Załącznik nr 1 do Zarządzenia Rektora nr 23/2018

Polityka Bezpieczeństwa Informacji

Uniwersytetu Muzycznego Fryderyka Chopina

Warszawa, kwiecień 2018

SPIS TREŚCI

1. WSTĘP

W obecnych czasach każda organizacja zbiera, przetwarza, przechowuje i przesyła informacje, które podlegają ochronie m.in. z uwagi na wymagania prawne, kwestie związane z wizerunkiem organizacji lub przed skutkami wynikającymi z ujawnieniem, utratą lub zmianą przetwarzanych informacji. Uniwersytet Muzyczny Fryderyka Chopina, jako publiczna akademicka uczelnia artystyczna działająca na podstawie przepisów prawa, posiada i przetwarza informacje, które są niezbędne do prowadzenia i wspierania działalności dydaktycznej, artystycznej i naukowej, zgodnie z misją i Statutem Uniwersytetu. Z uwagi na zakres informacji a także cel przetwarzania niezbędne jest zapewnienie im bezpieczeństwa na możliwie najwyższym poziomie.

Bezpieczeństwo informacji polega przede wszystkim na zapewnieniu im poufności, integralności i dostępności, w sposób świadomie przyjęty i zaakceptowany przez wszystkich pracowników i inne osoby posiadające uprawniony dostęp do informacji, na podstawie przepisów prawa, określonych standardów oraz przyjętych w tym celu reguł i zasad obowiązujących w Uniwersytecie Muzycznym Fryderyka Chopina. Wszystkie planowane i podejmowane działania związane z zapewnieniem bezpieczeństwa informacjom, w tym ochronie danych osobowych, przede wszystkim wynikają z przepisów krajowego i międzynarodowego prawa i kompleksowo określane są jako **System Zarządzania Bezpieczeństwem Informacji (SZBI)**. Informacja może przybrać bardzo różną formę i może być w różny sposób przetwarzana: może być wyrażona werbalnie, niewerbalnie, zapisana odręcznie lub elektronicznie, w formie liter, nut, cyfr lub innych zakodowanych znaków. Zarówno tradycyjny nośnik – papier, jak i system teleinformatyczny mogą być sposobem jej przetwarzania. Również zapisy monitoringu wizyjnego, nagrań rozmów telefonicznych a także wiedza i doświadczenie pracowników są źródłem cennych dla organizacji informacji. Bez względu na formę jaka informacja przybierze oraz sposób i miejsce jej przetwarzania wymaga ona ochrony i zapewnienia jej bezpieczeństwa.

Wprowadzony w Uniwersytecie Muzycznym Fryderyka Chopina spójny System Zarządzania Bezpieczeństwem Informacji ma na celu usystematyzowanie wszelkich działań związanych z bezpieczeństwem informacji, w tym bezpieczeństwem danych osobowych, SZBI UMFC obejmuje swoim zakresem wszystkie lokalizacje Uniwersytetu (w Warszawie i w Białymstoku), a także podległe mu jednostki (m.in. Bibliotekę Główną, domy studenckie).

2. DEKLARACJA ZAANGAŻOWANIA KIEROWNICTWA

Władze Uczelni przywiązują szczególną wagę do ochrony informacji przetwarzanej w Uniwersytecie Muzycznym Fryderyka Chopina, a także do ochrony informacji powierzonych Uniwersytetowi przez inne podmioty celem przetwarzania. Gwarancją odpowiedniej i skutecznej ochrony informacji jest zapewnienie właściwego poziomu bezpieczeństwa oraz zastosowanie adekwatnych do istniejących lub potencjalnych zagrożeń rozwiązań organizacyjnych i technicznych. Niniejszy dokument Polityki Bezpieczeństwa Informacji stanowi jeden z elementów wprowadzonego przez Rektora Systemu Zarządzania bezpieczeństwem Informacji, jest dokumentem ogólnym, odnoszącym się do szeroko pojętego bezpieczeństwa Informacji. Konkretne i szczegółowe polityki, instrukcje, procedury i inne regulacje wewnętrzne, wynikające zarówno z przepisów prawa jak i przyjętych przez Uniwersytet standardów w obszarze bezpieczeństwa, stanowią dokumenty wewnętrzne Uniwersytetu związane z niniejszą Polityką Bezpieczeństwa Informacji i składają się na całość dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji Uniwersytetu.

Władze Uczelni deklarują pełne zaangażowanie w ciągłe planowanie, tworzenie, aktualizowanie, sprawdzanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji w Uniwersytecie Muzycznym Fryderyka Chopina w celu utrzymania go na jak najwyższym poziomie zapewniającym bezpieczeństwo informacjom, w tym danym osobowym przetwarzanym w Uniwersytecie.

3. DEFINICJE I SKRÓTY

ABI	Administrator Bezpieczeństwa Informacji (zamiennie: IOD od 25.05.2018r.)
ABS	Administrator Bezpieczeństwa Systemów
ADO	Administrator Danych Osobowych
AI	Administrator Informacji
Aktywa/Zasoby	wszystko, co ma wartość dla organizacji – w obszarze informacji
ASI	Administrator Systemów Informatycznych
Dostępność	zapewnienie, że informacja jest dostępna i użyteczna dla osób uprawnionych zawsze gdy zaistnieje taka konieczność
Incydent	pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia ciągłości działania i zagrażają bezpieczeństwu informacji
Integralność	zapewnienie, że informacja jest zawsze dokładna i kompletna
IOD	Inspektor Ochrony Danych (zamiennie: ABI do 24.05.2018r.)
PBDO	Polityka Bezpieczeństwa Danych Osobowych
PBI	Polityka Bezpieczeństwa Informacji
PBST	Polityka Bezpieczeństwa Systemów Teleinformatycznych
Poufność	zapewnienie, że informacja nie jest udostępniana ani ujawniana uprawnionym do jej otrzymania osobom, podmiotom lub procesom
Pracownik uczelni	wszystkie osoby, które wykonują powierzone obowiązki na rzecz Uniwersytetu Muzycznego Fryderyka Chopina – nauczyciele akademiccy oraz pracownicy niebędący nauczycielami akademickimi – bez względu na podstawę zatrudnienia (umowa o pracę, o dzieło, umowa zlecenia, staż, praktyka i in.)
RUST	Regulamin Użytkowników Systemów Teleinformatycznych
System teleinformatyczny	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, w tym również za pomocą obrazu i dźwięku.
SZBI	System Zarządzania Bezpieczeństwem Informacji
UMFC/Uniwersytet	Uniwersytet Muzyczny Fryderyka Chopina
Użytkownik	każda osoba, która posiada login do systemu wykorzystywanego w Uniwersytecie
Władze Uczelni	Rektor, Prorektorzy, Kanclerz
Zdarzenie	określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może mieć wpływ na bezpieczeństwo

4. PODSTAWOWE ZASADY BEZPIECZEŃSTWA INFORMACJI

Wszyscy pracownicy UMFC oraz osoby wykonujące zadania na rzecz UMFC na podstawie umowy innej niż umowa o pracę muszą zostać zapoznani z regułami oraz z aktualnymi procedurami ochrony informacji oraz są zobowiązani do ochrony informacji i przestrzegania zapisów Polityki Bezpieczeństwa Informacji i dokumentów z nią związanych.

Bezpieczeństwo informacji to zachowanie poufności, integralności i dostępności informacji. Są to trzy podstawowe atrybuty bezpieczeństwa informacji, które zgodnie z normą ISO 27001 definiowane są w następujący sposób:

Poufność – zapewnienie, że informacja nie jest udostępniana ani ujawniana uprawnionym do jej otrzymania osobom, podmiotom lub procesom.

Integralność – zapewnienie, że informacja jest zawsze dokładna i kompletna.

Dostępność – zapewnienie, że informacja jest dostępna i użyteczna dla osób uprawnionych zawsze gdy zaistnieje taka konieczność.

Zapewnienie bezpieczeństwa informacjom zapewni przestrzeganie kilku uniwersalnych zasad, które stanowią podstawę realizacji zapisów niniejszej PBI:

1. **Zasada uprawnionego dostępu**. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
2. **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań (wykluczenie zasady „wszystko wszystkim”).
3. **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
5. **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
6. **Zasada obecności koniecznej.** Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
7. **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
8. **Zasada najsłabszego ogniwa**. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
9. **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
10. **Zasada ewolucji**. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
11. **Zasada odpowiedniości**. Używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.

12. **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
13. **Zasada segregacji zadań**. Zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełni władzy nad całym systemem.

5. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W UNIWERSYTECIE MUZYCZNYM FRYDERYKA CHOPINA

5.1. STRUKTURA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

System Zarządzania Bezpieczeństwem Informacji w UMFC został wprowadzony na podstawie zapisów 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*, uwzględnia wymagania polskich norm PN-ISO/IEC 27001:2014 oraz PN-ISO/IEC 27002:2014, natomiast kwestie związane z ochroną danych osobowych zgodne są z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej: RODO).

Zarządzanie bezpieczeństwem informacji w UMFC uwzględnia procesy utrzymania odpowiedniego poziomu zabezpieczeń i opiera się na następujących podstawowych procesach:

1. zarządzanie ryzykiem/oceną skutków dla przetwarzania danych osobowych;
2. nadzór i przeglądy SZBI – dokonywane w oparciu o:
   a. przeglądy i sprawdzenia przeprowadzane przez ABI/IOD
   b. kontrole i audyty wewnętrzne;
   c. kontrole i audyty zewnętrzne;
3. aktualizacja i doskonalenie SZBI;
4. nadzór nad dokumentacją;
5. zarządzanie dostępem do zasobów;
6. zarządzanie incydentem.

Zarządzanie bezpieczeństwem informacji w UMFC odbywa się na trzech poziomach:

1. poziom strategiczny;
2. poziom taktyczny;
3. poziom operacyjny.

Poziom strategiczny	Poziom taktyczny	Poziom operacyjny
Władze Uczelni	ABI/IOD, ABS	ABI/IOD, ABS,ASI, AI,
Określenie kierunków rozwoju SZBI Zapewnienie środków niezbędnych do wprowadzenia SZBI Wprowadzenie i zarządzanie SZBI Nadzór nad SZBI	Tworzenie i rekomendowanie standardów bezpieczeństwa Nadzór nad stosowaniem przyjętych standardów bezpieczeństwa Podnoszenie świadomości użytkowników	Stosowanie standardów bezpieczeństwa Podejmowanie działań w przypadku ujawnienia naruszeń bezpieczeństwa Przedstawianie propozycji udoskonaleń SZBI

5.2. CEL WDROŻENIA SZBI

Celem wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji jest osiągnięcie takiego poziomu organizacyjnego i technicznego w Uczelni, który:

1. zagwarantuje pełną ochronę informacji oraz ciągłości procesów ich przetwarzania,
2. zapewni zachowanie poufności, integralności oraz dostępności informacji chronionych, a także integralności i dostępności informacji publicznych,
3. zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
4. ograniczy występowanie zagrożeń związanych z bezpieczeństwem informacji, wynikających z celowych lub przypadkowych działań człowieka oraz ich ewentualnego wykorzystania na szkodę UMFC,
5. zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
6. zapewni gotowość do podjęcia działań w sytuacjach kryzysowych w ramach bezpieczeństwa UMFC, jego interesów oraz posiadanych i powierzonych mu informacji.

Powyższe cele realizowane są poprzez:

1. wyznaczenie struktury organizacyjnej w obszarze bezpieczeństwa informacji w UMFC,
2. wyznaczenie osób zarządzających kluczowymi aktywami przetwarzania informacji,
3. przyjęcie za obowiązujące przez wszystkich pracowników polityk i procedur bezpieczeństwa wdrożonych w UMFC,
4. wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych i technicznych,
5. przegląd i aktualizację polityk i procedur postępowania dokonywany przez odpowiedzialne osoby,
6. ciągłe podnoszenie świadomości i kwalifikacji pracowników w obszarze bezpieczeństwa informacji.

5.3. ZAKRES OBOWIĄZYWANIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

System Zarządzania Bezpieczeństwem Informacji UMFC obejmuje:

1. wszystkie jednostki organizacyjne UMFC, szczegółowo określone w Statucie;
2. pomieszczenia, w których przetwarzane są informacje podlegające ochronie, zlokalizowane w:
   - siedzibie UMFC w Warszawie,
   - Wydziale Zamiejscowym UMFC w Białymstoku,
   - Bibliotece Głównej UMFC,
   - Domach Studenckich w Warszawie i w Białymstoku,
3. zasoby informacyjne (aktywa) związane z realizacją zadań publicznych, a w szczególności:
   a. potencjał ludzki – wszystkich pracowników UMFC,
   b. dokumenty we wszelkiej ich formie (tradycyjnej /papierowej/, elektronicznej i każdej innej) stanowiące własność lub będące w posiadaniu UMFC,
   c. wszelkie stacjonarne i mobilne nośniki danych, przeznaczone do przetwarzania informacji,
   d. systemy, programy lub aplikacje służące do przetwarzania informacji.

5.4. ROLE I ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI W UNIWERSYTECIE MUZYCZNYM FRYDERYKA CHOPINA

Odpowiedzialność za bezpieczeństwo informacji w UMFC ponoszą wszyscy pracownicy UMFC (nauczyciele akademiccy i osoby niebędące nauczycielami akademickim bez względu na rodzaj zawartej umowy) – zgodnie z posiadanymi zakresami obowiązków oraz z nadanymi im upoważnieniami, a także osoby wykonujące zadania na rzecz UMFC na podstawie umów innych niż umowa o pracę – zgodnie z zakresem i celem umowy. Pracownicy muszą zostać zapoznani z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji zawartymi w PBI oraz w innych dokumentach wewnętrznych UMFC.

Władze Uczelni odpowiedzialne są za zapewnienie zasobów niezbędnych dla funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń.

Kierownicy jednostek organizacyjnych odpowiedzialni są za przestrzeganie zasad dotyczących ochrony bezpieczeństwa informacji w podległych im jednostkach przez podległych im pracowników, identyfikowanie i dokumentowanie zagrożeń w zakresie bezpieczeństwa informacji oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa. Zobowiązani są do powiadomienia ABI/IOD lub ABS o incydentach związanych z naruszeniem bezpieczeństwa.

Pracownicy Uczelni są zobowiązani do ochrony informacji przed dostępem osób nieuprawnionych, do ochrony danych przed przypadkowym lub umyślnym zniszczeniem, utratą lub nieuprawnioną modyfikacją. Każdy odpowiada za ochronę zasobu, do którego otrzymał dostęp – np. sprzęt komputerowy, nośniki mobilne. Pracownicy mają w obowiązku powiadomić ABI/IOD, ABS lub bezpośredniego przełożonego o każdym zdarzeniu zagrażającym bezpieczeństwu informacji: ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym, o możliwości zniszczenia informacji chronionych lub o ich nieautoryzowanej zmianie.

Na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w UMFC określono role i odpowiedzialność osób mających szczególne obowiązki w obszarze bezpieczeństwa informacji, ze szczególnym uwzględnieniem ochrony danych osobowych:

ADO – ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych osobowych w Uniwersytecie Muzycznym Fryderyka Chopina w rozumieniu krajowych przepisów o ochronie danych osobowych jest Rektor Uniwersytetu. Z uwagi na fakt, że ochrona danych osobowych zawiera się w szeroko pojętym bezpieczeństwie informacji, Rektor odpowiada za bezpieczeństwo wszystkich podlegających ochronie informacji, m.in. w następujący sposób:

1. wprowadza, zarządza i sprawuje nadzór nad SZBI;
2. określa rodzaje zasobów podlegających ochronie;
3. decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych;
4. zatwierdza i wprowadza polityki, instrukcje, procedury dotyczące obszaru bezpieczeństwa informacji w UMFC, w tym bezpieczeństwa danych osobowych;
5. sprawuje nadzór nad realizacją zapisów PBI, PBDO, PBST i innych regulacji dotyczących obszaru zarządzania bezpieczeństwem informacji, w tym ochrony danych osobowych;

6. upoważnia osoby do przetwarzania danych osobowych;
7. podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

ABI – ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI/ IOD – INSPEKTOR OCHRONY DANYCH

Osoba wyznaczona przez ADO, podana do wiadomości wszystkich pracowników oraz osób, których dane są przetwarzane w UMFC.. Jako ABI do dnia 24 maja 2018r. wykonuje zadania przewidziane w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, a od 25 maja 2018r. pełni funkcję IOD zgodnie z zapisami RODO i obowiązującymi po tej dacie krajowymi przepisami z obszaru ochrony danych, m.in.:

1. koordynuje/wspiera działania związane z SZBI w UMFC;
2. zapewnia przestrzeganie przepisów o ochronie danych osobowych;
3. zbiera informacje w celu identyfikacji procesów przetwarzania danych;
4. analizuje i sprawdza zgodność tego przetwarzania;
5. informuje, doradza i rekomenduje ADO określone działania dotyczące bezpieczeństwa informacji, w szczególności danych osobowych;
6. doradza w UMFC w sprawach związanych z przetwarzaniem danych;
7. prowadzi szkolenia pracowników z zakresu bezpieczeństwa informacji i danych osobowych.

Szczegółowy zakres działań ABI/IOD określony został w Polityce Bezpieczeństwa Danych Osobowych UMFC.

ABS – ADMINISTRATOR BEZPIECZEŃSTWA SYSTEMÓW

Kierownik Działu Informatyki UMFC/wyznaczona przez Rektora osoba

1. sprawuje nadzór nad bezpieczeństwem systemów teleinformatycznych,
2. sprawuje nadzór nad ASI powołanymi na jego wniosek,
3. sprawuje nadzór nad analizą ryzyka technologicznego,
4. sprawuje nadzór nad analizą podatności systemów,
5. sprawuje nadzór nad przygotowaniem dokumentów wymagań bezpieczeństwa dla systemów teleinformatycznych,
6. opiniuje standardy bezpieczeństwa dotyczące systemów teleinformatycznych,
7. inicjuje wypracowanie standardów dotyczących systemów teleinformatycznych,
8. analizuje raporty z wszelkich zdarzeń związanych z bezpieczeństwem systemów teleinformatycznych,
9. zawiadamia ADO o przypadkach naruszenia bezpieczeństwa informacji w systemach informatycznych oraz możliwych zagrożeniach,
10. prowadzi nadzór merytoryczny nad dokumentacją systemów teleinformatycznych i aplikacji;
11. prowadzi nadzór merytoryczny nad przygotowaniem dokumentów planów awaryjnych dla systemów teleinformatycznych;
12. dokonuje oceny i akceptacji proponowanych zmian i rozwiązań w politykach dla systemów teleinformatycznych, nad którymi sprawuje nadzór,
13. współpracuje z osobami odpowiedzialnymi za bezpieczeństwo informacji w SZBI w zakresie realizacji zadań dotyczących bezpieczeństwa informacji,
14. przygotowuje i aktualizuje dokumenty PBST, RUST.

ASI – ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH
Wskazani przez ABS pracownicy Działu Informatyki:

1. monitorują oraz zapewniają ciągłość działania systemu teleinformatycznego;
2. utrzymują konfigurację i wydajność systemu teleinformatycznego;
3. instalują i konfigurują sprzęt, systemy i aplikacje serwerowe;
4. odpowiadają za administrację oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem;
5. współpracują z dostawcami aplikacji;
6. nadzorują wdrożone aplikacje w zakresie serwerów;
7. zarządzają kopiami awaryjnymi danych, w tym danych osobowych zgodnie z otrzymanym upoważnieniem;
8. opracowują dokumentacje dla systemów teleinformatycznych;
9. opracowują procedury określające zarządzanie systemem teleinformatycznym;
10. zawiadamiają ABS o przypadkach naruszenia bezpieczeństwa informacji w systemach informatycznych oraz możliwych zagrożeniach;
11. wnioskują o zmiany do PBST i RUST.

AI – ADMINISTRATORZY INFORMACJI
Kierownicy podstawowych jednostek organizacyjnych, kierownicy jednostek organizacyjnych, osoby obejmujące samodzielne stanowiska w UMFC. Jako „właściciele" informacji (aktywów/zasobów informacyjnych – patrz pkt 7.1. niniejszej PBI) przetwarzanych w podległych im jednostkach zarządzają tymi, które zostały im powierzone i odpowiadają za ich ochronę w obrębie podległej im jednostki organizacyjnej, m.in.;

1. odpowiadają za poprawność merytoryczną danych gromadzonych w systemach teleinformatycznych i tradycyjnych w obrębie podległej im jednostki organizacyjnej;
2. odpowiadają za bezpieczeństwo przetwarzania danych osobowych i innych informacji w obszarze podległej im jednostki organizacyjnej;
3. wnioskują o nadanie lub odebranie uprawnień w zakresie podległej im jednostki organizacyjnej;
4. prowadzą inwentaryzację zasobów informacyjnych w podległych im jednostkach organizacyjnych;
5. zgłaszają wszelkie zauważone nieprawidłowości w pracy systemów teleinformatycznych ABS lub ABI/IOD w celu uniknięcia potencjalnych zagrożeń;
6. podejmują odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa;
7. nadzorują przestrzeganie zapisów polityk bezpieczeństwa, procedur, wewnętrznych regulacji przez podległych pracowników, w tym przeprowadzają kontrole przestrzegania zasad „czystego biurka" i „czystego ekranu" w obszarze podległej im jednostki organizacyjnej;
8. przedstawiają ABI/IOD uwagi i propozycje zmian do wdrożonych regulacji w obszarze bezpieczeństwa informacji w celu ich udoskonalenia.

6. BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

Władze Uczelni przykładają szczególną wagę, aby wyznaczone zadania realizowali kompetentni, świadomi swoich ról i odpowiedzialności pracownicy. Takie podejście ma na celu zminimalizowanie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów informacyjnych. Podstawowym i skutecznym sposobem realizacji tego celu jest przyjęcie w UMFC zgodnych z obowiązującym prawem praktyk uwzględniających obszar bezpieczeństwa informacji m.in. związanych z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonym procedurom rozwiązywania umów o pracę (przed zatrudnieniem – na etapie rekrutacji, podczas trwania umowy związanej z zatrudnieniem oraz po zakończeniu zatrudnienia). Niezwykle ważny jest też element szkoleń i ciągłego uświadamiania, rozwiązany systemowo i skierowany do wszystkich pracowników UMFC na każdym etapie zatrudnienia.

Dodatkowo Uczelnia zapewnia osobom mającym przypisane role w SZBI lub zajmującym stanowisko związane z bezpieczeństwem informacji specjalistyczne szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych w celu zapewnienia, podnoszenia i utrzymania kompetencji.

Forma i sposób szkoleń przeprowadzanych w UMFC z obszaru bezpieczeństwa informacji i ochrony danych osobowych zostały opisane w odrębnej procedurze.

6.1. PRZED ZATRUDNIENIEM

Zasady naboru kandydatów na wolne stanowiska w UMFC określają szczególne przepisy obowiązującego prawa. Szczegóły opisane zostały w odrębnej procedurze

Niedopuszczalne jest pozostawienie kandydata bez opieki pracownika w pomieszczeniach służbowych UMFC zarówno w trakcie trwania rozmowy lub testu kwalifikacyjnego jak i podczas ewentualnych przerw.

6.2. NA POCZĄTKU I W TRAKCIE ZATRUDNIENIA

Przystąpienie do wykonywania powierzonych obowiązków służbowych przez nowo zatrudnioną osobę musi zostać poprzedzone wstępnym szkoleniem z zakresu bezpieczeństwa informacji i ochrony danych osobowych oraz zapoznaniem z zapisami niniejszej Polityki Bezpieczeństwa Informacji oraz pozostałymi regulacjami wewnętrznymi UMFC z obszaru bezpieczeństwa informacji, w szczególności jeśli osoba posiada lub będzie posiadać dostęp do systemu teleinformatycznego Uczelni. Powyższe działania muszą zostać potwierdzone złożeniem pisemnego, zawierającego własnoręczny podpis oświadczenia przez nowo zatrudnionego pracownika.

Każda z osób, która będzie przetwarzała dane osobowe w Uczelni, bez względu na rodzaj ich przetwarzania, otrzymuje nadane przez ADO upoważnienie do przetwarzania danych osobowych w systemach teleinformatycznych oraz w tradycyjnych (papierowych). Upoważnienie do przetwarzania danych stanowi podstawę do nadania uprawnień w poszczególnych systemach teleinformatycznych użytkowanych w UMFC. Obieg wniosku o nadanie/zmianę/odbiór uprawnień do poszczególnych systemów teleinformatycznych został opisany w odrębnej procedurze.

W trakcie trwania zatrudnienia systematycznie budowana jest świadomość pracowników w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych, m.in. poprzez

informowanie o zmianach przepisów prawa w tym obszarze, organizowanie cyklicznych, okresowych szkoleń oraz doskonaleniem SZBI we współudziale administratorów informacji.

6.3. PO ZAKOŃCZENIU ZATRUDNIENIA

W przypadku ustania stosunku pracy z UMFC nadane pracownikowi upoważnienie do przetwarzania danych osobowych wygasa, a przyznane uprawnienia do systemów teleinformatycznych są niezwłocznie odbierane. „Rozliczenie" z posiadanych zasobów informacyjnych dotyczy również m.in. powierzonego do użytkowania sprzętu mobilnego, służbowych skrzynek mailowych oraz systemu kontroli dostępu do pomieszczeń UMFC.

Zobowiązania dotyczące zasad zapewnienia bezpieczeństwa informacji (np. zachowania ich w poufności) w innych umowach niż związanych ze świadczeniem pracy są egzekwowane w sposób przewidziany szczególnymi przepisami prawa.

7. ZARZĄDZANIE AKTYWAMI

Aktywa, to wszystkie zasoby informacyjne, które stanowią wartość dla Uniwersytetu Muzycznego Fryderyka Chopina. Należą do nich np. dane osobowe i inne informacje o studentach, teczki osobowe pracowników, Aby zapewnić im dostateczną ochronę w UMFC przeprowadza się okresowe inwentaryzacje posiadanych aktywów informacyjnych, w których określone zostają m.in. rodzaj i nazwa zasobu, jego właściciel, lokalizacja oraz stopień wrażliwości, który określa stopień ważności zasobu w celu zapewnienia stosownego poziomu jego zabezpieczenia.

Aktywa informacyjne aktywa chronione, zaangażowane w proces przetwarzania informacji:

1. aktywa materialne (fizyczne) –dokumenty, komputery stacjonarne, laptopy, pozostałe mobilne nośniki danych, serwery;
2. aktywa niematerialne – oprogramowanie, informacje w formie cyfrowej, bazy i zbiory danych, wiedza pracowników.

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub takie, które może wpłynąć w jakikolwiek sposób na bezpieczeństwo informacji powinno zostać zweryfikowane przez Dział Informatyczny pod kątem zgodności z wymaganiami systemu bezpieczeństwa informacji, a następnie dopiero dopuszczane do użytkowania – o ile spełni te wymagania.

7.1. WŁAŚCICIEL AKTYWÓW INFORMACYJNYCH

Właścicielem aktywów informacyjnych w UMFC są kierownicy podstawowych jednostek organizacyjnych, kierownicy jednostek organizacyjnych, osoby obejmujące samodzielne stanowiska jako administratorzy informacji (AI), ale również w szczególnych przypadkach mogą nimi być wskazani, konkretni pracownicy, w zależności od przydzielonych im zadań. Własność w rozumieniu systemu zarządzania bezpieczeństwem informacji nie oznacza prawa własności w rozumieniu zapisów kodeksu cywilnego, ale odnosi się do szczególnej odpowiedzialności za prawidłowe zarządzanie aktywem w całym cyklu jego życia, zgodnie z przyjętą zasadą „kaskadowej" odpowiedzialności za bezpieczeństwo informacji UMFC.

7.2. RODZAJE INFORMACJI PRZETWARZANYCH W UNIWERSYTECIE MUZYCZNYM FRYDERYKA CHOPINA

W oparciu o wymagania prawne wszystkie przetwarzane w UMFC informacje podzielone zostały na następujące grupy:

7.2.1. DANE OSOBOWE

Dane osobowe to informacje, które RODO definiuje, jako: "wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej".

Ochrona danych osobowych UMFC oparta jest m.in. na zapisach RODO, ustawy o ochronie danych osobowych, Polityce Bezpieczeństwa Danych Osobowych UMFC, przyjętych dobrych praktykach z tego obszaru. Za organizację systemu ochrony danych osobowych odpowiada ADO, za przestrzeganie przyjętych zasad ich ochrony odpowiada ABI/IOD. Dane osobowe przetwarzane w UMFC dotyczą m.in. studentów, doktorantów, nauczycieli akademickich, pracowników niebędących nauczycielami akademickimi, gości domów studenckich, osób związanych z wydawnictwem i in.

7.2.2. INFORMACJE NIEJAWNE

Ochrona informacji niejawnych odbywa się zgodnie z wymogami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Informacje niejawne posiadają własny, niezależny od definiowanego przez niniejszą PBI system ochrony zgodny z wymaganiami ustawy o ochronie informacji niejawnych. Za organizację systemu ochrony informacji niejawnych w UMFC odpowiada Pełnomocnik Rektora ds. Ochrony Informacji Niejawnych (dalej Pełnomocnik ds. OIN). Wszelkie procedury, zarządzenia, regulacje dotyczące obszaru informacji niejawnych dostępne są u Pełnomocnika ds. OIN.

7.2.3. INNE TAJEMNICE USTAWOWO CHRONIONE

Do tej grupy zostały przypisane informacje stanowiące m.in:

1. tajemnicę pracodawcy na podstawie ustawy z dnia 26 czerwca 1974 r. Kodeks pracy;
2. tajemnicę skarbową, którą objęte są indywidualne dane zawarte w deklaracji oraz innych dokumentach składanych przez podatników, płatników lub inkasentów na podstawie ustawy z dnia 29 sierpnia 1997 roku Ordynacja podatkowa;
3. tajemnicę lekarską zawartą w ustawie z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty;
4. tajemnicę adwokacją i radcowską określoną ustawą z dnia 6 czerwca 1997 r. Kodeks karny oraz ustawą z dnia 26 maja 1986 r. Prawo o adwokaturze;
5. tajemnicę autorską określoną ustawą z dnia 4 lutego1994 r. o prawie autorskim i prawach pokrewnych;
6. tajemnicę bankową zawartą w ustawie z dnia 29 sierpnia 1997 r. prawo bankowe oraz ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej, ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, ustawą z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji;
7. tajemnicę dziennikarską określoną w ustawie z dnia 26 stycznia 1984 r. Prawo prasowe oraz w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego;

8. tajemnicę handlową;
9. tajemnicę notarialną określoną w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, ustawą z dnia 14 lutego 1991 r. Prawo o notariacie;
10. tajemnicę przedsiębiorstwa określoną ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego oraz w ustawie z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego;
11. tajemnicę spowiedzi określoną w ustawie z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego oraz w ustawie 14 czerwca 1960 r. Kodeks postępowania administracyjnego;
12. tajemnicę statystyczną, o której mowa w ustawie z dnia 4 lutego 1994 r. o Prawie autorskich i prawach pokrewnych oraz w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego;
13. tajemnicę wynalazczą określoną w ustawie z dnia 4 lutego 1994 r. o Prawie autorskich i prawach pokrewnych;
14. tajemnicę ubezpieczeniową określoną w ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu;
15. tajemnicę śledztwa zawartą w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego;
16. tajemnicę żołnierzy zawodowych zawartą w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego;
17. tajemnicę korespondencji i komunikowania się określoną w Konstytucji z dnia 2 kwietnia 1997 r. Rzeczypospolitej Polskiej (Dz. U. 1997 Nr 78 poz. 483),
18. tajemnicę prokuratorską określoną w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego;
19. tajemnicę postępowania celnego określoną w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego oraz w ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej;
20. tajemnicę zawodową określoną w ustawie z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego.

7.2.4. INFORMACJE PUBLICZNE

Informacje publiczne to informacje, o których mowa w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej. Udostępnianie informacji publicznych, znajdujących się w posiadaniu UMFC następuje poprzez:

1. ogłaszanie informacji publicznych, w tym dokumentów urzędowych na stronie Biuletynu Informacji Publicznej UMFC;
2. udostępnianie na wniosek zainteresowanego, o ile nie została umieszczona w BIP UMFC;
3. wyłożenie lub wywieszenie w miejscach ogólnie dostępnych;
4. ustnie np. telefonicznie;

7.3. KLASYFIKACJA INFORMACJI

Wszelkie informacje przetwarzane w Uniwersytecie Muzycznym Fryderyka Chopina, które nie zostały oznaczone jako należące do osób trzecich, stanowią własność Uczelni i podlegają ochronie. W UMFC przyjęto ich klasyfikację i podzielone na: niejawne, chronione i publiczne.

1. Informacje niejawne – chronione są szczególnymi przepisami prawa (patrz podrozdział *7.2.2.*).
2. Informacje chronione – ze względu na ich poufność, integralność i dostępność.
3. Informacje publiczne – chronione są ze względu na ich integralność i dostępność.

Z uwagi na znaczną ilość wytwarzanych, przekazywanych i otrzymywanych dokumentów odstąpiono od oznaczania informacji chronionych i publicznych dodatkowymi klauzulami.

Klasyfikacja zasobów informacyjnych UMFC stanowi Załącznik nr 1 do niniejszej polityki.

8. KONTROLA DOSTĘPU

W celu skutecznej realizacji zasady uprawnionego dostępu w UMFC, dostęp do miejsc, urządzeń, systemów, w których informacje są przetwarzane jak i samej informacji jest kontrolowany.

8.1. KONTROLA DOSTĘPU DO POMIESZCZEŃ SŁUŻBOWYCH

Wszystkie pomieszczenia służbowe są zabezpieczane przed dostępem osób nieuprawnionych np. zamykane na klucz, zabezpieczone kartą dostępu lub zamkami szyfrowymi. Każdy pracownik odpowiada za powierzony mu klucz, kartę lub kod dostępu i nie może udostępniać go osobom trzecim.

Niedopuszczalne jest pozostawienie bez nadzoru w pomieszczeniu służbowym UMFC osób nieuprawnionych. Niedopuszczalne jest także pozostawienie niezabezpieczonego pomieszczenia służbowego w sytuacji, gdy nie znajdują się w nim osoby uprawnione.

8.2. KONTROLA DOSTĘPU DO OBSZARÓW CHRONIONYCH

Na terenie UMFC znajdują się wydzielone obszary lub pomieszczenia szczególnie chronione w związku z rodzajem informacji w nich przetwarzanych. Do obszarów tych zaliczają się m.in. Sekretariat Rektora, Prorektorów, Kanclerza, pomieszczenia zajmowane przez Dział Kadr i Płac, Informatyki, serwerownie, archiwa. Dostęp do wyżej wymienionych pomieszczeń chroniony jest za pomocą systemu kontroli dostępu, systemu alarmowego oraz osobnego zestawu zamków. Przebywanie w tym obszarze możliwe jest tylko w obecności upoważnionych pracowników.

Wykaz stref i pomieszczeń objętych kontrolą dostępu prowadzi i aktualizuje Kierownik Działu Administracyjno-Gospodarczego.

8.3. KONTROLA DOSTĘPU DO SIECI I SYSTEMÓW TELEINFORMATYCZNYCH

W UMFC jest sprawowany nadzór nad wszystkimi urządzeniami i systemami podłączanymi do sieci. Aby zapewnić dostateczną ochronę usług sieciowych przed nieautoryzowanym dostępem, każde urządzenie lub system podłączane do sieci musi spełniać określone wymagania.

Przed uzyskaniem dostępu do systemów teleinformatycznych wszystkie osoby wykonujące zadania na rzecz UMFC podpisują stosowne oświadczenie, w którym są zobowiązane do zachowania w tajemnicy informacji chronionych, natomiast pracownicy firm zewnętrznych

zobowiązani są do zachowania poufności stosownymi oświadczeniami zawartymi w umowach podpisywanych z podmiotami zewnętrznymi.

Szczegóły dotyczące wymagań dla urządzeń i systemów zostały opisane w Polityce Bezpieczeństwa Systemów Teleinformatycznych UMFC.

8.4. ZASADY NADAWANIA UPRAWNIEŃ

Szczegółowa procedura opisująca obieg wniosku o nadanie upoważnienia i uprawnień do systemów teleinformatycznych stanowi załącznik do PBDO UMFC.

8.5. ZASADA „CZYSTEGO BIURKA"

Wszystkie osoby wykonujące zadania na rzecz UMFC obowiązuje zasada „czystego biurka", która jest jednym ze sposobów zapobiegania nieautoryzowanemu dostępowi do informacji, jej utraty lub uszkodzenia, a także kradzieży środków do jej przetwarzania.

Zasada „czystego biurka" obejmuje zarówno dokumenty tradycyjne (papierowe) jak i przenośne nośniki pamięci. Wszelkie dokumenty, pieczęci, stemple, nośniki danych nie mogą pozostawać bez nadzoru, nawet w czasie nawet chwilowej nieobecności pracownika w pomieszczeniu służbowym. Dokumenty wadliwe muszą być niszczone jedynie w przeznaczonych do tego niszczarkach. Niedopuszczalne jest wyrzucanie dokumentów do kosza na śmieci.

Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników – wydrukowane lub skserowane dokumenty należy odbierać z podajnika urządzenia niezwłocznie. Nie powinny one pozostawać dostępne ani dla pracowników nieposiadających stosownych uprawnień ani dla interesantów lub innych osób „z zewnątrz".

Po zakończeniu pracy wszystkie dokumenty – a w szczególności te, które zawierają dane osobowe lub inne informacje prawnie chronione (np. akta osobowe, informacje o studentach, pieczęcie, stemple oraz mobilne nośniki danych) muszą być chowane do szaf lub szuflad zamykanych na klucz. Pomieszczenia zamyka się na czas nieobecności pracowników w sposób uniemożliwiający dostęp do nich przez osoby nieuprawnione (poza pomieszczeniami otwieranymi kartami dostępu).

Procedura przeprowadzania kontroli przestrzegania zasady „czystego biurka" opisana została w załączniku nr 2 do niniejszej PBI.

8.6. ZASADA „CZYSTEGO EKRANU"

Wszystkie osoby wykonujące zadania na rzecz UMFC, które otrzymują login do systemu teleinformatycznego obowiązuje zasada „czystego ekranu". Ma ona na celu zabezpieczenie przed nieautoryzowanym dostępem do systemów teleinformatycznych oraz przed ujawnieniem informacji chronionych, często w sposób niezamierzony i nieuświadomiony.

Zasada „czystego ekranu" oznacza stosowanie środków uniemożliwiających wgląd osobom trzecim (nieuprawnionym) do informacji widocznych na monitorze komputera, m.in. poprzez:

1. Każdorazowe odejście od stanowiska pracy powinno być poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu w sposób uniemożliwiający uzyskanie do niego dostępu,
2. Po zakończeniu pracy wszystkie aktywne aplikacje należy zamknąć a następnie wylogować się z systemu,
3. Monitor powinien być ustawiony w sposób uniemożliwiający osobom trzecim widok na jego zawartość,
4. Mobilne nośniki pamięci zewnętrznej muszą zostać zabezpieczone po zakończeniu pracy (schowane).

Szczegółowe wymagania zasady „czystego ekranu" zostały opisane w Regulaminie Użytkowników Systemów Teleinformatycznych, procedura przeprowadzania kontroli przestrzegania zasady „czystego ekranu" opisana została w załączniku nr 2 do niniejszej PBI.

9. ZABEZPIECZENIA KRYPTOGRAFICZNE

W celu zapewnienia poufności, autentyczności i integralności informacji w UMFC stosowane są zabezpieczenia kryptograficzne (szyfrujące) wszędzie tam, gdzie istnieje konieczność ich stosowania. Zastosowanie konkretnego narzędzia kryptograficznego jest poprzedzone oszacowaniem ryzyka pod kątem wyboru typu zabezpieczenia. Szczegółowe wymagania zostały opisane w odrębnych dokumentach.

10. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do UMFC wykorzystywane są wdrożone środki bezpieczeństwa fizycznego i środowiskowego m.in. system zamków i kontroli dostępu do pomieszczeń, system monitoringu wizyjnego, ochrona fizyczna budynku. W celu zabezpieczenia przed zagrożeniami zewnętrznymi i środowiskowymi kluczowe systemy techniczne i teleinformatyczne zostały wyposażone w systemy utrzymujące optymalne warunki środowiskowe oraz podtrzymujące zasilanie (UPS), a także opracowano praktyki i procedury postępowania w razie wystąpienia potencjalnych zagrożeń.

11. ZARZĄDZANIE SYSTEMEM I SIECIAMI

Władze Uczelni przykładają dużą wagę do przestrzegania zasad bezpieczeństwa związanych z utrzymywaniem i użytkowaniem systemów informatycznych oraz sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez ww. systemy informacji.

Skuteczna realizacja tego celu możliwa jest dzięki:

1. kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami wspomagającymi UMFC;
2. obowiązującym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
3. kontrolowaniu wprowadzania zmian do infrastruktury technicznej;

4. nadzorowaniu usług dostarczanych przez strony trzecie a w szczególności wszelkim wprowadzanym do nich zmianom. Plany zakupu lub wprowadzenia zmian do systemu uwzględniają wpływ nowych procesów na istniejący system bezpieczeństwa;
5. kontroli systemów - przed dopuszczeniem do użytkowania - pod kątem spełnienia standardów obowiązujących w UMFC;
6. wdrożonym zabezpieczeniom chroniącym przed złośliwym oprogramowaniem i złośliwym kodem mobilnym;
7. usystematyzowanemu tworzeniu i testowaniu kopii bezpieczeństwa;
8. przestrzeganiu opracowanych zasad postępowania z nośnikami;
9. bieżącemu monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów;
10. monitorowaniu poziomu incydentów w systemach informatycznych i odpowiedniej reakcji w przypadku ich wystąpienia.

Szczegółowe zasady zarządzania systemami i sieciami opisane zostały w dokumencie PBST.
Zasady postępowania z nośnikami informacji zostały opisane w załączniku nr 3 PBI.

11. ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

W UMFC zarządzanie zdarzeniami i incydentami związanymi z bezpieczeństwem informacji odbywa się w ramach procesu zarządzania incydentem.

Ogólne zasady zarządzania incydentem:

1. każdy zauważony incydent powinien zostać zgłoszony i zarejestrowany celem umożliwienia odpowiednim osobom właściwej reakcji na jego wystąpienie;
2. incydenty związane z bezpieczeństwem informacji należy zgłaszać zgodnie z ich źródłem – osobiście lub za pośrednictwem kierownika jednostki organizacyjnej do ABI/IOD lub Kierownika Działu Informatyki/Kierownika Działu Administracyjno-Gospodarczego, którzy podejmują niezwłoczne i adekwatne do zaistniałej sytuacji działania;
3. w przypadku wystąpienia klęski żywiołowej lub aktu terroru w pierwszej kolejności powiadamiane są właściwe służby (Policja/Pogotowie Ratunkowe/Straż Pożarna) a następnie ochrona budynku oraz Rektor i Kanclerz Uczelni. Postępowanie w poszczególnych sytuacjach kryzysowych regulują odrębne procedury;
4. w przypadku zauważenia próby włamania, kradzieży dokumentów lub sprzętu oraz wszelkich innych prób niszczenia mienia powiadamiana jest ochrona budynku oraz bezpośredni przełożony lub osoba go zastępująca i Władze Uczelni;
5. ochrona obiektu rejestruje incydenty we własnych dokumentach.

12. POSTANOWIENIA KOŃCOWE

Wszyscy pracownicy oraz osoby wykonujące zadania na rzecz Uniwersytetu Muzycznego Fryderyka Chopina na podstawie umowy innej niż umowa o pracę, a także personel firm

zewnętrznych zobowiązują się do zapoznania z niniejszą Polityką Bezpieczeństwa Informacji oraz dokumentami z nią związanymi.

W celu zapewnienia dostępności dokumentu Polityki Bezpieczeństwa Informacji została ona zamieszczona wraz z załącznikami w dysku sieciowym dostępnym dla wszystkich użytkowników UMFC.

Postępowanie naruszające zapisy Polityki Bezpieczeństwa Informacji stanowi naruszenie obowiązków pracowniczych i skutkuje sankcjami prawnymi przewidzianymi w Kodeksie Pracy oraz Regulaminie Pracy UMFC, a w przypadku podejrzenia popełnienia przestępstwa mogą mieć zastosowanie przepisy Kodeksu karnego.

12.1. ZGODNOŚĆ Z PRZEPISAMI PRAWA

Przyjęte zasady bezpieczeństwa informacji przedstawione w niniejszej PBI oraz w pozostałej dokumentacji składającej się na SZBI UMFC są zgodne z przepisami obowiązującego prawa, a także uwarunkowaniami umownymi i normatywnymi.

12.2. LISTA DOKUMENTÓW ZWIĄZANYCH

1. Statut UMFC;
2. Regulamin Organizacyjny UMFC;
3. Polityka Bezpieczeństwa Danych Osobowych UMFC;
4. Polityka Bezpieczeństwa Systemów Teleinformatycznych UMFC;
5. Regulamin Użytkowników Systemów Teleinformatycznych UMFC;
6. Polska norma PN-ISO/IEC 27000;
7. Polska norma PN-ISO/IEC 27001;
8. Polska norma PN-ISO/IEC 27002.

12.3. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 Klasyfikacja informacji UMFC,

Załącznik nr 2 Procedura dotycząca sposobu przeprowadzenia kontroli przestrzegania zasad „czystego biurka” i „czystego ekranu”,

Załącznik nr 3 Procedura dotycząca postępowania z nośnikami informacji.