasadom bardziej rygorystycznym niż przetwarzanie innych kategorii danych osobowych. Ich przetwarzanie jest co do zasady zabronione, a dopuszczalne jedynie w szczególnych, ściśle określonych w ustawie okolicznościach. Danymi osobowymi wrażliwymi są informacje - ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz o skazaniach, orzeczeniach o ukaraniu i mandatach karnych, a także o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.

Hasło *(Password)* – ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Identyfikator użytkownika *(LOGIN)* – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Osoba upoważniona lub użytkownik systemu – osoba posiadająca upoważnienie wydane przez **ABI** lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej jednostki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem.

Odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby, upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Osoba uprawniona – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności.

Przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych.

Sieć Lokalna *(LAN)* – lokalna sieć teleinformatyczna.

Sieć rozległa *(WAN)* – rozległa sieć teleinformatyczna.

UMFC – Uniwersytet Muzyczny Fryderyka Chopina w Warszawie

System informatyczny (SI) – jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. Na systemy informatyczne składają się obecnie takie elementy jak: sprzęt, oprogramowanie, zasoby osobowe, elementy oraz elementy informacyjne.

Użytkownik - osoba ujęta w ewidencji osób upoważnionych do przetwarzania danych, zidentyfikowana w systemach informatycznych wg nazwy identyfikatora*(login)* zabezpieczonego hasłem. Dla użytkownika po zalogowaniu do systemu informatycznego następuje automatyczna autoryzacja, mająca na celu ułatwienie korzystania z systemu informatycznego

Zalogowanie – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje).

Wprowadzenie

Niniejszy dokument opisuje stosowane reguły w celu zapewnienia bezpieczeństwa danych osobowych zawartych w systemach informatycznych w UMFC w Warszawie Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę w UMFC w Warszawie. Zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych, oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument ***„Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UMFC”***, zwanym dalej ***„Polityką bezpieczeństwa”***, wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z §3 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. Nr 100, poz. 1024). Polityka bezpieczeństwa jest zgodna z międzynarodową normą ISO/IEC 27001 standaryzująca systemy zarządzania bezpieczeństwem informacji oraz ISO/IEC 27000 oraz Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz. U. z 2012 r. poz. 526). ***Polityka bezpieczeństwa*** określa tryb postępowania w przypadku, gdy:

- stwierdzono naruszenie zabezpieczenia systemu informatycznego,
- stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji sieci informatycznej mogą wskazywać lub sugerować naruszenie zabezpieczeń tych danych,

Polityka bezpieczeństwa obowiązuje wszystkich pracowników UMFC. Każdy użytkownik ma obowiązek systematycznie zapoznawać się z regułami oraz z aktualnymi procedurami ochrony informacji w swojej jednostce organizacyjnej. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych UMFC. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. z 17.06.2002 r. Dz. U. Nr 2014, poz.1182 z późn. zm.),
- rozporządzeniem o ochronie danych osobowych Parlamentu Europejskiego
- rozporządzeniem KRI z dn. 12 kwietnia 2012 r.

Polityka bezpieczeństwa przetwarzania danych osobowych oraz bezpieczeństwa informacji w UMFC w Warszawie zwana dalej „Polityką”, została wydana w związku z § 3 ust. 1 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. Nr 100, poz. 1024).

Stanowi ona dokumentację systemu bezpieczeństwa informacji na podstawie rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, wydanego na podstawie art. 18 ustawy

z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. Zm.)

Wszędzie tam, gdzie niniejszy dokument odwołuje się do ogólnego, zintegrowanego systemu bezpieczeństwa informacji pierwszeństwo zapisów normy ISO27001 uznaje się odpowiednio, z zastrzeżeniem pierwszeństwa obowiązywania wewnętrznych zarządzeń Rektora UMFC. System zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001,

Niniejszy dokument :

1. dostępny jest każdemu upoważnionemu pracownikowi,
2. podlega weryfikacji i aktualizacji pod kątem aktualności nie rzadziej niż raz do roku oraz każdorazowo w przypadku:
   - zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji,
   - zaleceń wynikających z przeprowadzonej kontroli wewnętrznej bezpieczeństwa,
   - innych znaczących zmian dotyczących sposobu ochrony informacji.

Celem niniejszej Polityki jest:

1. określenie zasad bezpiecznego przetwarzania informacji chroniących przed nieuprawnionym przetwarzaniem, dostępem, ujawnieniem, utratą, nieprawidłowym wykorzystaniem lub kradzieżą. Zasoby informacyjne dotyczą wszelkich danych i wiadomości będących w posiadaniu UMFC. Informacja może przybierać różne formy, może być utrwalona w formie tradycyjnej – papierowej *(wydrukowana lub zapisana na papierze)*, przechowywana elektronicznie, przesyłana pocztą lub za pomocą urządzeń elektronicznych, wyświetlana lub wypowiadana słownie.
2. Zaprojektowanie, wdrożenie i utrzymanie zintegrowanego systemu zarządzania bezpieczeństwem informacji
3. stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych w zakresie prawidłowej ochrony przetwarzanych danych osobowych.
4. ustalenie celów bezpieczeństwa informacji,
5. Polityka określa również zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Uczelni oraz w kontaktach z otoczeniem gospodarczym.
6. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
7. Niniejszą Politykę stosuje się do:

   a. Danych osobowych:
      - przetwarzanych w systemach informatycznych,
      - zapisanych się na zewnętrznych nośnikach informacji,

   b. Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych
      - służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
      - dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
      - danych innych niż dane osobowe, a których ochrona wynika z odrębnych przepisów prawa, w tym Krajowych Ram Interoperacyjności
      - Dane osobowe przetwarzane są w celu realizacji statutowych celów UMFC, a w szczególności:

      a) dla zabezpieczenia prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Uczelni wynikających z przepisów ustawy z dnia 27.07.2005 roku Prawo o szkolnictwie wyższym. (Dz. U. z 2005r, Nr

164, poz. 1365 z późn. zm.)

b) w celu zapewnienia prowadzenia prawidłowej, zgodnej z przepisami prawa i potrzebami UMFC polityki personalnej oraz rozwoju kadry nauczycieli akademickich
c) prowadzenia kształcenia w różnych formach dydaktyczny, oceniania i dokumentowania w ten sposób nabytej wiedzy i umiejętności oraz wystawiania z tym związanych świadectw, dyplomów, certyfikatów uczestnikom kształcenia.
d) dla realizacji innych celów UMFC, w tym również gromadzenia i przetwarzania powierzonych uczelni danych osobowych osób związanych bezpośrednio lub pośrednio z UMFC z poszanowaniem ich prawa do ochrony tych danych oraz ich prywatności.

c. innych informacji, nigdzie nie sklasyfikowanych, a uznanych jako informacja przetwarzana w UMFC

6. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe lub sklasyfikowane gdzie indziej jako podlegające ochronie, których właścicielem i administratorem jest UMFC lub które uczelnia przetwarza na podstawie umów powierzeń, o których mowa w art. 31 Ustawy.
7. Niniejszy dokument ma charakter ogólny i określa podstawowe zasady zachowania bezpieczeństwa i wytyczne dla całej instytucji.
8. Polityka bezpieczeństwa jest inicjowana i współtworzona przez świadome omawianych w niej problemów Kierownictwo jednostki, który uchwalając niniejszą politykę daje wyraz woli bezpiecznej realizacji zadań UMFC.
9. Przedmiotem ochrony jest ochrona szeroko pojętych aktywów, ciągłość procesów biznesowych, zdolność produkcji i świadczenia usług, reputacja, zgodność działań z prawem oraz w szczególności wartości takie jak: kadra, środki techniczne, wartości niematerialne i prawne, wiedza, wizerunek organizacji, infrastruktura teleinformatyczna i innych.
10. Podmiotami zapewniającymi optymalny poziom bezpieczeństwa UMFC są jej pracownicy lub podmioty zewnętrzne świadczące usługi dla uczelni w ramach zawieranych umów cywilnoprawnych, działający w oparciu o najnowszą wiedzę i ogólnie dostępne zasoby techniczne.
11. Zasady przedstawione w niniejszym dokumencie obowiązują wszystkich pracowników, podwykonawców, konsultantów, pracowników pozostających w innym stosunku pracy jak również inne osoby świadczące usługi na rzecz UMFC, w tym pracowników osób trzecich korzystających z systemów informatycznych UMFC, świadczących usługi na podstawie umów cywilnoprawnych.
12. Kierownictwo UMFC odpowiedzialne jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń.
13. Za zapewnienie realizacji zapisów Polityki Bezpieczeństwa wraz z dokumentami wykonawczymi stanowiącymi jej integralne części odpowiedzialny jest osoba wyznaczona przez Rektora UMFC ds. Ochrony Danych Osobowych, zwany dalej ABI
14. Pracownicy o których mowa w p. 6 i 11 zobowiązują zapoznać się z Polityką Bezpieczeństwa w zakresie niezbędnym do skutecznego, adekwatnego i wydajnego świadczenia pracy jak również zobowiązują się dołożyć należytych starań, by odpowiednio wypełnić jej zapisy. Zakres obowiązywania Polityki Bezpieczeństwa zostanie określony w regulaminie pracy.
15. Nieprzestrzeganie zasad Polityki Bezpieczeństwa przez pracowników może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych oraz nieść za sobą skutki prawne. Szczególne wymogi w zakresie realizacji zapisów zdefiniowane zostaną w Regulaminie pracy lub stosownych

Zarządzeniach Rektora.

16. Nieprzestrzeganie zasad Polityki Bezpieczeństwa przez podwykonawców świadczących usługi na podstawie umów cywilnoprawnych może być potraktowane jako niedotrzymanie warunków umowy i nieść za sobą skutki prawne.
17. Kierownictwo UMFC odpowiedzialne jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji.
18. W ramach realizacji niniejszej Polityki kierownicy komórek organizacyjnych mają obowiązek wykonywać swoje zadania na dwóch poziomach:
    a. zapewnienie bezpieczeństwa bieżącego działania;
    b. bezpieczeństwo konkretnych systemów pozostających w gestii poszczególnych jednostek organizacyjnych.
19. UMFC zobowiązany jest do zastosowania spójnego systemu zabezpieczeń technicznych i organizacyjnych z uwzględnieniem czynnika ekonomicznego. System ten powinien być świadomie stosowany i właściwie zarządzany.
20. Administratorzy systemów, gestorzy sprzętu i oprogramowania, administrator bezpieczeństwa informacji oraz kierownicy wszystkich komórek zobowiązani są do ścisłej współpracy i koordynacji działań w celu zapewnienia przestrzegania zapisów niniejszej Polityki.
21. Rektor UMFC ma prawo podejmować działania o charakterze techniczno-organizacyjnym lub administracyjnym w celu zapewnienia optymalnego poziomu bezpieczeństwa UMFC.
22. Podstawą zapewnienia optymalnego poziomu bezpieczeństwa dla UMFC są systematycznie dokonywane analizy ryzyka na poziomie strategicznym i operacyjnym.
23. Różnorodne zabezpieczenia powinny być dobierane indywidualnie dla każdego z aktywów, z uwzględnieniem jego wartości i analizy ryzyka.
24. W wypadku gdy optymalne zabezpieczenia nie są możliwe do zastosowania ze względów finansowych, kierownictwo jednostek organizacyjnych ma obowiązek zastosować takie środki, które zapewnią skuteczny poziom bezpieczeństwa istotnych procesów.
25. Jednostki i komórki organizacyjne powinny znać obowiązujące regulacje prawne w zakresie obowiązków i zadań, jakie nakładają na nich przepisy prawa.
26. Wszelkie zmiany w polityce bezpieczeństwa powinny być dokonywane na piśmie pod rygorem nieważności i natychmiast publikowane.
27. Wszelkie zmiany w polityce bezpieczeństwa powinny być akceptowane przez Rektora UMFC.
28. Zmiany w polityce bezpieczeństwa powinny być dokonywane w oparciu o analizę ryzyka, analizę skutków finansowych ze szczególnym uwzględnieniem ryzyka reputacji UMFC.
29. Zmiany w zapisach Polityki Bezpieczeństwa powinny być konsultowane i opiniowane przez audyt wewnętrzny.
30. W przypadku wątpliwości co do charakteru działań podmiotu pod kątem obowiązywania niniejszej Polityki, należy zaniechać działania i rozstrzygnąć wątpliwości poprzez konsultację z bezpośrednim przełożonym.
31. Opisane zasady mają zastosowanie do wszystkich zasobów , w szczególności do:
    a. wszystkich nośników papierowych, magnetycznych, optycznych lub innych, na których są lub będą znajdować się dane osobowe lub inne informacje wrażliwe (sensytywne),
    b. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje.
    c. informacji będących własnością UMFC lub podmiotów, z którymi UMFC współpracuje, o ile zostały przekazane na podstawie umów powierzania przetwarzania danych osobowych,
    d. całego systemu informatycznego – wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych (aplikacji), oraz do dokumentów papierowych, w których przetwarzane są lub będą informacje,

32. Opisane w Polityce Bezpieczeństwa zasady dotyczą bez wyjątku wszystkich pracowników, bez względu na stosunek prawny, jak również praktykantów, stażystów, wolontariuszy, zleceniobiorców oraz innych osób upoważnionych do przetwarzania danych osobowych.

Oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa

UMFC wprowadzając, przestrzegając, realizując, monitorując i aktualizując niniejszą Politykę Bezpieczeństwa, dokłada najwyższej staranności, w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

a. przetwarzane zgodnie z prawem,
b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
d. przechowywane nie dłużej niż jest to niezbędne do realizacji celów, w których zostały zebrane

Przegląd dokumentacji z zakresu ochrony danych osobowych

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi, w szczególności o ochronie danych osobowych oraz zmianami faktycznymi w ramach UMFC, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności UMFC
3. Obowiązkiem UMFC jest zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok, na podstawie rozporządzenia o KRI
4. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych, w zakresie minimalizacji skutków i wystąpienia podobnych naruszeń w przyszłości.
5. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w UMFC.
6. Wszelkie zmiany Polityki powinny być zatwierdzane przez Rektora Uczelni.

ROZDZIAŁ I

Zasady postępowania przy przetwarzaniu danych osobowych

1. **Administrator Danych Osobowych,** którym jest Rektor UMFC, powierzył obowiązki **Administratora Bezpieczeństwa Informacji** dla danych zawartych w systemach informatycznych UMFC, zwanego dalej **Administratorem Bezpieczeństwa Informacji**.
2. **Administrator Bezpieczeństwa Informacji** – osoba powołana przez ADO – zakres zadań i odpowiedzialności został określony w umowie z podmiotem.
3. **Administrator Systemów Informatycznych** pracownik lub pracownicy Działu Informatyki– zakres zadań i odpowiedzialności w złączniku numer 16.
4. Kierownicy jednostek organizacyjnych UMFC realizują obowiązki wynikające z ustawy o ochronie danych osobowych wobec podległych pracowników, rezydentów, stażystów, studentów, kontrahentów, zbiorów danych, którymi zarządzają są zobowiązani do:
   a. współdziałania z **Administratorem Bezpieczeństwa Informacji,** w zakresie przestrzegania instrukcji o której mowa w rozdziale **VI**,
   b. sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,
   c. zwracania się do administratora danych o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania przepisów prawnych zakresu danych osobowych,
   d. niezwłocznego zawiadomienia **ABI** o konieczności utworzenia nowego zbioru danych osobowych.
5. Pracownik upoważniony przez **ABI** do przetwarzania danych osobowych, jest zobowiązany do:
   a. odbycia wewnętrznego szkolenia dotyczącego przetwarzania i ochrony danych osobowych
   b. zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   c. stosowania określonych przez administratora danych , procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   d. zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
   e. podporządkowania się poleceniom **ABI** oraz właściwego kierownika, w zakresie ochrony danych.
6. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez **Administratora Bezpieczeństwa Informacji**. Wzór upoważnienia stanowi załącznik nr 1 do niniejszego dokumentu.
7. Bezpośredni nadzór nad przetwarzaniem danych osobowych w jednostkach organizacyjnych UMFC sprawują kierownicy jednostek, a w przypadku pracowników na samodzielnych stanowiskach ABI. Pracownik, któremu **ABI** udzielił upoważnienia, o którym mowa w ust. 9 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik nr 2 do niniejszego dokumentu.
8. Pracownik, któremu **ABI** udzielił upoważnienia zobowiązany jest do dopełnienia szczególnej staranności w pracy, nie dopuszczając do ich udostępnienia osobom nieupoważnionym, zabrania przez osobę nieuprawnioną, nieautoryzowanych wpisów, uszkodzenia lub zniszczenia
9. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, kierownik jest zobowiązany bezzwłocznie skierować wniosek do **Administratora Bezpieczeństwa Informacji** o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje ABI. Wzór pisma o cofnięciu

upoważnienia stanowi załącznik nr 3 do niniejszego dokumentu.

10. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.
11. Upoważnienie, o którym mowa w pkt.9 po podpisaniu przez osobę, której upoważnienie dotyczy przekazuje się **Administratorowi Bezpieczeństwa Informacji.**
12. Po zaewidencjonowaniu upoważnienia, na podstawie dokumentu, o którym mowa w pkt 14. **ABI** przekazuje niezwłocznie:
    a) Oryginał upoważnienia – Kierownikowi Działu Spraw Pracowniczych
    b) Kopię upoważnienia – ABI
13. Na podstawie dokumentu, o którym mowa w pkt 15 ASI zakłada konto do systemów informatycznych – zgodnie z przydzielonym zakresem obowiązków.
14. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wydaje Rektor zgodnie z powszechnie obowiązującymi przepisami.
15. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.
16. **ADO** może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.
17. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.
18. Zbiory danych osobowych przetwarzane przez pracowników UMFC nie będą udostępniane do celów komercyjnych.

Obszar przetwarzania danych osobowych

Wyznacza się obszar przetwarzania danych osobowych w Uniwersytecie Muzycznym Fryderyka Chopina w Warszawie. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących ten obszar stanowi Załącznik nr 4 do niniejszego dokumentu.

Zbiory danych Osobowych

Podstawy przetwarzania zbiorów danych osobowych są zgodne z art. 23 ust. 1 oraz 27 ust. 2 UODO.

1. Na zbiory danych osobowych składają się:
    - dane w formie dokumentacji papierowej
    - dane w systemach informatycznych zgromadzone na nośnikach
2. Wykaz zbiorów danych osobowych prowadzi ABI według wzorów stanowiących załącznik 5a oraz 5b.
3. Kierownicy komórek organizacyjnych UMFC w Warszawie prowadzących zbiory danych osobowych lub zakładający takie zbiory zobowiązani są na bieżąco zgłaszać do ABI:
    1) zamiar założenia zbioru,
    2) rozpoczęcie pracy ze zbiorem,
    3) znaczącą modyfikacji lub zmianę sposobu wykorzystywania zbioru,
    4) zaprzestanie eksploatacji zbioru,
    5) konieczność likwidacji i sposób likwidacji zbioru.
4. Kierownicy komórek organizacyjnych UMFC, zobowiązani są do przekazywania do ABI wypełnionego formularza zgłoszenia zbioru danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych *(wzór stanowi załącznik do 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) jeżeli taki obowiązek wynika z przepisów prawa.

5. ABI przekazuje zgłoszenia zbiorów danych osobowych Generalnemu Inspektorowi Ochrony Danych Osobowych oraz prowadzi ewidencję zgłoszonych zbiorów po ich rejestracji.
6. Stosuje się pisemne umowy powierzenia przetwarzania danych przy współpracy z podmiotami zewnętrznymi przetwarzającymi dane osobowe. Powierzenie danych następuje wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący przetwarzanie danych zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych.

ROZDZIAŁ II

Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
   a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu informatycznego, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      - nieuprawniony dostęp do systemu z jego wnętrza,
      - pogorszenie jakości sprzętu i oprogramowania,
      - nieuprawniony przekaz danych,
      - bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym fakt pozostawienia serwisantów bez nadzoru,
   d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie

systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,

g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,

i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń np. login użytkownika i jego hasło,

j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,

k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki" (backdoor), itp.,

l) podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowano lub skopiowano dane osobowe,

m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych
w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, płytach CD/DVD w formie niezabezpieczonej itp.

ROZDZIAŁ III

Zabezpieczenie danych osobowych

1. **Administratorem Danych Osobowych** zawartych i przetwarzanych w systemach informatycznych UMFC jest Rektor.
2. **Administrator Bezpieczeństwa informacji** jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych UMFC, a w szczególności:
   - zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   - zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   - zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Do zastosowanych środków technicznych należy:
   - przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   - zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. wyżej,
   - szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,

- wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   - zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   - przeszkolenie osób, o których mowa w w/w ustępie, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych,
   - kontrolowanie otwierania i zamykania pomieszczeń, w którym są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
5. Niezależnie od niniejszych zasad 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.
6. Wykaz pomieszczeń w których przetwarzane są dane osobowe stanowi **załącznik nr 4** do niniejszego dokumentu.
7. Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób stanowi **załącznik nr 5a** i **5b** do niniejszego dokumentu.
8. Opis struktury zbiorów danych stanowi **załącznik nr 6** do niniejszego dokumentu.
9. Opis rejestracji baz danych stanowi **załącznik nr 7** do niniejszego dokumentu.
10. Opis zabezpieczeń systemów informatycznych stanowi **załącznik nr 8** do niniejszego dokumentu.

ROZDZIAŁ IV

Przestrzeganie zasad zabezpieczenia danych osobowych

1. **Administrator Danych Osobowych** lub osoba przez niego wyznaczona, którą jest **Administrator Bezpieczeństwa Informacji** sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. **Zasady bezpieczeństwa dotyczące informacji medycznej**
   a. Zasada legalności przetwarzania (przetwarzanie danych w sposób zgodny z prawem),
   b. Zasada związania celem przetwarzania danych osobowych (zbieranie danych dla oznaczonych zgodnych z prawem celów i niepoddawanie dalszemu przetwarzaniu niezgodnemu z tymi celami),
   c. Zasada merytorycznej poprawności i adekwatności przetwarzania danych osobowych (adekwatność danych w stosunku do celu ich przetwarzania, określenie w jakim celu, w jakim zakresie i przez kogo dane będą przetwarzane),
   d. Zasada ograniczenia czasu przetwarzania danych osobowych (przechowywanie danych nie dłużej niż jest to niezbędne do osiągnięcia celów, moment osiągnięcia celu obejmuje tak że czas archiwizacji, niejednokrotnie bowiem zaprzestanie „operacyjnego" przetwarzania danych nie wyczerpuje celu przetwarzania),
   e. Zasada przywilejów koniecznych (każdy użytkownik SI, posiada prawa ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań),
   f. Zasada wiedzy koniecznej (poszczególni pracownicy posiadają wiedzę o systemie informatycznym, ale ograniczoną wyłącznie do zagadnień , które są konieczne do realizacji powierzonych im zadań),
   g. Zasada pracy zbiorowej (wszyscy użytkownicy są świadomi o konieczności ochrony

wykorzystywanych zasobów),

h. Zasada indywidualnej odpowiedzialności (za utrzymanie właściwego poziomu bezpieczeństwa odpowiadają konkretne osoby, które mają świadomość tego, za co odpowiadają i jakie grożą im konsekwencje, jeżeli zaniedbają swoje obowiązki),
i. Zasada obecności koniecznej (prawo do przebywania w określonych pomieszczeniach obszaru mają wyłącznie osoby, które s ą do tego upoważnione).

ROZDZIAŁ V

Środki techniczne i organizacyjne

Część ta zawiera opis środków technicznych, organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Szczególny opis zawartości w „Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji" (rozdział VI).

Środki organizacyjne

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez ABI
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych.
3. W systemach informatycznych stosuje się wewnętrzny system uprawnień dostępu do danych, dla różnych roli (typ) użytkowników oraz uprawnienia przydzielane w ramach poziomów funkcjonalności eksploatowanych modułów.
4. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
5. Użytkownicy pojedynczych komputerowych stanowisk pracy w celu zabezpieczenia się przed skutkami utracenia informacji z dysków lokalnych powinni sporządzać kopie archiwizacyjne danych na dostępnych, zewnętrznych nośnikach informatycznych lub na udostępnionych im dyskowych zasobach sieciowych
6. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
7. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
8. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy UMFC. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest po uzgodnieniu z ABI
9. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy UMFC.
10. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem osoby upoważnionej. Opuszczone pomieszczenia są zamknięte na klucz.
11. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
12. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
13. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
14. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
15. Nośniki informatyczne wykorzystywane jednorazowo do celów archiwizacyjnych powinny być opatrzone identyfikatorem pozwalającym na ustalenie:
    1. daty sporządzenia,

2. zawartości,
3. danych personalnych osoby wykonującej archiwizację.

16. W przypadku wielokrotnego wykorzystywania nośnika informacje te umieszcza się w odpowiednim spisie
17. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

Środki techniczne

1. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy UMFC.
2. Stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
3. Nakazuje się podłączanie sprzętu komputerowego do gniazd wydzielonej sieci elektrycznej przeznaczonych wyłącznie do zasilania sprzętu komputerowego.
4. Zakazuje się podłączania innych urządzeń (w szczególności czajników, wentylatorów, sprzętu RTV) do gniazd wydzielonej sieci elektrycznej zasilającej sprzęt komputerowy.
5. Wszelkie narzędzia pracy przekazane przez UMFC, czyli zarówno komputer, terminal, drukarkę jak i dostęp do Internetu są własnością UMFC i powinny być wykorzystywane zgodnie z jego przeznaczeniem i wymaganiami właściciela
6. Za bezpieczne użytkowanie urządzeń przenośnych typu laptop lub pendrive, szczególnie w trakcie transportu, o ile użytkownik otrzymał zgodę na ich wynoszenie poza obszar przetwarzania danych odpowiada użytkownik.
7. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków służbowych
8. Każdy plik w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym.
9. W przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu.
10. Po zakończeniu pracy komputery (notebook) powinny być zabezpieczone w zamykanych na klucz szafach.
11. Komputerów tych nie należy wynosić poza budynek.
12. W wypadku potrzeby wyniesienia (np. notebooka dysk twardy notebooka musi być zaszyfrowany kluczem min. 128 bitowym Komputerów tych nie należy udostępniać osobom nieupoważnionym.
13. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą ABI.
14. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie/zniszczyć), aby nie zostały na nich dane osobowe.
15. W wypadku niemożliwości skasowania danych z nośnika (płyta CD/DVD) należy taką płytę zniszczyć fizycznie (np. za pomocą odpowiedniej niszczarki).
16. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
17. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
18. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
19. Do zabezpieczenia sieci należy stosować:
    - firewall,

- adresowanie stacji roboczych tylko adresami prywatnymi, nierutowalnymi,
- systemy wykrywania włamań IDS,
- logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach i stacjach roboczych,
- systemy antywirusowe i antyszpiegowskie,
- zabezpieczenia skrzynek poczty elektronicznej hasłami "trudnymi" (min. 8 znaków w tym litery, cyfry, znaki dodatkowe),
- zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż WWW, (zasada blokowania wszystkie i przepuszczania określonych usług w tym przypadku http, czyli port 80),
- zabezpieczenia stacji roboczych poprzez hasła w systemach MS Windows (autoryzacja użytkownika, login + hasło),
- zabezpieczenie wszelkich systemów teleinformatycznych hasłami „trudnymi" (min. 8 znaków w tym litery, cyfry, znaki dodatkowe),
- ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych, zmiany mogą zostać przeprowadzone tylko i wyłącznie przez administratora danego systemu (polityka ograniczonego zaufania).

ROZDZIAŁ VI

Instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji.

1. Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym
    a. Rejestracji użytkownika systemu informatycznego dokonuje się na podstawie upoważnienia, którego wzór stanowi Załącznik Nr 1 do niniejszego Zarządzenia
    b. Dostęp do danych osobowych przetwarzanych w systemach informatycznych może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła
    c. Dla każdego użytkownika ABI ustala niepowtarzalny identyfikator i hasło startowe
    d. Identyfikator użytkownika nie powinien być zmieniany, a po zablokowaniu konta użytkownika nie może być przydzielony innemu pracownikowi UMFC
    e. Konto użytkownika w systemie informatycznym i odpowiedni poziom uprawnień zakłada ASI na wniosek ABI lub przełożonego użytkownika
2. **Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.**
    a. hasło nie powinno zawierać mniej niż 8 znaków,
    b. hasło nie może być takie samo jak identyfikator,
    c. hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, **Administratora Bezpieczeństwa Informacji** lub automatycznie przez system,
    d. użytkownikowi nie wolno zapisywać hasła w sposób jawny oraz przekazywać ich innym osobom.
    e. użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
    f. komputery nie pracujące w sieci muszą mieć hasło założone na BIOS,
    g. w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować

się z systemu, lub uruchomić wygaszacz ekranu zabezpieczony hasłem,

h. za politykę hasłami odpowiedzialny jest **Administrator Bezpieczeństwa Informacji**,
i. hasło przy wpisywaniu nie może być wyświetlane na ekranie.
j. W przypadku podejrzenia, że hasło mogło zostać ujawnione, użytkownik zobowiązany jest do manualnej zmiany hasła.
k. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać : dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów itp.

3. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

a. administrator bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych, zawierającą ich identyfikatory, załącznik nr 11 do niniejszego dokumentu,
b. rejestracji użytkowników w systemie dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
c. zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
d. wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje administratora bezpieczeństwa informacji do odebrania dostępu do danych osobowych,
e. zalecane jest aby identyfikator składał się z imienia i nazwiska przedzielonych kropką.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

a. Dane osobowe, których administratorem jest UMFC mogą być przetwarzane z użyciem systemów informatycznych tylko na potrzeby realizowania zadań statutowych.
b. Rozpoczęcie pracy użytkownika w SI następuje po poprawnym uwierzytelnieniu się poprzez swoje indywidualne identyfikatory i hasła.
c. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu informatycznego opcji jego zamknięcia,
d. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu,
e. Po przekroczeniu okresu bezczynności 5 minut następuje automatyczne wylogowanie terminala z zamknięciem aplikacji i sesji sieciowej,
f. ABI ustala czas pracy użytkownikom systemu. Na pracę poza godzinami funkcjonowania UMFC musi wyrazić zgodę na piśmie kierownik jednostki organizacyjnej, w formie upoważnienia jednorazowego lub stałego,
g. w pomieszczeniach, gdzie przetwarzane są dane osobowe, monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,
h. dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania p.poż., UPS oraz alarm antywłamaniowy.
i. kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzi kierownik danej jednostki organizacyjnej,
j. o przekazywaniu danych osobowych innym podmiotom decyduje **ABI**,
k. osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się z danymi, zgodnie z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.
l. Po zakończeniu pracy obowiązują zasady: **„czystego biurka" i „czystego ekranu".**

5. Metoda i częstotliwość tworzenia kopii awaryjnych

a. Zbiory danych w systemach informatycznych są zabezpieczane przed utratą lub

uszkodzeniem za pomocą urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej oraz sporządzania kopii zapasowych zabiorów danych,

b. Sporządzane kopie bezpieczeństwa obejmują wszystkie systemy informatyczne, aplikacje i dane niezbędne do pełnego odtworzenia w razie awarii,
c. za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest **ABI**, lub osoba przez niego upoważniona,
d. kopii należy dokonywać poprzez przegrywanie (backup) całej bazy danych (bez kompresji),
e. w każdej chwili powinno być dostępnych jednocześnie cztery kopie z ostatniego dnia, tygodnia, miesiąca, i roku. Kopie należy zapisywać na taśmie lub dysku twardym, bądź innym nośniku niemodyfikowalnym,
f. kopie awaryjne może tworzyć jedynie administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
g. w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,
h. dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,
i. **ABI** lub administrator systemu wykonuje backup lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności .
j. Sporządzanie kopii bezpieczeństwa jest procesem zautomatyzowanym w celu uproszczenia zachowywania jak i odzyskiwania danych
k. Automatyczne wykonywanie kopii bezpieczeństwa podlega stałemu sprawdzeniu przez ABI lub osoby przez niego upoważnionej

Wprowadza się praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:

a. przeprowadzić składowanie informacji regularnie,
b. używać różnych typów nośników danych,
c. kopie umieszczać w różnych, oddalonych od siebie miejscach,
d. najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,
e. przed składowaniem danych sprawdzić je programem antywirusowym,
f. dokładnie opisywać składowane dane,
g. trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,
h. sprawdzić, czy składowanie przebiegło prawidłowo,
i. upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były pobrane,
j. regularnie konserwować urządzenia do składowania.

6. Ochrona przed szkodliwym oprogramowaniem. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposoby ich usuwania :

a. Ochrona komputerowego stanowiska pracy przez wirusami i innym szkodliwym oprogramowaniem jest obowiązkiem każdego pracownika.

b. Stosuje się hasła dostępu do warstwy BIOS komputerowych stanowisk pracy oraz hasła dostępu do konfiguracji aktywnych urządzeń sieciowych.

c. Aktualna wersja systemu ochrony antywirusowej jest dystrybuowana automatycznie poprzez sieć komputerową UMFC. W przypadku braku bezpośredniego dostępu do sieci należy uzyskać ją w Dziale Informatyki.

d. Zakazuje się przechowywania na komputerowych stanowiskach pracy i sieciowych

pamięciach masowych wszelkich prywatnych plików niezwiązanych z obowiązkami służbowymi określonymi w opisie stanowiska pracy.

e. Zakazuje się instalowania na stanowiskach komputerowych oprogramowania nie licencjonowanego dla UMFC. Oprogramowanie rozprowadzane na zasadach shareware i freeware, o ile w sposób udokumentowany nie zabraniają tego warunki jego używania, może być instalowane jedynie po zgłoszeniu tego na piśmie i uzyskaniu akceptacji Administratora Bezpieczeństwa Informacji.

f. W przypadkach stwierdzenia istnienia oprogramowania na stanowiskach komputerowych, które nie spełnia warunków określonych powyżej, podlega ono usunięciu wraz z danymi, z którymi jest bezpośrednio powiązane i które agreguje, z odnotowaniem tego faktu w notatce służbowej i przekazania informacji do Administratora Bezpieczeństwa Informacji.

g. Każde komputerowe stanowisko pracy, o ile oprogramowanie systemowe na to pozwala, jest zabezpieczane poprzez ograniczanie jego użytkownikowi prawa dokonywania zmian konfiguracyjnych w systemie operacyjnym oraz samodzielnego instalowania jakiegokolwiek oprogramowania. Ograniczenie to może nie obowiązywać w przypadku użytkowników, którzy na podstawie pisemnego zgłoszenia potwierdzonego przez własnego kierownika merytorycznego, uzyskali zgodę na rozszerzenie uprawnień od Administratora Bezpieczeństwa Informacji.

h. Ochrona w UMFC przed szkodliwym oprogramowaniem opiera się na wykrywaniu szkodliwego oprogramowania, naprawie oprogramowania, uświadamiania w zakresie zabezpieczeń oraz właściwej kontroli dostępu i zarządzaniu zmianami.

i. za ochronę antywirusową odpowiedzialny jest administrator bezpieczeństwa informacji,

j. do ochrony antywirusowej należy stosować program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie nośniki wymienne, przed ich uruchomieniem w sieci oraz na komputerach stacjonarnych,

k. sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w tygodniu (zalecane jest codzienne skanowanie komputera),

l. zalecane jest wykorzystanie programów pracujących w tle,

m. przy kontroli szczególną uwagę należy zwrócić na makra (dokumenty pakietów biurowych),

n. każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym,

o. korzystanie z zewnętrznych nośników i źródeł informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody ABI,

p. w przypadku wykrycia wirusa należy wykonać sprawdzenie danej stacji komputerowej.

q. Administrator Bezpieczeństwa Informacji działając wspólnie lub niezależnie są osobami uprawnionymi do przeprowadzania kontroli przestrzegania postanowień niniejszego zarządzenia na wszystkich komputerowych stanowiskach pracy UMFC. W przypadku stwierdzenia nieprawidłowości podejmują one działania w celu przywrócenia stanu zgodności
z niniejszym zarządzeniem i przygotowują notatkę służbową.

r. Zakazane jest wyłączenie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe

7. Sposób i czas przechowywania nośników informacji, w tym kopii zapasowych i wydruków.

a. nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,
b. za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest Właściciel, a za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest **ABI**,
c. W przypadku braku możliwości zrealizowania procedury zniszczenia nośników informacji, należy fakt ten zgłosić ABI, którzy podejmują stosowne kroki w celu zniszczenia przekazanych nośników.
d. zbędne dokumenty konwencjonalne (papierowe) powinny być zniszczone w niszczarce dokumentów lub przekazane do utylizacji firmie uprawnionej,
e. kopie bezpieczeństwa na nośnikach wymiennych powinny być przechowywane w zamkniętej metalowej szafie,
f. kopie na nośnikach wymiennych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
g. kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu danych,
h. wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane,
i. kopie przechowuje się co najmniej:
    - dzienne,
    - tygodniowe przez kolejny tydzień,
    - miesięczne przez kolejny miesiąc,
    - roczne przez cały kolejny rok od daty sporządzenia.
j. osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym, komputera nie należy pozostawiać w samochodzie,
k. kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności,
l. w przypadku nośników informacji przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych w sposób bezpieczny i pewny – np. poprzez spalenie lub pocięcie, lub pozbawienie danych w taki sposób, aby mogły zostać użyte przez inne aplikacje wewnątrz UMFC.
m. w przypadku kopii zapasowych sporządzanych przez użytkownika indywidualnie odpowiedzialnością za ich zniszczenie obarczony jest użytkownik

8. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych

a. przeglądu i konserwacji dokonuje ABI, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku,
b. sprawdzeniu podlega spójność danych, indeksów oraz stan nośników informacji np. dysków twardych, tasiemek,
c. zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia,
d. w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem, dokonać naprawy w obecności osoby upoważnionej przez administratora danych lub przekazać do naprawy firmie z która Urząd podpisuje odpowiednie dokumenty przekazania zbioru danych z zastrzeżeniem co do przetwarzania i wykorzystywania tych danych w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,
e. o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić **ABI**,
f. do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników).

9. Sposób postępowania w zakresie komunikacji w sieci komputerowej.

a. system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem (załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. poz. 1024).
b. przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione”,
c. Administrator Bezpieczeństwa Informacji określi zasoby dostępne dla każdego użytkownika,
d. użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania np. za pomocą skryptu logowania,
e. dostęp do serwerowni ma tylko ABI i pracownicy przez niego upoważnieni,
f. dostęp do konsoli serwera winien być zabezpieczony hasłem (min. 12 znaków, dostępnych w tablicy ASCII),
g. ABI winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików .log (plik z informacjami przekazywanymi przez system/program dla użytkownika),
h. w pomieszczeniu, gdzie ustawiony jest serwer może pracować tylko ABI, lub osoby przez niego upoważnione,
i. nie wolno instalować na żadnym z komputerów w sieci uczelni własnego oprogramowania bez zgody ABI,
j. użytkownicy nieuprawnieni nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i woluminów z poziomu systemu operacyjnego,
k. dostęp do archiwalnych plików pocztowych, mających status poufnych (informacje handlowe) należy zabezpieczyć hasłem,
l. wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do Sekretariatu Rektora Uczelni,
m. w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,
n. uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą ABI,
o. komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.
p. Każdy uprawniony użytkownik ma dostęp do :

a. Dysku sieciowego (katalog) - „Informacje dla Pracowników,
b. Portalu UMFC (intranet) w których udostępniane są istotne dla funkcjonowania uczelni oraz poszczególnych działów zarządzenia, plany, instrukcje, itp.;

10. Zasady korzystania z poczty elektronicznej

a) System Poczty Elektronicznej w domenie chopin.edu.pl jest przeznaczony wyłącznie do wykonywania obowiązków służbowych,
b) Przy korzystaniu z Systemu Poczty Elektronicznej, użytkownicy powinni posiadać świadomość, iż podlegają przepisom prawa, zwłaszcza w zakresie własności intelektualnej i prawa autorskiego,
c) Służbowe konto pocztowe zakładane jest użytkownikowi po wypełnieniu wniosku stanowiącego Załącznik nr 17 do niniejszej,
d) Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik wyraża zgodę na prowadzenie kontroli tych wiadomości przez Pracodawcę. Pracodawca nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych użytkownika w postaci naruszenia tajemnicy korespondencji,
e) Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, nieetycznym, uznawanym za powszechnie szkodliwe, gorszące, występującym wbrew prawom i godności osoby ludzkiej, bez względu na światopogląd, przekonania, wyznawane poglądy lub postawy, jak również niestosownym wobec powszechnie obowiązujących zasad postępowania, etyki zawodowej lub zasadom współżycia społecznego,
f) Użytkownik nie ma prawa wysyłać za pośrednictwem Internetu, w tym przy użyciu prywatnej skrzynki pocztowej wiadomości zawierających informacje poufne dotyczące UMFC, jego pracowników, pacjentów, kontrahentów, zawieranych umów lub relacji gospodarczych których stroną jest UMFC, ,
g) Użytkownicy nie powinni otwierać wiadomości od nieznanych osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi,
h) Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesłanych pocztą elektroniczną,
i) Użycie systemów teleinformatycznych i zasobów systemowych UMFC dla własnych celów komercyjnych jest ZAKAZANE,
j) Zakazane jest propagowanie lub wygłaszanie publiczne własnych opinii, jako oficjalnego stanowiska UMFC. Wątpliwości w tej materii każdorazowo należy komunikować bezpośredniemu przełożonemu
k) W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, użytkownik zobowiązany jest do zabezpieczenia ich hasłem. Hasło należy przekazać odrębnym kanałem komunikacji,
l) Całą korespondencja wpływająca na służbową skrzynkę jest korespondencją służbową.
m) Wobec zapisu powyżej, Pracodawca zastrzega sobie prawo monitorowania aktywności pracowników, w tym szczególnie skrzynek pocztowych oraz innych zasobów teleinformatycznych, z zachowaniem zasady poszanowania prywatności.

ROZDZIAŁ VII

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. **Niniejsze zasady określają tryb postępowania w przypadku gdy:**
    a. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
    b. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.
    c. udostępnienie osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzanie z naruszeniem ustawy oraz zmianę, utratę uszkodzenie lub zniszczenie
2. **O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:**
    a. brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
    b. brak możliwości zalogowania się do tej aplikacji,
    c. ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
    d. wygląd aplikacji inny niż normalnie,
    e. inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
    f. znaczne spowolnienie działania systemu informatycznego,
    g. pojawienie się nie standardowych komunikatów generowanych przez system informatyczny,
    h. ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
    i. ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych,
    j. włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych,
    k. zagubienie lub kradzież nośnika danych osobowych,
    l. zagubienie lub kradzież nośnika materiału,
    m. kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,
    n. informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
    o. fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,
    p. podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.
    q. telefoniczne próby wyłudzenia danych osobowych.
    r. otwarte drzwi do pomieszczeń, szaf gdzie przechowywane są dane osobowe,
    s. usytuowanie monitów pozwala na wgląd osób postronnych na dane osobowe,
    t. maile zachęcające do ujawnienia loginu/hasła
    u. hasła do systemów informatycznych przechowywane są w pobliżu stanowiska komputerowego
    v. próby nawiązywania rozmów telefonicznych z osobami, które nie przedstawiły się z

imienia i nazwiska, z jednoczesnym zastrzeżeniem swojej anonimowości

3. **O ujawnieniu danych osobowych decyduje:**
    a. dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą,
    b. w stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.
4. **Każdy pracownik UMFC biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych.**
    a. w szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania **Administratora Bezpieczeństwa Informacji** lub innej osoby wskazanej przez niego;
    b. osoba zatrudniona w UMFC, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym **Administratora Bezpieczeństwa Informacji** lub osobę zatrudnioną przy przetwarzaniu danych osobowych, albo inną upoważnioną przez niego osobę;
    c. **Administrator Bezpieczeństwa Informacji** jest odpowiedzialny za przygotowanie i opublikowanie wykazu osób, które mogą być informowane w przypadku wystąpienia zagrożenia danych osobowych;
    d. w przypadku niemożliwości zawiadomienia **Administratora Bezpieczeństwa Informacji** lub osób przez niego upoważnionych, pracownik winien powiadomić bezpośredniego przełożonego.
5. **Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych.**
    a. informacja przekazywana jest przez pracownika osobiście, telefonicznie lub pocztą elektroniczną;
    b. informacja, o której mowa w w/w podpunkcie powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia;
    c. w przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż **ABI**, jest ona obowiązana poinformować o tym fakcie **ABI**;
    d. pracownik może zostać poproszony przez **ABI** o potwierdzenie zauważonego faktu na piśmie.
6. **Czynności „pierwszej reakcji" użytkownika zgłaszającego naruszenie.**

    Do czasu przybycia **Administratora Bezpieczeństwa Informacji** lub upoważnionej przez niego osoby, zgłaszający:
    a. niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
    b. zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
    c. wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
    d. nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
    e. podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
    f. podejmuje inne działania przewidziane określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
    g. wstępnie udokumentować zaistniałe naruszenie;
    h. dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu

niebezpieczeństwu.

7. **Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:**
    a. zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy UMFC,
    b. zapisać wszelkie informacje związane z danym zdarzeniem,
    c. na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
    d. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
    e. dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,
    f. wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
    g. dokonać zmiany hasła na konto **ABI** i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
    h. zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
    i. rozważyć możliwość i potrzebę powiadomienia o zaistniałym naruszeniu **PDO**,
    j. nawiązać bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza UMFC,
    k. zamknąć i opieczętować urządzenia, w których przechowywane są dane osobowe w formie cyfrowej.
8. **Administrator Bezpieczeństwa Informacji podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W szczególności może on dokonywać, w zależności od zgłoszonego zdarzenia:**
    a. wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia,
    b. przeprowadzenia wywiadów z pracownikami w celu ustalenia zaistniałych faktów,
    c. przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
    d. przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,
    e. przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych,
    f. sporządzenia dokumentacji fotograficznej,
    g. zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu,
    h. zebrania innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.
9. **Po wykonaniu czynności, o których mowa w pkt. 7 i w pkt. 8, Administrator Bezpieczeństwa Informacji jest zobowiązany do podjęcia kroków w celu:**
    a. wyjaśnienia zdarzenia - w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
    b. wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów - w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich,
    c. zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
    d. usunięcie skutków incydentu i przywrócenie pierwotnego stanu systemu informatycznego (to jest sprzed incydentu).
10. **Czynności „pierwszej reakcji" Administratora Bezpieczeństwa Informacji**

ABI przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:

a. przeprowadzenie naprawy sprzętu informatycznego,
b. rekonfigurację sprzętu informatycznego,
c. wprowadzenie poprawek do oprogramowania,
d. rekonfigurację oprogramowania,
e. odtworzenie danych z kopii awaryjnych,
f. modyfikację danych w celu odtworzenia ich integralności,
g. wycofanie z użycia materiału kryptograficznego,
h. inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie systemu informatycznego.

11. Administrator Bezpieczeństwa Informacji może odstąpić od usuwania skutków incydentu, jeżeli został on spowodowany działaniem celowym, a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego jest niezmieniany w celach dowodowych do czasu wyjaśnienia sprawy.
12. Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych Administrator Bezpieczeństwa Informacji obowiązany jest upewnić się, że odtworzone dane zostały zapisane przed wystąpieniem incydentu - w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.
13. **Osoby upoważnione.**
    a. w sytuacjach wyjątkowych wszystkie powyżej opisane działania związane z usuwaniem skutków incydentu i wyjaśnianiem jego przyczyn mogą być realizowane przez osoby upoważnione przez Administratora Bezpieczeństwa Informacji.
    b. **ABI** odpowiada za sporządzenie listy pracowników mających prawo do podejmowania odpowiednich kroków w razie wystąpienia incydentu w sytuacji, gdy nie mogą one być wykonane osobiście przez niego.
14. **Raporty i powiadomienia.**
    a. ABI określa, na podstawie przeprowadzonych wyjaśnień, przyczyny zaistnienia incydentu,
    b. jeżeli incydent był spowodowany celowym działaniem, **ABI** jest zobowiązany do pisemnego powiadomienia Rektora Uczelni - Administratora Danych lub ABI, Rektor Uczelni - Administrator Danych lub ABI, biorąc pod uwagę charakter zdarzenia, mogą poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.
15. **Korzystanie z urządzeń po naruszeniu ochrony.**
    Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża **ABI** lub osoba przez niego upoważniona.
16. **Czynności końcowe - obserwacja.**
    System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.
    Okres kwarantanny, o którym mowa powyżej , jest uzależniony charakterem incydentu i specyfiki systemu informatycznego - jest on każdorazowo określany przez Administratora Bezpieczeństwa Informacji.
17. **Czynności końcowe - dokumentacja.**
    a. **ABI** dokumentuje w raporcie każdy zaistniały przypadek naruszenia ochrony danych osobowych,
    b. dokumentacja, o której mowa powyżej, obejmuje następujące informacje:
        - imię i nazwisko osoby zgłaszającej incydent,

- imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
- datę i godzinę przyjęcia zgłoszenia incydentu,
- określenie czasu i miejsca incydentu,
- opis zgłoszonego incydentu oraz okoliczności towarzyszące,
- przyczyny wystąpienia naruszenia,
- opis podjętych działań naprawczych,
- wyniki przeprowadzonego badania wyjaśniającego,
- ocenę skuteczności przeprowadzonego postępowania naprawczego,
- podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych.

c. wzór raportu, o którym mowa w ust.17, określa załącznik nr 9 do Polityki Bezpieczeństwa.

18. **Czynności końcowe - analiza.**
Administrator Bezpieczeństwa Informacji w oparciu o posiadaną dokumentację, odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:
   a. określenia skuteczności podejmowanych działań wyjaśniających i naprawczych.
   b. określenia wymagań działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów.
   c. określenia potrzeb w zakresie szkoleń użytkowników systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ VIII

Zasady dostępu do sieci rozległej dla pracowników i studentów UMFC w Warszawie

Sieć Komputerowa Uniwersytetu Medycznego Fryderyka Chopina w Warszawie jest kontrolowana poprzez podział na odseparowane logiczne domeny sieciowe – sieć wewnętrzną i sieć zewnętrzną z których każda jest chroniona poprzez zdefiniowany obwód bezpieczeństwa. Podział sieci został dokonany w oparciu o wartości i klasyfikację informacji przechowywanej lub przetwarzanej w sieci, poziomie zaufania, ocenę ryzyka wraz z innymi wymaganiami bezpieczeństwa dla każdej z nich celem ograniczenia wystąpienia zakłócenia usług. Ruch filtrowany jest w każdej ze skonfigurowanej sieci poprzez twz. BRAMY (gates), które blokują możliwość nieuprawnionego dostępu. Kontrola routingu opiera się na mechanizmach sprawdzania adresów źródłowych i docelowych przy wewnętrznych i zewnętrznych punktach kontrolnych sieci wraz ze stosowaniem serwera pośredniczącego PROXY.

Zdalni użytkownicy są uwierzytelniani poprzez stosowanie technik kryptograficznych w rozwiązaniach dla wirtualnych sieci prywatnych (VPN) poprzez klucze i certyfikaty. Do szyfrowania połączeń między hostami przez sieć publiczną Internet(tunel) używana jest biblioteka OpenSSL oraz protokoły SSLv3/TLSv1.

Pracownicy Uczelni mają zapewniony dostęp do sieci wewnętrznej oraz tylko do tych usług sieciowych, do których mają uprawnienia, które wynikają ze szczegółowego zakresu wykonywanych obowiązków uzgodnionych i przekazanych przez Kierownika jednostki organizacyjnej do Administratora Bezpieczeństwa Informacji. W sieci wewnętrznej dostępne są serwisy internetowe poprzez serwer

pośredniczący PROXY administracji rządowej, publicznej oraz inne wymagane w podziale na jednostki organizacyjne uzgodnione z Kierownikiem jednostki organizacyjnej.

W wypadku korzystania z dostępu do Internetu z prywatnych komputerów przenośnych oraz wyznaczonych komputerów osobistych przez pracowników Uczelni konieczne jest wypełnienie oświadczenia stanowiący załącznik nr 12 do Polityki Bezpieczeństwa Informacji. Pracownik wypełnia oświadczenie i składa je u Administratora Bezpieczeństwa Informacji *(wzór takiego wniosku stanowi załącznik nr 12 do Polityki Bezpieczeństwa Informacji)*. Po pozytywnym rozpatrzeniu takiego wniosku przez Rektora Naczelnego zostaje on przekazany Administratorowi Bezpieczeństwa Informacji w celu nadania uprawnień. Administrator Bezpieczeństwa Informacji lub wskazana przez niego osoba np. Administrator Sieci kontaktuje się z wnioskodawcą, uzyskuje od niego niezbędny do nadania uprawnień adres fizyczny jego karty sieciowej (MAC), poucza wnioskodawcę o konsekwencjach jakie mogą go spotkać jeśli stworzy zagrożenie w sieci Internet lub też naruszy prawo swoimi działaniami sieci rozległej, a także instruuje gdzie i w jakim zakresie możliwe jest korzystanie z połączenia internetowego Uczelni. Uzyskany adres fizyczny oraz nadany adres IP wpisuje w odpowiednie miejsce w oświadczeniu, które jest przechowywane do czasu odebrania lub wygaśnięcia uprawnienia do korzystania z Internetu.

W zakresie dozwolonym przepisami prawa ABI zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej

Administrator Bezpieczeństwa Informacji dokonuje kontroli nad dostępem do sieci zewnętrznej dokonuje odebrania uprawnień przekreślając oświadczenie w sposób niezmieniający czytelności dokumentu i następnie archiwizuje go. Ruch w sieci LAN(wewnętrznej) i WAN(zewnętrznej) jest monitorowany i zapisywany w postaci logów, które są archiwizowane na serwerze usług katalogowych NAS02. Każdorazowe wejście na daną stronę internetową lub serwis jest zapisywane i kojarzone z danym adresem IP w naszej sieci wewnętrznej, a co za tym idzie możliwe jest zidentyfikowanie użytkownika sieci który narusza wewnętrzne przepisy lub prawo.

Pracownikom będącym użytkownikiem sieci zabrania się:

1. Zmiany adresu IP
2. Zmiany adresu MAC karty sieciowej
3. Wykorzystywania sieci do działań niezgodnych z prawem, w tym przesyłania i udostępniania treści zakazanych prawem lub powszechnie uznanych za obraźliwe
4. Rozsyłania treści reklamowych
5. Korzystania z aplikacji typu peer to peer
6. Rozpowszechniania wirusów i złośliwego oprogramowania komputerowego
7. Korzystania z sieci Internet w sposób uciążliwy dla pozostałych pracowników uczelni
8. Korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, nieetycznym, uznawanym za powszechnie szkodliwe, gorszące, występującym wbrew prawom i godności osoby ludzkiej, bez względu na światopogląd, przekonania, wyznawane poglądy lub postawy, jak również niestosownym wobec powszechnie obowiązujących zasad postępowania, etyki zawodowej lub zasadom współżycia społecznego,
9.
10. Grać w gry komputerowe w Internecie lub w systemie informatycznym UMFC, za pośrednictwem urządzeń teleinformatycznych UMFC
11. podłączać modemy lub inne urządzenia służące umożliwieniu transmisji danych
12. dokonywać prób naruszania lub przełamywania zabezpieczeń teleinformatycznych UMFC
13. pobierać z Internetu jakichkolwiek plików multimedialnych niezwiązanych z prowadzoną

działalnością zawodową

W zakresie dozwolonym przepisami prawa ABI zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad. ABI może również blokować dostęp do niektórych treści dostępnych przez Internet. Ponadto, w uzasadnionym zakresie, ADO zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.

Za naruszenie przepisów wewnętrznych Administrator Bezpieczeństwa Informacji odbiera uprawnienie do korzystania z Internetu i informuje o tym ABI. W przypadku naruszenia przepisów prawa Administrator Bezpieczeństwa Informacji informuje o tym Rektora Naczelnego, a on organy ścigania.

Zasady dostępu do sieci rozległej dla pacjentów UMFC w Warszawie

Uniwersytet Muzyczny Fryderyka Chopina w Warszawie dla pacjentów zarejestrowanych i przebywających na terenie Uczelni nie udostępnia dostępu do Internetu.

Zasady dostępu do zewnętrznych baz danych dla pracowników uczelni

Dla personelu UMFC w Warszawie zostały udostępnione poniższe bazy danych celem pogłębiania swojej wiedzy i pozyskiwania nowych informacji z zakresu piastowanych stanowisk. W celu skorzystania z poniższych linków personel może do tego celu wykorzystywać sprzęt komputerowy i łącze internetowe w ramach jednostek organizacyjnych pod warunkiem, że nie dezorganizują pracy pozostałego personelu. Nie wyklucza się innego dostępu pod warunkiem uzgodnienia z ABI.

LP	Link	Tematyka	Uwagi
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

ROZDZIAŁ IX

Sprawdzenia

a. ABI dokonuje sprawdzeń zgodnie z trybem i sposobem realizacji określonymi w aktach wykonawczych wydanych na podstawie art. 36a ust. 9 UODO .
b. ABI przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Sprawdzenie powinno odbyć się co najmniej raz w roku – załącznik nr 18.
c. Z przeprowadzonych czynności sprawdzających ABI opracowuje sprawozdanie dla AD – załącznik nr 19.
d. Na wniosek GIODO – ABI dokonuje sprawdzenia wymienionego w pkt. 1. i za pośrednictwem AD przedstawia Generalnemu Inspektorowi sprawozdanie.
e. Do sprawdzeń stanu ochrony danych osobowych upoważniony jest ABI.
f. Sprawdzeniu podlegają zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych.
g. przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Sprawdzenie powinno odbyć się co najmniej raz w roku.
h. Po dokonanym sprawdzeniu ABI przekazuje sprawozdanie do AD.

ROZDZIAŁ X

Postanowienia końcowe

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Kierownicy komórek organizacyjnych są zobowiązani zapoznać z treścią Polityki Bezpieczeństwa każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
5. 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 nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
6. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 10 do niniejszego dokumentu.
7. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
8. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę

o zrekompensowanie poniesionych strat.

9. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. z 17.06.2002 r. Dz. U. Nr 2014, poz.1182 z późn.zm.), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
10. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UMFC" wchodzi w życie z dniem jej podpisania przez Rektora UMFC.

Rozdział XI

Załączniki do Polityki Bezpieczeństwa systemu zarządzania bezpieczeństwa informacji

Lista załączników:

Załącznik nr 1: Wzór upoważnienia,
Załącznik nr 2: Wzór oświadczenia o przeszkoleniu z zakresu zapisów ustawy o ochronie danych osobowych, przepisów wewnętrznych obowiązujących w UMFC oraz Zarządzeń Rektora dotyczących Polityki Bezpieczeństwa UMFC
Załącznik nr 3: Wzór wycofania upoważnienia,
Załącznik nr 4: Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane,
Załącznik nr 5a: Wykaz zbiorów przetwarzanych elektronicznie,
Załącznik nr 5b: Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie,
Załącznik nr 6: Opis struktury zbioru danych
Załącznik nr 7: Opis rejestracja baz danych
Załącznik nr 8: Opis zabezpieczeń systemów informatycznych
Załącznik nr 9: Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego w UMFC
Załącznik nr 10: Wzór wykazu osób które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UMFC"
Załącznik nr 11: Ewidencja osób upoważnionych do przetwarzania danych
Załącznik nr 12: Podłączanie do sieci UMFC komputerów prywatnych

Nr ewidencyjny.....

(nadany przez Administratora Bezpieczeństwa Informacji)

IDENTYFIKATOR.....

(nadany przez Administratora Bezpieczeństwa Informacji)

ROLA.....

(uprawnienia nadawane przez Lokalnego Administratora Danych Osobowych- zgodnie z ROZDZIAŁEM V)

UPOWAŻNIENIE

do przetwarzania danych osobowych

I. Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U.Nr 2014, poz.1182 z późn. zm.),

Upoważniam Panią/Pana.....

(imię i nazwisko)

zatrudnioną na stanowisku ……..

(nazwa stanowiska i komórki organizacyjnej)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na wyżej wymienionym stanowisku w formie papierowej *(dokumentacja medyczna, kartoteki, ewidencje, rejestry, spisy itp.)* oraz elektronicznej w określonym upoważnieniem ROLI w terminie……..…….. *(*od-do/ na czas nieokreślony)*

.....

(data, pieczątka i podpis Lokalnego Administratora Danych Osobowych)

OŚWIADCZENIE PRACOWNIKA

II. Ja niżej podpisany (na) oświadczam, iż:

1) Zostałam(em) przeszkolona(ny) w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. z 17.06.2002 r. Dz. U. Nr 2014, poz.1182 z późn. zm.), i 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. z 2004 r. Nr 100, poz. 1024), oraz innych obowiązujących w UMFC aktów prawnych.

Zadania i czynności do wykonania:

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (Dz. U. Nr 2014, poz.1182 z późn. zm.),
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym. (Rozdział VI)
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych. (Rozdział VII)
4. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.
5. Przestrzeganie zasad określonych w Instrukcji postępowanie z dokumentacją medyczną

....

(podpis pracownika) *(podpis bezpośredniego przełożonego)*

.....
(imię i nazwisko)

.....
(PESEL)

.....
miejscowość, data

OŚWIADCZENIE

Oświadczam, że przeszkolono mnie w zakresie przepisów prawa dotyczących ochrony danych osobowych, a w szczególności z ustawy z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Nr 2014, poz.1182 z późn. zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Uniwersytecie Muzycznym Fryderyka Chopina w Warszawie wprowadzoną zarządzeniem nr 32 Rektora Uczelni z dnia 20 grudnia 2013 r.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w:

Uniwersytet Muzyczny Fryderyka Chopina w Warszawie
ul. Okólnik 2
00-368 Warszawa

.....
(podpis składającego oświadczenie)

.....
(podpis prowadzącego szkolenie)

....., dnia ..... r.

.....
miejscowość, data

WYCOFANIE UPOWAŻNIENIA

Na podstawie art.37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 2014, poz.1182 z późn. zm.) w związku z:
.....
.....
.....
.....
.....

cofam upoważnienie

Pana/Pani .....
zatrudnionego/zatrudnionej w

.....

na stanowisku.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....
(data i podpis Administratora Bezpieczeństwa Informacji)

.....
(podpis pracownika)

....., dnia ..... r.

Wykaz pomieszczeń lub części pomieszczeń w których przetwarzane są dane

Lp.	Budynek / nr pokoju	Dział/Oddział/ samodzielne stanowisko Imię i nazwisko	Określenie części pomieszczenia, w którym przetwarza się lub archiwizuje dane
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Wykaz zbiorów przetwarzanych elektronicznie

Lp.	Budynek / nr pokoju	Jednostka organizacyjna / samodzielne stanowisko Imię i nazwisko	Nazwa urządzenia i program zastosowany do przetwarzania (urządzenie / system / program / wersja)	Nazwa zbioru / Cel przetwarzania
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie

Lp.	Budynek / nr pokoju	Jednostka organizacyjna / samodzielne stanowisko Imię i nazwisko	Określenie części pomieszczenia, w którym przetwarza się lub archiwizuje dane
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			

Opis struktury zbiorów danych

Zgodnie z §4 pkt 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024), dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.
W §4 pkt 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024) wyraźnie wskazano, że w polityce bezpieczeństwa ma być zawarty opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Opis ten może być przedstawiony w postaci formalnej, w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami, jak również opisu tekstowego.

Opisy struktury zbioru danych znajdują się w dokumentacji technicznej eksploatowanych systemów. Dokumentacja jest załączona w formie elektronicznej lub papierowej.

1. Zbiory danych używane podczas przetwarzania danych osobowych, są zbiorami pojedynczymi lub zbiorami stanowiącymi część bazy danych.
2. Przepływ danych w integralnym systemie opisują instrukcje obsługi systemów
3. Przepływ danych pomiędzy integralnymi systemami następuje albo za pomocą mechanizmów eksportu/importu danych, albo w drodze współdziałania systemów na zasadzie użytkownik - serwer, kiedy to system użytkownika uzyskuje dane od systemu serwera automatycznie na życzenie.
4. Zestawienie zawartości informacyjnej zbiorów danych osobowych przetwarzanych w UMFC znajduje się w dokumentacji prowadzonej przez Administratora Bezpieczeństwa Informacji

Załączniki:

1. .....
2. .....
3. .....
4. .....
5. .....

Opis rejestracji baz danych

W przypadku konieczności przetwarzania danych w nowej bazie danych, wymagana jest konsultacja z ABI). W przypadku konieczności rejestracji bazy danych w **Generalnym Inspektoracie Danych Osobowych**, rejestracja następuje zgodnie z art.41 ustawy o ochronie danych osobowych (Dz. U. Nr 2014, poz.1182 z późn. zm.)na wniosek danej jednostki/komórki organizacyjnej.

Każda jednostka/komórka organizacyjna powinna prowadzić dokumentację opisującą bazy danych osobowych, w której są przetwarzane.

Dokumentacja winna zawierać:

- nazwę bazy,
- imię i nazwisko osoby tworzącej,
- datę utworzenia,
- ewentualną datę zakończenia przetwarzania danych,
- podstawę prawną przetwarzania,
- cel przetwarzania,
    - opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,
- listę osób przetwarzających dane,
- sposób zbierania oraz udostępniania danych
    - informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane
- zakres danych osobowych zawartych w bazie,
- przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy),
- dodatkowe ważne informacje (zmiany osób uprawnionych itp.).
- opis środków technicznych i organizacyjnych zastosowanych w celach określonych w rozdziale V Środki techniczne i organizacyjne oraz w załączniku nr 8 do PBSZBI
- Informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego

Opis zabezpieczeń systemów informatycznych

1. W celu ochrony przed **utratą danych** w UMFC stosowane są środki techniczne i organizacyjne opisane w **Rozdziale V**, w tym m.in. następujące zabezpieczenia:

   a. odrębne zasilanie sprzętu komputerowego,
   b. ochrona serwerów przed zanikiem (wahaniami) zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   c. ochrona newralgicznych elementów sieciowych (przełączników) przed zanikiem zasilania,
   d. ochrona przed utratą zgromadzonych danych przez robienie okresowych kopii zapasowych na taśmach magnetycznych, dyskach przenośnych lub płytach CD/DVD, z których w przypadku awarii odtwarzane są dane i system operacyjny,
   e. ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych (mirroring); uszkodzenie jednego z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu.

2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych UMFC:

   a. wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (skrosowanie) danego użytkownika do szkieletu sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   b. aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie mają być udostępnione,
   c. w systemie informatycznym UMFC zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera UMFC podając login oraz hasło, drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika oraz hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

3. Zabezpieczenia fizyczne

   a. Zastosowano system kontroli fizycznego dostępu(karty chipowe) we wszystkich drzwiach w obwodzie centrum przetwarzania danych (Dział Informatyki, serwerownia).
   b. W centrum przetwarzania danych (Dział Informatyki, serwerownia) wydzielono 3 strefy :
      - Drukarnia
      - Dział Informatyki
      - Serwerownia
   c. centrum przetwarzania danych (Dział Informatyki, serwerownia) zabezpieczone jest systemem alarmowym
   d. centrum przetwarzania danych (Dział Informatyki, serwerownia) objęte systemem przeciwpożarowym SYSTEM GASZENIA TA-200 Z CENTRALĄ IGNIS 1520M.
   e. centrum przetwarzania danych (Dział Informatyki, serwerownia) posiada zabezpieczenia przed nieuprawnionym dostępem. Drzwi wyposażone są w zamki samozatrzaskowe, okna posiadają zewnętrzną ochronę w postaci krat.

4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych UMFC poprzez Internet. W zakresie dostępu do sieci wewnętrznej UMFC z rozległej sieci Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz ich filtrowanie w oparciu o adres IP i inne parametry. Zablokowano wszystkie nieużywane porty celem

zmniejszenia potencjalnych luk, które mogą być wykorzystane przez osobę próbującą uzyskać nieautoryzowany dostęp do sieci wewnętrznej. Ruch pakietów, oraz otwarte porty zostały określone przez Administratora Bezpieczeństwa. Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących.

W efekcie zapewnione jest:

a. zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wszystkich zbędnych portów,
b. objęcie ochroną antywirusową wszystkich danych ściąganych z sieci Internet na stacjach lokalnych,
c. zapisywanie do logów połączeń użytkowników z siecią Internet.

5. Postanowienia końcowe.

a. do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami, lub aplikacjami. Dostęp ten powinien być kontrolowany za pomocą drzwi z elektronicznym zamkiem szyfrowym;
b. zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ABI zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego;
c. osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.;
d. w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewni właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego;
e. w pobliżu wejścia do pomieszczenia z serwerami i innymi urządzeniami powinna znajdować się gaśnica, która jest okresowo napełniana i kontrolowana przez stosownego specjalistę.
f. Użytkownikom zabrania się ujawniania loginu i hasła
g. Zapisywania haseł w miejscach widocznych dla innych osób
h. Udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym
i. Używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna
j. Kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia poza UMFC
k. Samowolnego instalowania i używania jakichkolwiek programów komputerowych
l. Przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego
m. Narażania sprzętu komputerowego i nośników danych na kradzież
n. Wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia
o. Pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach lub centrów wydruku
p. Pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe
q. Pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady terminala
r. Przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym
s. Samowolnego podłączania komputerów, laptopów, terminali, do gniazd sieciowych w sieci informatycznej UMFC

Raport nr ...../.....

z naruszenia bezpieczeństwa systemu informatycznego w UMFC

Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię i nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

.....
(Imię i nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Lokalizacja zdarzenia:

.....
(np. nr pokoju; nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

.....
.....
.....

Podjęte działania:

.....
.....
.....

Przyczyny wystąpienia zdarzenia:

.....
.....
.....

Postępowanie wyjaśniające:

.....
.....
.....

Ocena skuteczności przeprowadzonego postępowania naprawczego:

.....

.....

.....

Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnym naruszeniom ochrony danych osobowych:

.....

.....

.....

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Wykaz osób, które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UMFC."

Wykaz osób, które zostały zapoznane z **„Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UMFC",** przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

LP	Nr ewidencyjny w upoważnieniu (zał. Nr 1 do PBI)	Nazwisko	Imię	Data nadania	Upoważniający	Data odebrania	Odbierający

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

Ewidencja osób upoważnionych do przetwarzania danych UMFC

Lp.	Identyfikator	Nazwisko	Imię	Stanowisko	Rola	Data
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						

.....
Imię Nazwisko

.....
Adres

.....
Jednostka/komórka organizacyjna

.....
Lokalizacja

OŚWIADCZENIE

1. Oświadczam, że posiadany przeze mnie komputer przenośny ……..

   ……..
   będzie użytkowany w sieci UMFC przeze mnie lub osoby upoważnione z poszanowaniem ogólnie przyjętych norm moralnych i etycznych oraz z zachowaniem obowiązujących przepisów prawa.
2. Komputer przenośny posiada legalne i stale aktualizowane oprogramowanie antywirusowe, pozostałe użytkowane i zainstalowane na nim oprogramowanie jest licencjonowane (w przypadku kontroli posiadam dowody legalności/zakupu oprogramowania).
3. Będę dokładać starań, by komputer przenośny nie stał się zagrożeniem dla innych użytkowników sieci (np. poprzez rozsyłanie wirusów, uniemożliwienia przejęcia nad nim zdalnej kontroli osobom postronnym spowodowane obecnością oprogramowania typu spyware lub niewłaściwego zabezpieczenia systemu).
4. Mam świadomość, że opieka nad prywatnym komputerem przenośnym nie leży w zakresie obowiązków Działu Informatyki UMFC w Warszawie.
5. Przyjmuję do wiadomości, że Uniwersytet Muzyczny Fryderyka Chopina w Warszawie nie są zobligowane do zapewnienia na prywatnych komputerach pracowników oprogramowania potrzebnego do pracy
6. W przypadku naruszenia któregokolwiek z powyższych punktów i przyjętych zasad korzystania z sieci (Netykieta, Ethical Uses of Software) oraz przepisów obowiązującego prawa jestem świadom(a) wynikających z tego konsekwencji prawnych (Ustawa z dnia 04.02.1994 o prawie autorskim i prawach pokrewnych, Dz. U Nr 80 z 2000r. poz 904 z późń. zm.; ustawa z dnia 06.06.1997 Kodeks karny Dz. U Nr 88 z 1997r poz. 553 z późń.zm.; ustawa z dnia 26.06.1974r. Kodeks pracy tekst jednolity Dz. U Nr 21 z 1998 poz. 94 z późń. zm.) oraz pozbawienia możliwości korzystania z sieci UMFC w Warszawie.
   Powyższe punkty przeczytałem(am), rozumiem je i zgadzam się z ich treścią

   ……
   Data czytelny podpis

   Komputer włączono do sieci, adres MAC: ……..

   Przydzielony adres IP: ……..

   Data, podpis pracownika Działu Informatyki :……

ZAKRES ZADAŃ I ODPOWIEDZIALNOŚCI

1. **Administrator Bezpieczeństwa Informacji (ABI)** realizuje zadania w zakresie ochrony danych zgodnie
   z Rozporządzeniami Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r w sprawie: *trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez ABI oraz prowadzenia rejestru zbiorów danych*, a w szczególności:
   a) Nadzorowania i koordynowania systemu zarządzania bezpieczeństwem informacji
   b) Stałego monitorowania, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem,
   c) zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w UMFC danych osobowych,
   d) sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych
   e) rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych, zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych.
   f) klasyfikowania zbiorów danych osobowych przetwarzanych w UMFC
   g) wnioskowania o usunięcie uchybień w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych,
   h) prowadzenia ewidencji miejsc przetwarzania danych osobowych i sposobu ich zabezpieczenia,
   i) opracowaniu programu szkoleń w zakresie ochrony danych osobowych.
   j) sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   k) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych UMFC,
   l) podejmowania stosownych działań zgodnie z niniejszą **Polityką bezpieczeństwa** w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   m) niezwłocznego informowania **Administratora Danych Osobowych** lub osoby przez niego upoważnionej (PDO) o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   n) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
   o) opracowania i wdrożenia programu szkolenia w zakresie zabezpieczenia systemu informatycznego.
   p) zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych
   q) bieżącej aktualizacji Polityki Bezpieczeństwa,

2. **Lokalni Administratorzy Danych Osobowych** realizują zadania w zakresie ochrony danych, którym przekazuje się odpowiednio do zakresu realizowanych przez nich celów statutowych obowiązki i uprawnienia administratora danych osobowych (ADO) w rozumieniu Rozdziału I pkt. 3 a w szczególności:
    a. Przetwarzania danych osobowych zgodnie z prawem,
    b. stworzenia właściwych warunków organizacyjno – technicznych zapewniających ochronę danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem
    z naruszeniem ustawy, nieautoryzowanymi wpisami oraz zmianą, utratą uszkodzeniem lub zniszczeniem,
    c. nadzorowania zaleceń dotyczących Instrukcji Zarządzania Systemami Informatycznymi opisanych w Rozdziale VI
    d. zapewnieniu kontroli nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu i w jakim celu są przekazywane,
    e. gromadzeniu danych osobowych dla oznaczonych, zgodnych z prawem celów i niepoddawaniu ich dalszemu przetwarzaniu, niezgodnemu z tymi celami,
    f. zapewnienie, aby przetwarzane dane osobowe były merytorycznie poprawne i adekwatne w stosunku do celów w jakim są przetwarzane,
    g. przechowywaniu danych osobowych w postaci uniemożliwiającej identyfikację osób, których dane dotyczą nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
    h. nadawaniu upoważnień do przetwarzania danych osobowych, w zakresie określonym w załączniku nr 1 do Polityki Bezpieczeństwa Systemu Zarządzania Bezpieczeństwem Informacji,
    i. zgłaszanie ABI osób, które upoważniono do przetwarzania danych osobowych w celu ujęcia w ewidencji,
    j. dopuszczeniu do przetwarzania danych wyłącznie osób upoważnionych,
    k. przedstawianie propozycji nowego zbioru danych osobowych UMFC,
    l. zapoznawaniu osób upoważnionych do przetwarzania danych osobowych ze zmianami w obowiązujących przepisach,
    m. zawiadomieniu właściwej komórki organizacyjnej oraz PDO o zmianach/aktualizacji obszaru przetwarzania danych osobowych,
    n. w przypadku naruszenia bezpieczeństwa danych osobowych zgłoszenie tego faktu PDO, przeprowadzenie analizy okoliczności i przyczyn, które doprowadziły do naruszenia obowiązujących przepisów i wnioskowanie o wprowadzenie niezbędnych zabezpieczeń,

3. **Administrator Systemów Informatycznych** pracownik lub pracownicy Działu Informatyki wyznaczeni przez ABI. Do podstawowych obowiązków ASI należy:
    a. zakładanie i blokowanie kont użytkowników systemu,
    b. dokonywanie zamiany uprawnień użytkowników systemu,
    c. przestrzeganie opracowanych dla systemu procedur bezpieczeństwa,
    d. bieżące utrzymywanie systemów informatycznych w sprawności technicznej w stopniu

określonym w dokumentacji powykonawczej,

e. aktualizowanie i konfigurowanie oprogramowania antywirusowego,
f. reagowanie na naruszenia bezpieczeństwa i usuwanie ich skutków,
g. nadzorowanie właściwego użytkowania oraz serwisowania urządzeń i oprogramowania,
h. prowadzenie rejestru awarii systemu,
i. wykonywanie kopii bezpieczeństwa informatycznych baz danych osobowych oraz systemów informatycznych,
j. wykonywanie innych zadań służących ochronie danych osobowych przetwarzanych w UMFC, które ABI uzna za konieczne,