Załącznik nr 3 do Zarządzenia Rektora nr 23/2018

Polityka Bezpieczeństwa Systemów Teleinformatycznych

Uniwersytetu Muzycznego Fryderyka Chopina

SPIS TREŚCI

1. WSTĘP

Polityka Bezpieczeństwa Systemów Teleinformatycznych Uniwersytetu Muzycznego Fryderyka Chopina (dalej PBST UMFC) jest wewnętrznym dokumentem związanym z Polityką Bezpieczeństwa Informacji Uniwersytetu Muzycznego Fryderyka Chopina, składającym się na dokumentację Systemu Zarządzania Bezpieczeństwem Informacji UMFC. PBST wraz z Regulaminem Użytkowników Systemów Teleinformatycznych UMFC tworzą tzw. Instrukcję Zarządzania Systemem Informatycznym, natomiast wraz z Polityką Bezpieczeństwa Danych Osobowych UMFC stanowią dokumentację mającą na celu zapewnienie ochrony danych osobowych przetwarzanych w UMFC.

Z PBST powinna być zapoznana kadra kierownicza oraz wszyscy pracownicy UMFC odpowiadający za systemy teleinformatyczne UMFC. Wszystkich pozostałych użytkowników systemów teleinformatycznych obowiązuje Regulamin Użytkowników Systemów Teleinformatycznych UMFC (dalej RUST), w którym zawarte są najważniejsze informacje dotyczące bezpieczeństwa systemów teleinformatycznych oraz podstawowych zasad ich użytkowania.

2. SŁOWNIK UŻYTYCH TERMINÓW I SKRÓTÓW

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

PBI – Polityka Bezpieczeństwa Informacji

PBST – Polityka Bezpieczeństwa Systemów Teleinformatycznych

RUST – Regulamin Użytkowników Systemów Teleinformatycznych

PBDO – Polityka Bezpieczeństwa Danych Osobowych

Autoryzacja (środków przetwarzania informacji) – zgodność urządzeń z minimalnymi wymaganiami w zakresie bezpieczeństwa

UMFC/Uniwersytet – Uniwersytet Muzyczny Fryderyka Chopina

Poufność informacji – zapewnienie, że informacje są dostępne tylko dla osób uprawnionych

Integralność informacji – zagwarantowanie dokładności i kompletności informacji oraz metod ich przetwarzania (zapewnienie, że dane nie zostały zmodyfikowane w nieautoryzowany sposób)

Dostępność informacji – zapewnienie, że dostęp do informacji mają osoby upoważnione zawsze wtedy, gdy istnieje taka potrzeba

System brzegowy – urządzenie zabezpieczające sieć wewnętrzną przed nieautoryzowanym dostępem z zewnątrz (firewall)

Podatność – potencjalne zagrożenie naruszenia bezpieczeństwa danych

Incydent – związany z bezpieczeństwem informacji – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia ciągłości działania i zagrażają bezpieczeństwu informacji

3. ORGANIZACJA BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

W celu zapewnienia prawidłowego zarządzania bezpieczeństwem informacji w systemach teleinformatycznych niezbędne jest wdrożenie właściwych procedur, z których będą wynikały zadania przypisane konkretnym osobom.

Przetwarzanie informacji w UMFC musi być wykonywane na urządzeniach zgodnych z minimalnymi wymaganiami w zakresie bezpieczeństwa – określonymi m.in. w rozporządzeniu 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 (Dz.U. z 2016 r. poz. 113, tj. z późn. zm.).*

W UMFC informacje przetwarzane są na urządzeniach dostosowanych do przyjętych standardów opisanych w odrębnej procedurze wg wzoru stanowiącego załącznik nr 1 do PBST.

Autoryzacja środków przetwarzania informacji obejmuje swoim zakresem wszystkie urządzenia teleinformatyczne: m.in. serwery, komputery, laptopy, urządzenia sieciowe. Kontakt z grupami zainteresowania bezpieczeństwem powinny utrzymywać wszystkie osoby związane z bezpieczeństwem oraz administracją systemami w jednostce organizacyjnej.

Bezpieczeństwo systemów teleinformatycznych podlega audytom wewnętrznym, niezbędne są również regularne, niezależne przeglądy bezpieczeństwa dotyczące wdrożonych zabezpieczeń, stosowania wdrożonych dokumentów, świadomości pracowników oraz innych aspektów związanych z bezpieczeństwem UMFC.

Dostęp podmiotów zewnętrznych do systemów teleinformatycznych musi być kontrolowany. Zagadnienie to regulują odpowiednie zapisy w umowach. Umowy ze stronami trzecimi dotyczące dostępu, przetwarzania, przekazywania lub zarządzania informacjami Uniwersytetu lub środkami przetwarzania informacji powinny obejmować stosowne zapisy z zakresu bezpieczeństwa informacji, a w tym celu Inspektor Ochrony Danych musi być uwzględniony w obiegu dokumentów przy wszystkich projektach umów.

4. BEZPIECZEŃSTWO DANYCH

Bezpieczeństwo danych, będących w posiadaniu UMFC jest związane z utrzymaniem ich poufności, integralności i dostępności. W celu zachowania wyżej wymienionych atrybutów informacji stosuje się środki bezpieczeństwa według zasady adekwatności.

W celu zapewnienia poufności stosuje się zabezpieczenia kryptograficzne oraz działania uświadamiające pracowników w zakresie m.in. zachowania tajemnicy pracodawcy, danych osobowych jak i informacji niejawnych.

Aby zachować dostępność danych w uzasadnionych przypadkach stosuje się podwojenie rozwiązań teleinformatycznych (rozwiązania klastrowe, redundancja łączy sieciowych, itp.) oraz nadmiarowość wykorzystywanych dysków (np. RAID5).

Dostęp do obszarów bezpiecznych (m.in. serwerowni, punktów dystrybucyjnych) jest kontrolowany, stosowane są fizyczne granice tych obszarów. Kontrola dostępu do pomieszczeń uregulowana jest odrębna procedurą.

W miejscach gdzie jest to konieczne stosuje się monitoring pomieszczeń. W obszarach bezpiecznych mogą przebywać tylko osoby upoważnione, pod nadzorem pracowników.

Za ochronę przed zagrożeniami zewnętrznymi i środowiskowymi odpowiadają wyznaczone jednostki organizacyjne.

Wykaz pomieszczeń i obszarów bezpiecznych prowadzony jest przez Dział Informatyki wg wzoru stanowiącego załącznik nr 2 do PBST.

5. BEZPIECZEŃSTWO ZARZĄDZANIA SYSTEMAMI TELEINFORMATYCZNYMI

5.1. BEZPIECZEŃSTWO PLIKÓW SYSTEMOWYCH

Instalacja oprogramowania wykonywana jest tylko i wyłącznie przez pracowników Działu Informatyki. Kody źródłowe aplikacji są przechowywane w pomieszczeniach bezpiecznych.

Zaleca się, aby dostęp do plików systemowych był kontrolowany, a projekty informatyczne były prowadzone zgodnie z PBST, w sposób zapewniający bezpieczeństwo. Dokłada się starań, aby uniknąć ujawnienia wrażliwych danych w środowiskach testowych. Niezbędne jest wykonywanie kopii bezpieczeństwa systemów teleinformatycznych, zasady wykonywania kopii zapasowych zostały opisane w odrębnej Procedurze.

5.2. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI

Sieć lokalna UMFC zarządzana jest w sposób zapewniający sprawną i bezawaryjną komunikację systemów. Urządzenia sieciowe stanowią jeden z elementów, który może być wykorzystany do przechwycenia informacji. Urządzenia sieciowe są monitorowane i konfigurowane w celu zmniejszenia zagrożenia bezpieczeństwa. Zarządzanie nimi odbywa się poprzez podłączenie się lokalnie do urządzenia oraz za pomocą dedykowanego oprogramowania.

Komunikacja z Internetem jest automatycznie monitorowana i logowana. Udostępnienie witryny zabronionej przez system brzegowy następuje po napisaniu pisemnego, uzasadnionego wniosku skierowanego do Administratora Danych Osobowych za pośrednictwem Kierownika Działu Informatyki.

5.3. KONTROLA DOSTĘPU DO SIECI

Dostęp do zasobów sieci wewnętrznej (m.in. dyski sieciowe) oraz systemów teleinformatycznych odbywa się na podstawie pisemnego wniosku. Procedury nadania/zmiany i odbioru uprawnień regulują odrębne procedury.

W UMFC stosowana jest separacja logiczna oraz fizyczna sieci wewnętrznych. Brzegowy system nadzorujący dostęp do sieci teleinformatycznej powinien posiadać funkcjonalność IDS/IPS. Serwery pocztowe powinny być chronione przez dedykowane rozwiązania przeciw niechcianej korespondencji (antyspam). W uzasadnionych przypadkach dopuszczalne jest wyznaczenie gniazd lub ustanowienie zabezpieczonej sieci wi-fi z dostępem do Internetu, z których można korzystać publicznie. Sieć w takich przypadkach musi zostać odizolowana fizycznie lub logicznie od sieci wewnętrznej oraz odłączana (likwidowana), gdy ustanie potrzeba korzystania z niej.

5.4. MONITORING

Dział Informatyki regularnie monitoruje wykorzystanie zasobów sprzętowych przez systemy. Do podstawowych elementów fizycznych, które są monitorowane, należą: pamięć dyskowa i operacyjna, przepustowość karty sieciowej, procesor, pod kątem wykorzystania tych zasobów. Na podstawie wykazanych tendencji Dział Informatyki przewiduje konieczność zwiększenia zasobów dla konkretnych systemów, o czym informuje władze UMFC. Dla systemów, których działanie ma decydujący wpływ na funkcjonowanie UMFC (tzw. usług krytycznych), stworzone są automatyczne alarmy, wyzwalane przy przekroczeniu dopuszczalnej wartości obciążenia. Wykaz systemów prowadzony jest i aktualizowany przez Dział Informatyki wg wzoru stanowiącego załącznik nr 3 do PBST.

W celu monitorowania działań niepożądanych w systemach, stosuje się następujące środki:

1. każdy krytyczny dla działalności jednostki organizacyjnej system posiada włączone logowanie zdarzeń związanych z bezpieczeństwem, co umożliwia identyfikację źródła zagrożenia. Pliki, w których przechowywane są zebrane logi podlegają archiwizacji;
2. logi systemowe są regularnie przeglądane. Szczególny nacisk jest położony na informacje płynące z procesów tworzenia kopii zapasowych oraz wszelkie anormalne informacje z innych systemów;
3. systemy podczas tworzenia logów oraz proces archiwizacji i ich przechowywania są zbudowane w sposób, który daje gwarancję zachowania bezpieczeństwa przed edycją i nieautoryzowanym dostępem;
4. w systemach jednostki organizacyjnej zegary urządzeń teleinformatycznych są zsynchronizowane;
5. każdy z krytycznych systemów posiada dziennik prowadzony w formie elektronicznej. W dzienniku systemu administrator odnotowuje istotne działania wykonywane w systemie oraz sytuacje nadzwyczajne.

6. KONTROLA DOSTĘPU DO SYSTEMÓW, USŁUG I DANYCH

6.1. ZABEZPIECZENIA KRYPTOGRAFICZNE

W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne (szyfrowanie). Zabezpieczenia kryptograficzne występują

między lokalizacjami. W uzasadnionych przypadkach tworzy się połączenia między lokalizacją a klientem mobilnym. Do wymienionych zabezpieczeń zaliczamy:

1. Tunele VPN.
2. Udostępnienie poczty elektronicznej oraz wybranych aplikacji poprzez protokół https.

Na przenośnych nośnikach danych (np. pendrive, laptop, tablet, smartfon) wprowadza się sukcesywne stosowanie zabezpieczeń kryptograficznych chroniące dane.

6.2. KONTROLA DOSTĘPU DO ZASOBÓW SYSTEMOWYCH

Kontrola dostępu do systemów realizowana jest poprzez odpowiednie procedury. Udostępnianie zasobów systemowych odbywa się według zasad opisanych w PBI. Użytkownicy otrzymują uprawnienia do systemów, danych i usług w zakresie zgodnym z zakresem ich czynności służbowych. Udzielanie dostępu do zasobów systemowych stron trzecich są regulowane na mocy umów między stronami lub wynikają z przepisów obowiązującego prawa.

Dostęp do systemów operacyjnych serwerów posiadają tylko administratorzy sieci. Użytkownicy mogą korzystać jedynie z wybranych usług świadczonych przez serwery na podstawie standardowych uprawnień.

Przydzielanie użytkownikom uprawnień administratora lokalnego odbywa się tylko w uzasadnionych przypadkach.

Korespondencja, którą przechowuje i dostarcza system pocztowy, jest własnością pracodawcy - UMFC. Pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli służbowych skrzynek pocztowych użytkowników.

6.3. DOSTĘP UŻYTKOWNIKÓW

Proces przydzielania hasła użytkownikowi odbywa się na zasadach opisanych szczegółowo w odrębnej wewnętrznej procedurze.

6.4. DOSTĘP ADMINISTRACYJNY

Administratorów Systemów Informatycznych obowiązują wszystkie zasady dotyczące użytkowników. O ile jest to możliwe, zaleca się wyłączanie bądź zmianę nazwy kont administracyjnych domyślnie wbudowanych w system. Uruchamianie usług bądź aplikacji w systemach wykonuje się poprzez logowanie się na konto z uprawnieniami użytkownika, stosując do wykonania zadania narzędzia tymczasowo podnoszące poziom uprawnień.

Hasła kont administracyjnych systemów zdeponowane są w zaklejonej kopercie i przechowywane w sejfie. Szczegółowy opis postępowania reguluje odrębna wewnętrzna procedura.

6.5. PRACA NA ODLEGŁOŚĆ

Urządzenia mobilne (np. telefon, laptop, tablet) należy użytkować zgodnie z postanowieniami RUST.

Zdalny dostęp do sieci wewnętrznej UMFC może nastąpić jedynie ze stacji, która posiada przynajmniej aktualne oprogramowanie antywirusowe. Prawo dostępu do zasobów informatycznych (zarówno danych jak i oprogramowania) UMFC poza siedzibami UMFC (dostęp zdalny VPN) normują odrębne procedury.

Połączenie z sieci publicznych do wewnętrznych systemów teleinformatycznych może odbywać się tylko poprzez komunikację zaszyfrowaną.

7. ZARZĄDZANIE ROZWOJEM SYSTEMÓW – W TYM ZARZĄDZANIE ZMIANAMI I KONFIGURACJĄ

7.1. WYMAGANIA BEZPIECZEŃSTWA DLA NOWYCH SYSTEMÓW

Budując nowe rozwiązania, należy uwzględnić aspekty bezpieczeństwa. Każdy nowy system powinien spełniać obowiązujące standardy bezpieczeństwa. Każdy nowy system, w którym przetwarzane są dane osobowe jest wdrażany przy uwzględnieniu roli Inspektora Ochrony Danych, przede wszystkim musi ten proces poprzedzać ocena skutków.

7.2. ZARZĄDZANIE ZMIANAMI

Wprowadzanie zmian oraz szczegółowy sposób postępowania podczas incydentu zostały szczegółowe opisane w odrębnych wewnętrznych procedurach.

8. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

Zarządzanie ciągłością działania jest kluczowym elementem dla działania organizacji. Należy rozważyć wszystkie możliwe do zastosowania środki podnoszące dostępność systemów.

W przypadku kopiowania na taśmy magnetyczne należy stosować się do zaleceń producenta w zakresie eksploatacji, a w szczególności czasu żywotności.

Konfiguracja systemów wymagających wysokiej dostępności musi uwzględniać redundancję wszystkich elementów systemu.

W celu zachowania ciągłości działania podczas awarii zasilania, serwerownie są podłączone do systemu podtrzymania zasilania. System podtrzymania zasilania powinien utrzymywać konieczne napięcie do czasu włączenia zasilania z zapasowego źródła lub wyłączenia urządzeń.

Aby zachować ciągłość obsługi systemów stosuje się zastępstwa. System powinien mieć zapewnioną obsługę przez kompetentnego administratora z wymaganymi uprawnieniami systemowymi.

Procedury awaryjnego odtwarzania powoływane przez Polityki Bezpieczeństwa poszczególnych Systemów Informatycznych powinny być testowane minimum raz na 6 miesięcy.

Zewnętrzne nośniki danych z kopiami zapasowymi przechowywane są w dwóch miejscach uniemożliwiających jednoczesne zniszczenie wszystkich kopii. Kopie zapasowe na zewnętrznych nośnikach danych przechowywane są w ognioodpornych sejfach.

9. ZASADY ROZPOWSZECHNIANIA DOKUMENTU PBST ORAZ TRYB WPROWADZANIA ZMIAN

Aktualizacja niniejszego dokumentu dokonywana jest przynajmniej raz w roku. Za przegląd i aktualizację odpowiedzialny jest ABS. Podział ról i obowiązków w zakresie bezpieczeństwa teleinformatycznego opisany został w PBI.

10. POSTANOWIENIA UZUPEŁNIAJĄCE

10.1. ODSTĘPSTWA OD REGUŁ OCHRONY

W uzasadnionych przypadkach dopuszcza się odstąpienie od przyjętej PBST. Aby postępować inaczej niż przewidują reguły ochrony należy:

1. postępować zgodnie z wymogami obowiązującego prawa;
2. ustalić osobistą odpowiedzialność osoby, nie stosującej się do przyjętych zasad bezpieczeństwa;
3. uzasadnić pisemnie powód odstąpienia od przyjętych zasad bezpieczeństwa;
4. odstępując od przyjętych zasad, starać się zachować możliwie jak najwięcej z obowiązujących.

Zabrania się stosowania precedensu w celu zmiany przyjętych reguł. O odstąpieniu od przewidzianych reguł bezpieczeństwa decydować może jedynie Rektor UMFC lub osoby przez niego upoważnione.

10.2. NADZÓR NAD PRZESTRZEGANIEM PBST W UMFC

Nadzór nad przestrzeganiem PBST oraz dokumentów związanych z bezpieczeństwem teleinformatycznym pełni Administrator Bezpieczeństwa Systemów.

Postępowanie niezgodne z niniejszą PBST wiąże się z konsekwencjami, przewidzianymi w Regulaminie Pracy.

10.3. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 Standard wyposażenia stanowiska pracy w sprzęt teleinformatyczny (wzór)

Załącznik nr 2 Wykaz pomieszczeń i obszarów bezpiecznych (wzór)

Załącznik nr 3 Wykaz systemów, oprogramowań i aplikacji (wzór)

Załącznik nr 4 Procedura dostępu do serwerowni

Załącznik nr 5 Polityka wymiany sprzętu

Załącznik nr 6 Procedura tworzenia, testowania i wykorzystania kopii bezpieczeństwa

Załącznik nr 7 Polityka haseł i tworzenia kont w systemach teleinformatycznych

Załącznik nr 8 Polityka przechowywania haseł

10.4. WYKAZ DOKUMENTÓW ZWIĄZANYCH

1. Polityka Bezpieczeństwa Informacji UMFC,
2. Polityka Bezpieczeństwa Danych Osobowych UMFC,
3. Regulamin Użytkowników Systemów Teleinformatycznych UMFC.

Załącznik nr 1

STANDARD WYPOSAŻENIA STANOWISKA PRACY

W SPRZĘT TELEINFORMATYCZNY

W Uniwersytecie Muzycznym Fryderyka Chopina wykorzystywany jest sprzęt komputerowy wg poniższego podziału:

Stanowisko	Komputer	Drukarka (urządzenie wielofunkcyjne)	Oprogramowanie

Oprogramowanie standardowe:

Oprogramowanie standardowe dla Działu Kadrowo-Płacowego:

Oprogramowanie standardowe dla Działu Finansowo-Księgowego:

Oprogramowanie standardowe Wydziałów Dydaktycznych:

Urządzenia opcjonalne:

Oprogramowanie opcjonalne:

Załącznik nr 2

do PBST UMFC

WYKAZ POMIESZCZEŃ I STREF BEZPIECZNYCH BĘDĄCYCH W UŻYTKOWANIU DZIAŁU INFORMATYKI UNIWERSYTETU MUZYCZNEGO FRYDERYKA CHOPINA

Lp.	Lokalizacja	Numer pomieszczenia/oznaczenie strefy	Uwagi

Załącznik nr 3

do PBST UMFC

PROCEDURA DOSTĘPU DO SERWEROWNI

UNIWERSYTETU MUZYCZNEGO FRYDERYKA CHOPINA

Procedura ma zastosowanie do pracowników Działu Informatyki UMFC oraz wszystkich osób współpracujących z Działem Informatyki (trzecich), które muszą swoje zadania wykonać w serwerowniach. Nad prawidłowym wykonywaniem niniejszej procedury nadzór sprawuje Kierownik Działu Informatyki.

WYKAZ POMIESZCZEŃ SERWEROWYCH

1. W budynku przy ul. Okólnik 2 w Warszawie – pomieszczenie nr 130 i 131
2. W budynku przy ul. Kawaleryjskiej 5 w Białymstoku – pomieszczenie nr 204

ZASADY

Pomieszczenia techniczne powinno być zabezpieczone elektronicznie. W pomieszczeniu technicznym można przebywać tylko w wyjątkowych sytuacjach oraz w czasie wykonywania rutynowych obowiązków związanych z infrastrukturą.

Dostęp do kluczy do serwerowni mają:

- Rektor, Prorektorzy, Kanclerz – na każde żądanie;
- Pracownicy Działu Informatyki – stale.

Nieograniczony dostęp do pomieszczeń technicznych mają:

- Rektor, Prorektorzy, Kanclerz;
- Pracownicy Działu Informatyki;

Osoby trzecie (np. pracownicy firm zewnętrznych wykonujących czynności serwisowe) mogą przebywać w serwerowni tylko w obecności pracownika Działu Informatyki (w godzinach pracy UMFC). W przypadku konieczności wykonania zadań poza godzinami pracy UMFC potrzeba taka powinna zostać zgłoszona wcześniej, praca może być wykonywana jedynie w obecności pracownika Działu Informatyki. Zapasowe klucze do serwerowni dostępne są na portierni.

SPOSOBY ZABEZPIECZANIA POMIESZCZEŃ SERWEROWNI

1. Zabezpieczenie mechaniczne oraz – w przypadku dostępności – zabezpieczenie elektroniczne.