TEATR im. H. CH. ANDERSENA
20-037 Lublin, ul. Aleje Racławickie 8/22B
tel. 81 532 16 28, fax 81 534 36 11
NIP 712-010-37-46

Zarządzenie Nr 11 /2017
Dyrektora Teatru im. H. Ch. Andersena w Lublinie
z dnia 05 lipca 2017 r.
w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w im. H. Ch. Andersena w Lublinie

Na podstawie § 2 pkt 6 Regulaminu organizacyjnego Teatru im. H. Ch. Andersena w Lublinie oraz art. 7 pkt 4 i art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016r. poz. 922) w związku z § 3, § 4 i § 5 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) zarządzam, co następuje:

§ 1
Cel zarządzenia

Celem określenia reguł i zasad obowiązujących przy przetwarzaniu danych osobowych w Teatrze im. H. Ch. Andersena w Lublinie, wprowadzam:
1) politykę bezpieczeństwa danych osobowych;
2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 2
Terminy używane w zarządzeniu

Jeżeli jest mowa w zarządzeniu o:
1) administratorze danych – rozumie się przez to Dyrektora Teatru im. H. Ch. Andersena w Lublinie;
2) administratorze systemu – rozumie się przez to osobę upoważnioną do zarządzania systemem lub systemami informatycznymi;
3) administratorze bezpieczeństwa informacji – rozumie się przez to osobę powołaną imiennie przez administratora danych do zapewnienia przestrzegania przepisów o ochronie danych osobowych oraz prowadzenia rejestru zbiorów danych osobowych administratora danych;
4) osobie upoważnionej – rozumie się przez to osobę upoważnioną przez administratora danych do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, zobowiązanej jednocześnie do zachowania w tajemnicy danych osobowych, do których miała dostęp oraz sposobów ich zabezpieczenia;
5) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922);
6) rozporządzeniu – rozumie się przez to rozporządzenie 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);
7) GIODO – rozumie się przez to Generalnego Inspektora Ochrony Danych

Osobowych;

8) polityce – rozumie się przez to politykę bezpieczeństwa danych osobowych im. H. Ch. Andersena w Lublinie;
9) instrukcji – rozumie się przez to instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Teatru im. H. Ch. Andersena w Lublinie;
10) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
11) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione w sposób nieautoryzowany;
12) poufności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;
13) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej;
14) przetwarzaniu – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych przez osoby upoważnione a zwłaszcza wykonywane w systemach informatycznych;
15) zbiorze danych osobowych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, zarówno na nośniku papierowym, jak i elektronicznym;
16) powierzeniu przetwarzania danych osobowych – rozumie się przez to wykonywanie przez podmiot zewnętrzny jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza tych, które wykonuje się w systemach informatycznych;
17) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych i innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
18) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych i innych, znany jedynie osobie upoważnionej, służący do uzyskania dostępu do systemu informatycznego przetwarzającego dane osobowe;
19) środkach kryptograficznej ochrony – rozumie się przez to mechanizmy szyfrowania danych lub szyfrowania ich transmisji;
20) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych w zbiorze danych.

§ 3
Wyłączenie jawności niniejszego zarządzenia

Jawność niniejszego zarządzenia dla osób nieupoważnionych przez administratora danych do przetwarzania danych osobowych jest wyłączona na podstawie art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922) oraz art. 5. ust 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej Dz. U. 2001 nr 112 poz. 1198 ze zm.

Rozdział I
Polityka bezpieczeństwa danych osobowych

§ 4
Organizacja zabezpieczania danych osobowych

1. Administrator danych wyznacza osoby, które zostaną upoważnione do przetwarzania danych osobowych i określa granice tego przetwarzania w zakresie czynności, dla pracownika zatrudnionego na podstawie umowy o pracę lub dla innych osób – w umowie cywilnoprawnej.
2. Administrator danych zapoznaje osobę upoważnioną z zakresem obowiązków, w tym z odpowiedzialnością za przetwarzanie danych osobowych, a następnie zleca administratorowi bezpieczeństwa informacji przygotowanie upoważnień do przetwarzania danych osobowych w 2 egzemplarzach (jeden dla osoby upoważnionej, drugi do teczki akt osobowych pracownika).
3. Osoby upoważnione podpisują się na upoważnieniu do przetwarzania danych osobowych, potwierdzając zapoznanie się z niniejszym zarządzeniem (polityką bezpieczeństwa, instrukcją, ustawą i rozporządzeniem do niej oraz zobowiązują się do przetwarzania danych osobowych wyłącznie w zakresie upoważnienia do przetwarzania i ewentualnie przyznanych uprawnień w systemie informatycznym oraz do zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia.
4. Administrator bezpieczeństwa informacji, prowadzi ewidencję osób upoważnionych, nadaje upoważnieniom kolejny numer, wprowadza dane osoby upoważnionej do ewidencji.
5. Administrator danych wyznacza administratora systemu.
6. Administrator bezpieczeństwa informacji przekazuje administratorowi systemu aktualną wersję ewidencji osób upoważnionych do przetwarzania danych osobowych.
7. Administrator systemu, na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych, nadaje w systemie informatycznym uprawnienia osobom upoważnionym, identyfikator i hasło, celem rozpoczęcia pracy w systemie.
8. Upoważnienia do przetwarzania danych osobowych są wystawiane każdej osobie wyznaczonej do przetwarzania danych osobowych w zbiorze, na czas nieokreślony.
9. Administrator danych cofa upoważnienie do przetwarzania danych osobowych osobie upoważnionej, wydając w tym zakresie polecenie administratorowi bezpieczeństwa informacji, w przypadku gdy:
   1) osoba upoważniona zakończyła zatrudnienie, pracę, staż lub praktykę lub inny stosunek prawny z administratorem danych;
   2) osoba upoważniona zmieniła zakres upoważnienia;
   3) osoba upoważniona nie zapewnia zachowania w tajemnicy danych osobowych, jak i sposobów ich zabezpieczenia.

§ 5
Główne zasady bezpiecznego przetwarzania danych osobowych

1. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana zapewnić ochronę danych osobowych przed:
   1) udostępnieniem osobom nieupoważnionym;
   2) zabraniem przez osobę nieupoważnioną;

3) przetwarzaniem z naruszeniem ustawy;
4) zmianą;
5) utratą;
6) uszkodzeniem;
7) zniszczeniem;

2. Osoba upoważniona może przetwarzać dane osobowe wyłącznie w zakresie upoważnienia do przetwarzania danych osobowych i tylko w celu wykonania obowiązków służbowych.
3. Osoba upoważniona zobowiązuje się do zachowania poufności danych osobowych oraz sposobów ich zabezpieczenia, zarówno w trakcie, jak i po zakończeniu pracy, praktyki lub stażu oraz cofnięcia upoważnienia, podpisując upoważnienie do przetwarzania danych osobowych.
4. Osoba upoważniona rozpoczynając przetwarzanie danych jest obowiązana ocenić stan bezpieczeństwa danych w pomieszczeniu będącym częścią obszaru przetwarzania danych osobowych i informować przełożonych o wszelkich faktach budzących niepokój w zakresie bezpieczeństwa danych.
5. Po zakończeniu przetwarzania danych osobowych osoba upoważniona jest obowiązana zabezpieczyć dokumenty zawierające dane osobowe przed dostępem osób nieupoważnionych, zamknąć szafy i pomieszczenia oraz zdeponować klucze w miejscu do tego wyznaczonym.

§ 6
Zasada czystego biurka

1. Osoba upoważnione organizuje stanowisko pracy tak, aby osoby nieupoważnione nie miały dostępu do danych osobowych.
2. Przebywanie osób nieupoważnionych w obszarze przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej.
3. Dokumenty zawierające dane osobowe po zakończeniu przetwarzania przechowywane są w szafach zamykanych na klucze, przechowywane w ustalonym za wiedzą administratora danych miejscu, do którego dostęp mają jedynie osoby upoważnione.
4. Dokumenty zawierające dane osobowe transportuje się w zaklejonych kopertach.
5. Dokumenty zawierające dane osobowe niszczy się w sposób uniemożliwiający ich odczytanie.

§ 7
Ochrona obszaru przetwarzania danych osobowych

1. Dane osobowe są przetwarzane w pomieszczeniach lub częściach pomieszczeń, do których dostęp mają osoby upoważnione.
2. Osoby nieupoważnione mogą przebywać w tych pomieszczeniach wyłącznie w obecności osób upoważnionych.
3. Administrator budynku, służby ochrony oraz osoby utrzymujące czystość pomieszczeń mogą przebywać w obszarze przetwarzania danych osobowych w celu wykonania obowiązków służbowych, ale bez możliwości dostępu do danych.
4. Klucze do pomieszczeń, w których przetwarza się dane osobowe są wydawane zgodnie z polityką klucz obowiązującą w Teatrze.

§ 8
Organizacja pozostałych czynności związanych z zabezpieczeniem przetwarzania danych osobowych

1. Administrator bezpieczeństwa informacji sporządza i aktualizuje:
   1) elektroniczny wykaz zbiorów danych osobowych;
   2) elektroniczny wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe w zbiorach danych;
   3) elektroniczny opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   4) elektroniczny opis przepływu danych osobowych pomiędzy poszczególnymi zbiorami danych osobowych;
   5) jawny rejestr zbiorów danych osobowych przetwarzanych przez administratora danych z wyjątkiem zbiorów o których mowa w art. 43 ust.1 ustawy;
   6) politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
2. Administrator bezpieczeństwa informacji:
   7) rejestruje zbiór danych osobowych w rejestrze GIODO wysyłając za pomocą platformy elektronicznej eGIODO wypełniony i podpisany wspólnie z administratorem danych wniosek zgłoszeniowy, stosując przepisy art. 41.1 ustawy oraz art. 46.2, chyba że administrator danych jest zwolniony z obowiązku rejestracji zbioru zgodnie z art. 43.1 ustawy;
   8) aktualizuje wniosek zgłoszeniowy w terminie 30 dni od dokonania zmian w zbiorze danych osobowych, stosując przepisy art. 41.2 ustawy;
   9) wyrejestrowuje zbiór danych osobowych stosując przepisy art. 44a ustawy.
3. Administrator bezpieczeństwa informacji przygotowuje i przedstawia do podpisu administratorowi danych wniosek zgłoszenia lub odwołania administratora bezpieczeństwa informacji do/z rejestru administratorów bezpieczeństwa informacji prowadzonego przez GIODO.

§ 9
Zasady przetwarzania danych osobowych przez administratora danych

Administrator danych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, stosując zapisy art. 26 ustawy, a w szczególności zapewnia aby dane te były:

1. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
2. merytorycznie poprawne i adekwatne w stosunku do celów przetwarzania;
3. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to niezbędne do osiągnięcia celu przetwarzania;
4. przetwarzane zgodnie z prawem, stosując zapisy art. 23 – 30 ustawy odnośnie zasad przetwarzania danych, zbierania danych, przetwarzania danych wrażliwych oraz udostępniania danych;
5. przekazywane do państwa trzeciego, stosując zapisy art. 47 – 48 ustawy.

§ 10
Powierzenie przetwarzania danych osobowych innemu podmiotowi

1. Jeżeli administrator danych nie dysponuje odpowiednimi środkami sprzętowymi lub programowymi zapewniającymi przetwarzanie danych osobowych, powierza przetwarzanie danych innemu podmiotowi.
2. Powierzenie przetwarzania następuje w formie umowy na piśmie zawartej pomiędzy administratorem danych a podmiotem zewnętrznym. Umowa powierzenia, pod rygorem nieważności, musi mieć jasno sprecyzowany cel i zakres przetwarzania.
3. Podmiot, któremu powierzono przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a.
4. Administrator danych przekazuje do zaopiniowania pod względem zachowania bezpieczeństwa danych osobowych administratorowi bezpieczeństwa informacji projekty umów powierzenia przetwarzania z podmiotami zewnętrznymi.
5. Zapisy umowy o powierzenie przetwarzania mogą stanowić część innych umów zawartych z podmiotem zewnętrznym.

§ 11
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

1. Za naruszenie bezpieczeństwa przetwarzania danych osobowych uważa się w szczególności:
   1) przetwarzanie bez upoważnienia do przetwarzania;
   2) przetwarzanie niezgodnie z zakresem upoważnienia;
   3) złamanie tajemnicy danych osobowych i sposobów ich zabezpieczenia;
   4) wykorzystanie sprzętu informatycznego administratora danych do celów prywatnych;
   5) używanie prywatnego sprzętu informatycznego w sieci służbowej;
   6) zainfekowanie systemu informatycznego wirusem;
   7) używanie prywatnych przenośnych nośników informatycznych.
2. Osoba upoważniona jest obowiązana powiadomić administratora danych lub osobę zastępującą albo administratora systemu o następujących incydentach mogących obniżyć bezpieczeństwo danych osobowych w systemach informatycznych:
   1) możliwości przetwarzania danych osobowych bez wprowadzenia hasła;
   2) dostępie do danych w szerszym lub węższym zakresie niż przyznany;
   3) podejrzeniu nieautoryzowanej modyfikacji danych;
   4) pojawieniu się zmian w wyglądzie prezentowanych na ekranie danych;
   5) wykryciu wirusa komputerowego;
   6) utracie tajności kluczy kryptograficznych;
   7) zgubieniu lub kradzieży przenośnego nośnika danych;
   8) podejrzeniu kradzieży sprzętu informatycznego lub dokumentów zawierających dane;
   9) zauważeniu śladów włamania do szaf lub pomieszczeń w obszarze przetwarzania;
   10) zauważeniu innych niepokojących faktów.
3. Administrator systemu natychmiast podejmuje działania zmierzające do ochrony

systemu informatycznego przed dalszym naruszeniem.

4. Po opanowaniu incydentu naruszenia bezpieczeństwa przetwarzania danych osobowych administrator danych zleca administratorowi bezpieczeństwa informacji przeprowadzenie postępowania wyjaśniającego, mającego na celu ustalenie okoliczności zdarzenia, sporządzenie raportu z naruszenia bezpieczeństwa danych, zawierającego opis przyczyn, zaistniałe dla administratora danych skutki oraz proponowane działania naprawcze.

§ 12
Dokonywanie sprawdzeń przez administratora bezpieczeństwa informacji

1. Administrator bezpieczeństwa informacji nadzoruje przestrzeganie zasad ochrony danych osobowych wykonując sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdanie dla administratora danych.
2. Administrator bezpieczeństwa informacji wykonuje sprawdzenia:
   1) planowe;
   2) po incydencie naruszającym bezpieczeństwo danych osobowych;
   3) na żądanie GIODO.
3. Administrator bezpieczeństwa informacji, ma prawo:
   1) wstępu do wszystkich pomieszczeń obszaru przetwarzania;
   2) asystowania przy wszystkich czynnościach związanych z przetwarzaniem danych osobowych;
   3) wglądu do dokumentów zawierających dane osobowe;
   4) wglądu do systemu informatycznego służącego do przetwarzania danych osobowych;
   5) żądania od osób upoważnionych ustnych i pisemnych wyjaśnień;
   6) wnioskowania do administratora danych o wycofanie osobie upoważnionej upoważnienia do przetwarzania danych osobowych i zlecenie administratorowi systemu odebrania uprawnień w systemie informatycznym w wyniku stwierdzonego naruszenia bezpieczeństwa przetwarzania danych osobowych.
4. Do przeprowadzenia sprawdzenia administrator bezpieczeństwa informacji nie potrzebuje odrębnego upoważnienia.
5. Osoby upoważnione są obowiązane do udzielenia w czasie sprawdzenia, wszystkich koniecznych informacji administratorowi bezpieczeństwa informacji.

§ 13
Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

1. W celu zapewniania przestrzegania przepisów o ochronie danych osobowych administrator bezpieczeństwa informacji przeprowadza szkolenia z zakresu bezpieczeństwa przetwarzania danych osobowych dla osób upoważnionych.
2. Administrator bezpieczeństwa informacji podpisuje zaświadczenia o odbytym szkoleniu.
3. Osoby upoważnione mają obowiązek zapoznać się z obowiązującymi przepisami o ochronie danych osobowych (ustawie i rozporządzeniu) oraz z obowiązującym w tym zakresie niniejszym zarządzeniu.

Rozdział II
Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§ 14
Poziomy bezpieczeństwa przetwarzania danych osobowych

Administrator danych wyznacza administratora systemu do określenia na podstawie rozporządzenia i zastosowania dla danego zbioru danych osobowych poziomu bezpieczeństwa:

1) podstawowego – jeżeli przetwarzane są dane osobowe zwykłe oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną;
2) podwyższonego – jeżeli przetwarzane są dane osobowe wrażliwe, wymienione w art. 27 ustawy oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną;
3) wysokiego – jeżeli przynajmniej jedno urządzenie systemu informatycznego jest połączone z siecią publiczną.

§ 15
Podstawowe mechanizmy w jakie powinny być wyposażone urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Systemy informatyczne służące do przetwarzania danych osobowych są wyposażone w następujące mechanizmy:

1) rozliczalności, przez który rozumie się właściwość zapewniającą, że działania podmiotu (osoby upoważnionej) mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
2) integralności, przez który rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) raportu, przez który rozumie się przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
4) poufności danych, przez który rozumie się właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom (osobom nieupoważnionym);
5) uwierzytelniania, przez który rozumie się możliwość weryfikacji deklarowanej tożsamości osoby upoważnionej.

§ 16
Mechanizmy rozpoczęcia, zawieszenia i zakończenia pracy

1. W celu rozpoczęcia przetwarzania danych osobowych w systemie informatycznym osoba upoważniona:
   1) uruchamia komputer;
   2) loguje się do systemu poprzez zastosowanie unikalnego identyfikatora oraz co najmniej ośmioznakowego, indywidualnego, poufnego, własnego hasła, zapewniającego w sposób jednoznaczny przypisanie danej osobie wykonywanych czynności.
2. Osoby upoważnione nie mają prawa udostępniać hasła innym osobom.
3. Monitory komputerów powinny wyłączyć się automatycznie po minimum 15 minutach od przerwania pracy a wznowienie pracy monitora następuje po

wprowadzeniu hasła.

4. Jeżeli monitory komputerów nie mają zainstalowanego automatycznego wygaszacza, osoby upoważnione przerywając pracę na stacji roboczej, są obowiązane skuteczne wylogować się z systemu informatycznego stosując kombinację klawiszy „wnidows+L", ewentualnie wyłączyć komputer.
5. Stanowiska pracy mają tak zlokalizowane urządzenia informatyczne służące do przetwarzania danych osobowych, żeby osoby nieupoważnione nie mogły widzieć treści danych wyświetlanych na ekranów monitorów komputerowych.
6. Po zakończeniu przetwarzania danych osobowych w systemie informatycznym osoba upoważniona jest obowiązana sprawdzić stację roboczą, czy nie pozostały w niej zewnętrzne nośniki danych, następnie poprawnie się wylogować z systemu.
7. Ewentualnych napraw systemu informatycznego dokonuje administrator systemu lub, za jego wiedzą, podmiot któremu powierzono przetwarzanie danych w tym zakresie.
8. Niedopuszczalne jest zakończenie pracy w systemie informatycznym bez wykonania pełnej i poprawnej procedury wylogowania i wyłączenia stacji roboczej.

§ 17
Procedury nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz rejestrowania i wyrejestrowywania tych uprawnień w systemach informatycznych

1. Administrator danych decyduje o nadaniu osobom wyznaczonym do przetwarzania danych osobowych uprawnień do przetwarzania danych oraz uprawnień w systemie informatycznym obsługującym zbiór danych osobowych, zlecając administratorowi bezpieczeństwa informacji przygotowanie upoważnień do przetwarzania danych.
2. Po podpisaniu upoważnień do przetwarzania przez administratora danych, administrator bezpieczeństwa informacji przekazuje zaktualizowany wykaz osób upoważnionych do przetwarzania danych osobowych administratorowi systemu, który na tej podstawie nadaje identyfikator i przydziela hasło osobie upoważnionej.
3. Zakres uprawnień w systemie odpowiada nazwom czynności charakterystycznych dla danego zbioru, które będzie wykonywać osoba upoważniona w ramach zakresu upoważnienia.
4. Administrator danych decyduje o cofnięciu osobie upoważnionej uprawnień do przetwarzania danych osobowych oraz o zablokowaniu uprawnień w systemie informatycznym obsługującym zbiór danych osobowych zlecając administratorowi bezpieczeństwa informacji przygotowanie cofnięcia upoważnienia do przetwarzania danych.
5. Po podpisaniu cofnięć upoważnień do przetwarzania administrator bezpieczeństwa informacji przekazuje zaktualizowany wykaz osób upoważnionych do przetwarzania danych osobowych administratorowi systemu, który blokuje użytkownika w systemie informatycznym.
6. W sytuacjach powzięcia uzasadnionego podejrzenia, że doszło do naruszenia tajemnicy danych osobowych lub naruszenia tajemnicy ich bezpieczeństwa administrator danych lub administrator bezpieczeństwa informacji wydają administratorowi systemu polecenie zablokowania uprawnień osoby upoważnionej w systemie. Cofnięcie upoważnienia osobie upoważnionej do przetwarzania danych osobowych następuje w takim przypadku najszybciej jak to możliwe.

§ 18
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Administrator systemu przydziela osobie upoważnionej indywidualny identyfikator potwierdzający zadeklarowaną tożsamość osoby upoważnionej.
2. Systemy informatyczne, których parametry uniemożliwiają zastosowanie prawidłowego hasła i jego cyklicznej zmiany są chronione na poziomie systemu operacyjnego komputera.
3. Pierwsze przydzielone hasło powinno jest jednorazowe a po jego poprawnym użyciu system automatycznie wymusza wpisanie nowego hasła do dalszego użytkowania co 30 dni.
4. Hasła zmieniają osoby upoważnione.
5. System zapewnia:
   1) jakość hasła, czyli zastosowanie odpowiedniej ilość znaków, wielkich i małych liter, cyfr lub znaków specjalnych w zależności od poziomu bezpieczeństwa przetwarzania;
   2) generowanie hasła różniącego się od co najmniej trzech ostatnio stosowanych przez osobę upoważnioną.
6. Osoba upoważniona posiadająca hasło dostępu do systemu jest obowiązana zachować je w tajemnicy i nie ujawniać innym osobom.
7. Osoba upoważniona ponosi odpowiedzialność za czynności wykonywane przy użyciu przyznanego identyfikatora i hasła w systemie informatycznym.
8. W przypadku powzięcia przez osobę upoważnioną podejrzenia, że hasło jej przydzielone uległo odtajnieniu, osoba ta jest obowiązana zmienić hasło na nowe.
9. System powinien wymuszać tworzenie haseł składających się z niepowtarzalnego zestawu co najmniej:
   1) sześciu znaków na poziomie bezpieczeństwa podstawowym;
   2) ośmiu znaków w tym dużych i małych liter, cyfr lub znaków specjalnych, na poziomach bezpieczeństwa podwyższonym i wysokim.
10. Praca w systemie informatycznym na identyfikatorze i haśle innym niż własne jest zabroniona.
11. Hasła wpisywane z klawiatury nie mogą pojawiać się w formie jawnej na ekranie komputera.

§ 19
Procedury tworzenia i przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz sposób, miejsce i okres przechowywania elektronicznych nośników danych

1. Kopie zapasowe są tworzone przez administratora systemu lub wyznaczoną osobę upoważnioną w szczególności na:
   1) elektronicznych nośnikach danych;
   2) specjalnie do tego celu przeznaczonych komputerach lub zewnętrznych sieciowych dyskach twardych.
2. Zapasowe kopie zbioru danych są tworzone w systemie informatycznym codziennie, po zakończeniu przetwarzania lub okresowo, po użyciu systemu

informatycznego, jak np. dla aplikacji „Płatnik".

3. Kopie zapasowe konfiguracji programów i narzędzi programowych wraz z uprawnieniami osób upoważnionych są wykonywane w przypadku zmiany systemu informatycznego.
4. Elektroniczne nośniki danych zawierające kopie zapasowe, pozbawia się zapisu poprzez:
   1) zapisanie nowej kopii zapasowej na tym samym nośniku;
   2) skasowanie danych programem usuwającym trwale pliki;
   3) fizyczne zniszczenie.
5. Elektroniczne nośniki danych przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
6. Kopie zapasowe przechowuje się w zamkniętej szafie w pomieszczeniu, do którego dostęp mają jedynie osoby upoważnione.
7. Elektroniczne nośniki danych zawierające dane osobowe przechowuje się w zamkniętych szafach w obszarze przetwarzania.
8. Kopie zapasowe oraz elektroniczne nośniki danych zawierające dane osobowe usuwa się niezwłocznie po ustaniu ich użyteczności, chyba że przepisy szczegółowe stanowią o ich dłuższym przechowywaniu.
9. Instalację oprogramowania systemu informatycznego i jego aktualizacje oraz odczyty kopii przeprowadza administrator systemu.
10. Referat księgowości dokonuje inwentaryzacji zainstalowanego oprogramowania.
11. Zabronione jest użytkowanie oprogramowania systemu informatycznego bez posiadania aktualnej licencji.

§ 20
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Systemy informatyczne chronione są przed działaniem wirusów komputerowych aktualnym, licencjonowanym oprogramowaniem antywirusowym, zainstalowanym przez administratora systemu na serwerach, stacjach roboczych w tym na komputerach przenośnych.
2. Oprogramowanie antywirusowe sprawuje ciągły nadzór nad pracą systemu i zasobami danych osobowych na serwerach i stacjach roboczych, poprzez skanowanie dysków.
3. Sposób postępowania w przypadku wystąpienia wirusów określa instrukcja producenta programu antywirusowego.
4. Oprogramowanie antywirusowe powinno aktualizować się automatycznie o nową wersję bazy wirusów.
5. Osoby upoważnione są obowiązane do przeprowadzania każdorazowo kontroli antywirusowej elektronicznych nośników danych i ich zawartości przed ich użyciem w stacji roboczej.
6. Osoby upoważnione są obowiązane do poinformowania administratora danych lub administratora systemu o wykryciu przez oprogramowanie antywirusowe incydentu zagrażającemu bezpieczeństwu danych osobowych lub systemu informatycznego.
7. Zabrania się osobom upoważnionym wyłączania oprogramowania antywirusowego.

§ 21
Wymagania wobec systemu informatycznego

przetwarzającego dane osobowe

1. Systemy informatyczne powinny rejestrować:
   1) identyfikator osoby upoważnionej, przetwarzającej dane osobowe w systemie i przypisywać tę czynności tylko jej;
   2) datę i czas zalogowania i wylogowania z systemu;
   3) tożsamość stacji roboczej;
   4) nieudane i udane próby zalogowania się;
   5) wygaśnięcie czasu obowiązywania hasła dostępu do stacji roboczej i informują o tym fakcie;
2. Systemy informatyczne powinny zapewnić sporządzanie dla każdej osoby, której dane są przetwarzane w systemie informatycznym, raportu zawierającego:
   1) datę pierwszego wprowadzenia danych do systemu;
   2) identyfikator osoby upoważnionej wprowadzającej te dane;
   3) źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą;
   4) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione;
   5) dacie i zakresie udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   6) sprzeciwu wobec przetwarzania danych osobowych o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
3. Raport, o którym mowa w pkt. 2 musi być zrozumiały dla przeciętnego odbiorcy, czyli powinien prezentować informacje w pełnym brzmieniu, poprzedzone nazwą opisową danego pola (nie w postaci kodowanej lub skróconej) i powinien generować dane tylko i wyłącznie jednej osoby.
4. Systemy służące do przetwarzania danych osobowych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie nie muszą generować raportu, o którym mowa w punkcie 2.

§ 22
Procedury wykonywania przeglądów i konserwacji systemów oraz elektronicznych nośników danych służących do przetwarzania danych osobowych

1. Przeglądy i konserwacje systemów informatycznych odbywają się przy zachowaniu pełnej separacji danych osobowych od osób nieupoważnionych do przetwarzania, pod nadzorem administratora systemu lub w obecności osoby upoważnionej.
2. Elektroniczne nośniki danych przeznaczone do przekazania osobie nieupoważnionej pozbawia się wcześniej zapisu danych osobowych w sposób uniemożliwiający odzyskanie danych.
3. Elektroniczne nośniki danych przeznaczone do naprawy pozbawia się wcześniej zapisu danych osobowych lub naprawia się je pod nadzorem osoby upoważnionej.
4. Elektroniczne nośniki danych nie nadające się do dalszego użytkowania niszczy się mechanicznie.

§ 23
Przetwarzanie danych osobowych na komputerach przenośnych

1. Decyzję o przechowywaniu danych osobowych na komputerach przenośnych podejmuje administrator danych po konsultacji ryzyka przetwarzania z administratorem bezpieczeństwa informacji oraz administratorem systemu.
2. Przy przechowywaniu danych osobowych na komputerach przenośnych obowiązują

te same zasady jak przy pracy na komputerach stacjonarnych oraz stosowanie mechanizmów kryptograficznych wobec danych osobowych.

3. Po ustaniu powodu przechowywania danych osobowych na komputerach przenośnych, dane te należy przenieść na serwer a następnie trwale usunąć z pamięci komputera przenośnego.
4. Osoby upoważnione użytkujące komputer przenośny zawierający dane osobowe zachowują szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania.

§ 24
Zasady zarządzania środkami kryptograficznej ochrony

1. Środki kryptograficznej ochrony stosuje się przy:
   1) przesyłaniu danych osobowych metodą teletransmisji siecią publiczną;
   2) przenoszeniu danych na nośnikach danych poza obszar przetwarzania;
   3) przetwarzaniu danych za pomocą komputerów przenośnych.
2. Administrator systemu decyduje o rodzaju zastosowanych środków kryptograficznej ochrony i zapewnia instruktaż z zakresu ich użytkowania.
3. Administrator systemu zarządza:
   1) aplikacjami kryptograficznymi;
   2) generowaniem kluczy kryptograficznych;
   3) wycofywaniem kluczy kryptograficznych.

§ 25
Ochrona serwera bazodanowego

1. Dostęp do pomieszczeń w których pracują serwery mają administrator systemu i administrator bezpieczeństwa informacji.
2. Pomieszczenia, w których pracują serwery, są zabezpieczone drzwiami wyposażonymi w zamek patentowy oraz dodatkowo kratami w oknach, jeżeli pomieszczenia te są zlokalizowane w piwnicy, na parterze, pierwszym lub ostatnim piętrze budynku.
3. Serwery posiadają zasilacze awaryjne, pozwalające poprawnie zapisać dane osobowe i bezpiecznie wyłączyć system.

§ 26
Zasady dostępu do sieci publicznej

1. Administrator systemu definiuje zasady dostępu do sieci publicznej osób upoważnionych za pomocą instalacji i konfiguracji właściwego oprogramowania.
2. Administrator systemu konfiguruje oprogramowanie tak żeby:
   1) monitorowało przenoszenie treści pomiędzy stacjami roboczymi a siecią publiczną i odwrotnie;
   2) uniemożliwiało zapisanie nieakceptowalnych treści z sieci publicznej na stacji roboczej;
   3) odnotowało i jednoznacznie przypisało osobie upoważnionej: adres IP komputera, identyfikator, użycie hasła, godzinę zalogowania się, czas trwania połączenia oraz wszystkie wydarzenia, które miały miejsce podczas logowania;
   4) odnotowało i jednoznacznie przypisało adresowi IP komputera nieautoryzowane próby połączenia się z serwerem, próby wywołania adresów URL;

5) komunikacja pomiędzy stacjami roboczymi a serwerem odbywała się poprzez automatyczne szyfrowanie.

3. Administrator systemu konfiguruje zabezpieczenia logiczne zapory sieciowej, tak aby obejmowały :
   1) autoryzację wysyłanych danych;
   2) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
   3) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
4. Niedozwolona jest praca z wykorzystaniem sieci publicznej w sposób naruszający przepisy o ochronie danych osobowych, lub inne przepisy.
5. Zabrania się korzystania z sieci publicznej do celów prywatnych lub pobierania plików których treść jest niezwiązana z wykonywanymi czynnościami służbowymi.
6. Zabrania się używania sprzętu informatycznego nie będącego własnością administratora danych.

§ 27
Prowadzenie korespondencji elektronicznej

1. Dostęp do imiennych kont poczty elektronicznej przysługuje tylko osobom upoważnionym, którym administrator systemu przyznał identyfikator i hasło.
2. Osoba upoważniona chcąc uzyskać dostęp do konta poczty elektronicznej jest obowiązana autoryzować tę operację hasłem.
3. Zabrania się otwierania załączników poczty elektronicznej pochodzących od nieznanych nadawców, zwłaszcza załączonych plików typu *.exe, *.src, *.pif.
4. Oprogramowanie antywirusowe skanuje pocztę elektroniczną w czasie rzeczywistym.
5. Zabrania się udzielania odpowiedzi na wiadomości zawierające spam.

§ 28
Postanowienia końcowe

1. Tracą moc: Zarządzenie Nr 9/12 Dyrektora Naczelnego i Artystycznego Teatru im. H. Ch. Andersena w Lublinie z dnia 31 grudnia 2012 r. w sprawie określenia i wdrożenia zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Teatrze im. H. Ch. Andersena w Lublinie.

2. Nadzór nad wykonaniem Zarządzenia powierzam administratorowi bezpieczeństwa informacji.

3. Zarządzenie wchodzi w życie z dniem podpisania.

P.O. DYREKTORA
Karolina Rozwód

TEATR im. H. CH. ANDERSENA
20-037 Lublin, ul. Aleje Racławickie 8/22B
tel. 81 532 16 28, fax 81 534 36 11
NIP 712-010-37-46