Zarządzenie nr 46/2022
Rektora Akademii Teatralnej im. Aleksandra Zelwerowicza
z dnia 30 grudnia 2022 roku

w sprawie zmiany Zarządzenia nr 51/2021 z dnia 22 grudnia 2021 r. wprowadzającego Politykę ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie

Na podstawie art. 23 ust. 1 i ust. 2 pkt 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2022, poz. 574 z późn. zm.) oraz § 12 ust 1 i 2 Statutu Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie, postanawiam co następuje:

§ 1

W Załączniku nr 1 do Zarządzenia, tj. *Polityce ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie* wprowadza się następujące zmiany:

1. § 4 ust. 4 otrzymuje następujące brzmienie: *Upoważnienie może być przyznane na czas określony lub do odwołania (wzór upoważnienia oraz odwołania upoważnienia znajduje się odpowiednio w **Załączniku nr 4 oraz 4a**). Osoba otrzymująca upoważnienie do przetwarzania danych osobowych jest zobowiązana podpisać Oświadczenie o zachowaniu poufności Przetwarzanych Danych Osobowych (wzór oświadczenia znajduje się w **Załączniku nr 5**). Proces powyższy realizowany jest według Procedury nadawania upoważnień znajdującej się w **Załączniku nr 3.** Dopuszcza się elektroniczne wnioskowanie o nadanie upoważnienia*.
2. § 17 ust. 1 w otrzymuje następujące brzmienie: *Integralną częścią niniejszej Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie są **Załączniki*.**

§ 2

W Załączniku nr 1 do *Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie*, tj. do *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie* wprowadza się następujące zmiany:

1. Dodaje się § 11^1, w następującym brzmieniu:

§11^1
Zasady zabezpieczenia sieci teleinformatycznej przed nieautoryzowanym dostępem

1) ASI odpowiedzialny jest za zabezpieczenie sieci teleinformatycznej przed nieautoryzowanym dostępem z uwzględnieniem poniższych zasad:
   a. ochronę sieci kablowej przed nieautoryzowanym dostępem;
   b. odłączanie nieużywanych gniazd;
   c. zablokowanie nieużywanych portów na przełączniku;
   d. blokowanie portów na podstawie Mac adresu urządzenia;
   e. stosowanie sprawnego, z aktualnym oprogramowaniem firewall'a;
   f. udostępniania sieci z zewnątrz tylko za pośrednictwem VPN w każdym uzasadnionym przypadku;
   g. Ochrona antywirusowa na komputerach;
   h. Stosowania sprawdzonych polityk bezpieczeństwa w zakresie dostępu do zasobów sieciowych dla Użytkowników;
   i. Zabezpieczenie dostępu Wi-Fi przez odpowiedni protokół zabezpieczenia sieci i szyfrowanie. W przypadku użytkowników domowych zalecane jest stosowanie protokołu WPA2 Personal z szyfrowaniem AES oraz WPA3. Nie są zalecane protokoły WPA z szyfrowaniem TKIP i WPA-PSK;
   j. regularną zmianę domyślnego hasła administratora, zalecana jest również zmiana loginu;

k. *usuwanie naklejki z hasłem z routera;*
l. *wyłączenie funkcji WPS – czyli Wi-Fi Protected Setup;*
m. *aktualizowanie oprogramowania routera;*
n. *filtrowanie adresów MAC (Media Access Control);*
o. *zainstalowanie oprogramowania antywirusowego na komputerach podłączonych do sieci WiFi, co pomoże zabezpieczyć przed kradzieżą hasła WiFi;*
p. *zmniejszenie zasięgu Wi-Fi – jeśli w ustawieniach routera możliwe jest ograniczenie zasięgu sieci, tak, żeby nie mogli z niej korzystać osoby postronne;*
q. *upewnienie się że sieć nie zawiera nieautoryzowanych punktów dostępowych (ang. rogue access point);*
r. *zablokowanie zdalnego dostępu do routera*.

2. Dodaje się § 11^2, w następującym brzmieniu:

§11^2
Zabezpieczenie stron internetowych administrowanych przez ADO
Podmiot, któremu powierzono stworzenie lub aktualizację strony internetowej zobowiązywany jest do monitorowania i testowania serwisu internetowego pod względem występowania podatności na naruszenie bezpieczeństwa. Administrator wprowadza do umów z podmiotami, którym powierzono aktualizację strony internetowej zapisy o odpowiedzialności za monitorowanie i testowanie serwisu internetowego pod względem występowania podatności wystarczające do jej prawidłowego i bezpiecznego funkcjonowania. Odpowiedzialnym za monitoring i testowanie serwisu jest podmiot, któremu powierzono aktualizację strony internetowej, za umieszczenie odpowiednich zapisów w umowie odpowiedzialny jest ADO.

3. Dodaje się § 11^3, w następującym brzmieniu:

§11^3
Zawieranie umów serwisowych IT

Przy zawieraniu umów z podmiotami zewnętrznymi na świadczenie usług serwisowych lub dotyczących obsługi systemów informatycznych należy:
a) dokonać oceny konieczności zawarcia umowy powierzenia danych osobowych;
b) w przypadku powierzenia przetwarzania danych osobowych przeprowadzić ocenę wybranego podmiotu pod kątem stosowanych zabezpieczeń;
c) wprowadzać bezwzględnie zapisy dotyczące poufności;
d) w miarę możliwości i potrzeby wprowadzić do zapisów umów kary umowne lub inne zabezpieczenia prawne umożliwiające dochodzenie roszczeń z tytułu naruszenia poufności lub bezpieczeństwa.

4. Dodaje się § 14^1, w następującym brzmieniu:

§14^1
Zasady przeprowadzania zmian, aktualizacji oprogramowania dla zapewnienia bezpieczeństwa informacji
1) *W celu wprowadzania zmian w systemach teleinformatycznych dokonuje się aktualizacji jego części składowych w tym w szczególności oprogramowania.*
2) *Aktualizacje polegają m.in. na wprowadzeniu do systemu poprawek, uaktualnień, nowych funkcjonalności, a także zagwarantowania większego bezpieczeństwa i odporności systemów teleinformatycznych.*
3) *Administrator wprowadzając aktualizacje, kieruje się przede wszystkim następującymi celami:*

a) *utrzymaniem wsparcia producenta;*
b) *naprawa błędów w oprogramowaniu.*
c) *ochrona przed złośliwym oprogramowaniem.*
d) *ochrona przed kradzieżą tożsamości*
e) *naprawianiem luk w zabezpieczeniach;*
f) *uzupełnianie funkcjonalności lub ich rozwój, w celu umożliwienia wykonywania nowych zadań*
g) *lepszej ochrony zasobów przed niepożądanymi działaniami i atakami.*

4) *Aktualizacje oprogramowania w zakresie ochrony zasobów oraz naprawy luk w zabezpieczeniach należy robić możliwie szybko po ukazaniu się stosownej poprawki.*
5) *Przeprowadzając aktualizację uwzględnia się, że poprawki mogą nie być wszechstronnie przetestowane, a co za tym idzie mogą powodować nieprzewidziane zachowanie systemu teleinformatycznego lub oprogramowania. W związku z powyższym przed aktualizacją należy przygotować sobie ścieżkę powrotu do stanu sprzed aktualizacji:*
   a) *przejrzeć fora w poszukiwaniu opinii o implementacji konkretnej poprawki;*
   b) *wykonać pełną kopię systemu, zabezpieczyć dane;*
   c) *o ile to możliwe, wykonać aktualizację na środowisku testowym;*
   d) *monitorować zachowanie systemu po wykonaniu aktualizacji.*

5. Dodaje się § 15[1], w następującym brzmieniu:

§15[1]
Rodzaje naruszenia bezpieczeństwa systemu informatycznego („incydenty")

1) ADO w celu szybkiego identyfikowania zagrożenia oraz skutecznego reagowania na incydenty wprowadza definicje i typowy sposób reagowania na naruszenia bezpieczeństwa systemu informatycznego oraz ich oznaczenie. Na podstawie wagi incydentu, a w przypadkach nieudanych prób naruszenia bezpieczeństwa, także na podstawie częstotliwości zagrożenia ich występowania podejmowane są decyzje co do stosowanych rozwiązań zabezpieczających.

2) Incydenty dzieli się na:
   a) *incydenty Cyber;*
   b) *incydenty IT*
   c) *incydenty RODO*

3) Przez naruszenie bezpieczeństwa systemu informatycznego typu cybernetycznego – Cyber - rozumie się naruszenie bezpieczeństwa skutkujące niedostępnością zasobu/serwisu lub nieautoryzowany dostęp do systemu informatycznego. Źródłem takich incydentów jest najczęściej atak pochodzący z sieci internetowej, rzadziej działanie pracownika. Jeżeli w ich wyniku narusza się bezpieczeństwo danych osobowych, incydent taki kwalifikuje się i ocenia również pod kątem przepisów RODO.

4) W przypadku wystąpienia naruszenia bezpieczeństwa systemu informatycznego oznacza się go jako naruszenie typu „Cyber", wskazując dodatkowo jaki typ naruszenia bezpieczeństwa zaistniał uwzględniając podtypy wskazane w pkt. 5) poniżej. Jeżeli incydent dotyczy danych osobowych incydent oznacza się dodatkiem „RODO".

5) Podtypy incydentów Cyber oraz działań podejmowanych w odpowiedzi na nie:
   a) ***Malware[1].*** *Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie systemu antywirusowego oraz regularne aktualizowane oprogramowania.*
   b) ***Man in the Middle***[2]*. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to*

[1] zbitka wyrazowa pochodząca od wyrażenia malicious software („złośliwe oprogramowanie"). Wspólną cechą programów uznawanych za malware jest fakt, że wykonują działania na komputerze bez jego zgody i wiedzy użytkownika, na korzyść osoby postronnej.
[2] od sformułowania „człowiekiem pośrodku", jest to typ ataku w ramach którego w transakcji lub korespondencji między dwoma podmiotami

zapewnienie aktualności certyfikatu bezpieczeństwa i szyfrowanie transmisji danych.

c) ***Cross-site scripting***[3]*. Typ działań podejmowanych w odpowiedzi na podtyp incydentu: najskuteczniejszym sposobem reakcji jest korzystanie z zaufanego oprogramowania oraz dobrego programu antywirusowego.*

d) ***Phishing***[4]*. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to budowanie świadomości wśród użytkowników oraz edukacja.*

e) ***DDoS*** *(distributed denial of service)*[5]*. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to filtrowanie ruchu dzięki dobrze skonfigurowanemu firewallowi u dostawcy usług internetowych, stosowaniu monitoringu oraz metody honeypot.*

f) ***SQL Injection***[6]***.*** *Typ działań podejmowanych w odpowiedzi na podtyp incydentu to odpowiednie zabezpieczenia na poziomie bazy danych.*

g) ***Ransomware***[7]***.*** *Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie aktualnego oprogramowania antywirusowego oraz dokonywanie regularnych aktualizacji systemu.*

h) ***Malvertising***[8]*. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie filtrów blokujących reklamy oraz współpraca z zaufanymi dostawcami;*

i) ***Atak siłowy*** *(brute force)*[9]*. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie odpowiednio mocnych haseł przy czym długość hasła powinna być wyznacznikiem jego siły.*

6) incydenty IT, to zdarzenia, występujące w sieci lokalnej i dzieli się je na trzy grupy:

a) *awarie sprzętowe, wadliwy sprzęt, przestarzałe i wyeksploatowane urządzenia, przepięcia w sieci zasilającej, klęski żywiołowe.*

b) *awarie oprogramowania będące skutkiem błędów oprogramowania, których nie wyeliminował producent*

c) *błędy użytkownika jako działania celowe lub przypadkowe wynikające z nieumiejętności obsługi, pomyłki.*

7) Incydenty typu RODO to incydenty Cyber oraz IT jeżeli w ich wyniku narusza się bezpieczeństwo danych osobowych.

8) W celu analizy i zbiorczego zarządzania incydentami odnotowuj ilość i rodzaj incydentów w systemach teleinformatycznych odnotowuje się w okresowych sprawozdaniach i mogą być odnotowywane na podstawie wzoru Załącznika nr 2 do niniejszej Instrukcji lub za pomocą formularza elektronicznego. Incydenty RODO odnotowuje się dodatkowo zgodnie z procedurą wskazaną w Załączniku nr 7 do Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie. Okresowo (raz na 6 miesięcy lub częściej w razie potrzeby) przeprowadza się ich zbiorczą analizę.

(na przykład sklepem internetowym i klientem) bierze udział osoba trzecia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych. Celem może być również podsłuchanie poufnych informacji oraz ich modyfikacja.

[3] jest to atak, który polega na umieszczeniu na stronie internetowej specjalnego kodu, który może skłonić ich do wykonania działania, którego nie planowali.

[4] atak polegający na próbie pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw.

[5] atak hakerski, mający na celu sparaliżowanie systemu komputerowego albo sieci, poprzez wysłanie sporej ilości zapytań do konkretnego systemu.

[6] atak tego rodzaju polega na uzyskaniu nieuprawnionego dostępu do bazy danych poprzez lukę w zabezpieczeniach aplikacji, na przykład systemu do obsługi handlu internetowego.

[7] celem ataku jest zaszyfrowanie danych użytkownika, a następnie ponowne ich udostępnienie w zamian za opłatę.

[8] atak poprzez użycie nośnika jakim są reklamy internetowe wyświetlane poprzez sieci takie jak Google Adwords. Poprzez reklamy może być zainstalowane złośliwe oprogramowanie na komputerze.

[9] atak opiera się on na niskim poziomie bezpieczeństwa haseł używanych przez pracowników i polega na generowaniu losowych haseł do momentu znalezienia pasującego

6. § 17 otrzymuje następujące brzmienie:

§17

Postanowienia końcowe

1. *W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.*
2. *Każda osoba upoważniona do przetwarzania danych osobowych jest zapoznawana przed dopuszczeniem do przetwarzania danych z niniejszą Instrukcją oraz składa pisemne oświadczenie, potwierdzające znajomość jej treści.*
3. *Niezastosowanie się do procedur określonych w niniejszej Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.*
4. *ASI odnotowuje wykonane prace i przeglądy dotyczące działań podejmowanych w strukturze teleinformatycznej odzwierciedlający wykonanie w danym miesiącu prace, a także okresowe przeglądy systemu zgodnie z harmonogramem wynikającym z przyjętych dokumentów w tym zakresie. Okresowe sprawozdania mogą być odnotowywane na podstawie wzoru Załącznika nr 2 do niniejszej Instrukcji lub za pomocą formularza elektronicznego.*
5. *ASI opracowuje i aktualizuje także dodatkową dokumentację (która może być prowadzona elektronicznie lub możliwa do sporządzenia ad hoc na podstawie wyciągów z systemów informatycznych i oprogramowania) której podstawie można określić aktualną i kompletną:*
    a) *dokumentacje architektury sieci oraz inwentaryzacja linii telekomunikacyjnych;*
    b) *ewidencje sprzętu i oprogramowania służącego do przetwarzania informacji przekazywanego pracownikowi*
    c) *wykaz użytkowników systemów teleinformatycznych wraz z nadanymi uprawnieniami;*
    d) *ewidencje aplikacji, do których niezbędne jest nadanie uprawnień dodatkowych;*
    e) *wykaz dopuszczonego do użytkowania oprogramowania systemowego i niesystemowego zawierający m.in. informacje o wsparciu przez producenta.*
6. *W odniesieniu do uprawnień do systemu informatycznego na poziomie domeny, aplikacji lub podobnym, przeprowadza się przegląd uprawnień w celu wykrycia nieprawidłowości, w tym nadmiarowych uprawnień lub wykrycia nieaktywnych kont pracowników z aktywnym dostępem raz na 6 miesięcy. Przeglądu dokonuje ASI na podstawie przesłanej przez ADO listy aktualnych pracowników jednostki.*
7. *Kierownik jednostki zarządza raz do roku audyt w zakresie bezpieczeństwa informacji zgodnie z wymogami § 20 ust. 2 pkt. 14 rozporządzenia KRI.*

§ 3

Wprowadza się nowy wzór Załącznika nr 2 do *Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie*, tj. wzór raportu stanu infrastruktury teleinformatycznej:

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym

- W Z Ó R –

Data sporządzenia raportu ……

Stan struktury teleinformatycznej
na miesiąc …… 202….roku

DZIENNIK ASI
Akademia Teatralna im. A. Zelwerowicza w Warszawie

Liczba awarii krytycznych:
Liczba zgłoszeń standardowych (w tym usterki i wsparcie techniczne użytkowników):
Prace administracyjne:
Status backupów:
Dodatkowe prace wdrożeniowe:
Zgłoszone incydenty ochrony danych (PROTOKÓŁ AWARII/INCYDENTU):
Testy kopii zapasowych (styczeń/sierpień):
Nadane/odebrane uprawnienia do systemu:
Skanowanie systemu po zgłoszeniu działania szkodliwego oprogramowania:
Odtworzenie z kopii zapasowej:
Aktualizacja listy oprogramowania:
Protokół zniszczenia nośnika:
Planowy przegląd systemu informatycznego (grudzień):
Przegląd logów systemowych (marzec, czerwiec, wrzesień, grudzień)

…….....
Podpis ASI

§ 4

Wprowadza się nowy Załącznik nr 4a do *Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie*, tj. wzór odwołania Upoważnienia do Przetwarzania Danych Osobowych:

Załącznik nr 4a do Polityki ochrony informacji oraz danych osobowych

- W Z Ó R –

Odwołanie Upoważnienie numer […] do Przetwarzania Danych Osobowych

Niniejszym odwołuję upoważnienie do przetwarzania danych osobowych

Pani/Pana

……...

zatrudnioną/ego na stanowisku

……..

(od ……...)

i zobowiązuję do niezwłocznego zaprzestania ich przetwarzania.

Warszawa, dnia …….. r.

.....

podpis osoby upoważnionej do nadawania upoważnienia

……..…..

podpis ADO lub osoby wyznaczonej przez ADO

§ 5

Załącznik nr 13 do *Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie*, tj. S*pis obowiązujących rejestrów, ewidencji, lis i innych dokumentów sporządzonych w jednostce w zakresie przetwarzania danych osobowych* otrzymuje brzmienie:

Załącznik nr 13 do Polityki ochrony danych osobowych

SPIS OBOWIĄZUJĄCYCH REJESTRÓW, EWIDENCJI, LIST I INNYCH DOKUMENTOW SPORZĄDZONYCH W JEDNOSTCE W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

Lista aktualna na dzień: […]

Rejestry oraz listy (ewidencje) prowadzone przez IOD na podstawie Polityki ochrony danych osobowych:

Podstawowe rejestry i listy:

1. *Rejestr czynności przetwarzania danych osobowych (obejmującym wykaz zbiorów oraz oprogramowanie do jego przetwarzania);*
2. *Rejestr kategorii przetwarzania danych osobowych (brak zdarzeń uzasadniających konieczność prowadzenia na dzień aktualności niniejszej listy)*
3. *Lista (ewidencja) osób upoważnionych do przetwarzania danych prowadzona na podstawie procedury nadawania upoważnień;*
4. *Lista (ewidencja) obowiązków informacyjnych prowadzona na podstawie procedury udzielania informacji podanej w przypadku pozyskiwania danych wraz z treścią obowiązków informacyjnych;*
5. *Lista umów powierzenia prowadzona na podstawie Polityki ochrony danych osobowych;*
6. *Lista (ewidencja) miejsc przetwarzania danych osobowych wraz z zabezpieczeniami prowadzona na podstawie Polityki ochrony danych osobowych.*
7. *Lista incydentów realizowana na podstawie procedury reagowania i oceny naruszeń bezpieczeństwa danych.*

Dokumenty uzupełniające:

8. *Szkolenie stanowiskowe – dokument aktualizowany w miarę potrzeb przez IOD w uzgodnieniu z ADO;*
9. *Wzór umowy powierzenia przetwarzania danych osobowych;*
10. *Analizy prawne zagadnień opiniowanych przez IOD w tym konieczności prowadzenia określonych rejestrów;*
11. *Instrukcja wraz z Oświadczeniem i obowiązkiem informacyjnym COVID – widownia Teatru;*
12. *Specyfikacja techniczna zawierająca wymagania minimalne dla systemów informatycznych;*
13. *Zarządzeniem Rektora nr 1/2019 z dnia 3 stycznia 2019 ZASADY DOSTĘPU DO UCZELNI OSÓB NIEPOSIADAJĄCYCH KARTY DOSTĘPOWEJ DO BUDYNKU AKADEMII TEATRALNEJ.*

Dokumenty sporządzane okresowo:

14. *Plan sprawdzeń – dokument aktualizowany corocznie przez IOD w uzgodnieniu z ADO – raz do roku wraz z notatkami ze sprawdzenia;*

15. *Plan szkoleń – dokument aktualizowany corocznie przez IOD w uzgodnieniu z ADO – raz do roku;*
16. *Całościowa analiza ryzyka przetwarzania danych osobowych – raz na dwa lata – dotyczy całości przetwarzania danych osobowych.*

Dokumenty do wdrożenia w przypadku wystąpienia zdarzenia uzasadniającego ich prowadzenie:

17. *Lista realizacji uprawnień (wniosków) osób, których dane są przetwarzane prowadzona na podstawie procedury realizowania uprawnień osób, których dane są przetwarzane (brak zdarzeń uzasadniających konieczność prowadzenia na dzień aktualności niniejszej listy);*
18. *Lista realizacji wniosków o udostępnienie danych osobowych (brak zdarzeń uzasadniających konieczność prowadzenia na dzień aktualności niniejszej listy).*

§ 6

1. Pozostałe postanowienia Zarządzenia nr 51/2021 z dnia 22 grudnia 2021 roku pozostają bez zmian.
2. Ujednolicony tekst Zarządzenia zawarty jest w Załączniku nr 1.

§ 7

Zmiany wchodzą w życie z dniem 1 stycznia 2023 roku.

REKTOR

/- / Prof. dr hab. Wojciech Malajkat