Zarządzenie nr 8
Dyrektora Suwalskiego Ośrodka Kultury
z dnia 24.05.2018 roku
w sprawie wprowadzenia Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie § 3 ust. 5 pkt 3 regulaminu organizacyjnego Suwalskiego Ośrodka Kultury, ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (tekst jedn. Dz. U. z 16 kwietnia 2012 r. poz. 406), § 3 i § 4 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 ze zm.) oraz na postawie Rozporządzenia 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) zarządzam, co następuje:

§ 1

1. Wprowadza się do stosowania z dniem 25 maja 2018 r „Politykę bezpieczeństwa informacji Suwalskiego Ośrodka Kultury" oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
2. Polityka bezpieczeństwa Suwalskiego Ośrodka Kultury stanowi załącznik nr 1 do niniejszego Zarządzenia.
3. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszego Zarządzenia.

§ 2

Polityka bezpieczeństwa określa zbiór zasad obowiązujących przy zbieraniu, przetwarzaniu danych osobowych we wszystkich zbiorach administrowanych przez Suwalski Ośrodek Kultury w Suwałkach zgodnie z Rozporządzeniem 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).

§ 3

Wykonanie Zarządzenia powierzam Zastępcy Dyrektora oraz kierownikom poszczególnych jednostek organizacyjnych Suwalskiego Ośrodka Kultury i zobowiązuję do zapoznania z treścią niniejszego Zarządzenia oraz z załącznikami wszystkich pracowników Suwalskiego Ośrodka Kultury.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

p.o. Dyrektor
Suwalskiego Ośrodka Kultury
Alicja Andrulewicz

Załącznik nr 1 do Zarządzenia
Dyrektora Suwalskiego Ośrodka Kultury
nr ...8... z dnia 24.05.2018

Polityka bezpieczeństwa informacji Suwalskiego Ośrodka Kultury

Rozdział 1

Postanowienia ogólne

1. Polityka bezpieczeństwa informacji w Suwalskim Ośrodku Kultury, zwana dalej „Polityką", jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych, w szczególności w wykazach, listach wycieczek/wyjazdów, uczestników konkursów/ festiwali oraz w innych zbiorach ewidencyjnych zgodnie z Rozporządzeniem 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)
2. Suwalski Ośrodek Kultury zwany dalej „Ośrodkiem" realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:
    a. przetwarzane zgodnie z prawem;
    b. zbierane dla oznaczonych, zgodnych z planem pracy Ośrodka celów;
    c. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Rozdział 2

Ewidencja zasobów

1. Wyjaśnienia używanych pojęć:
1) Dane osobowe – wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
2) Baza danych osobowych – każdy zbiór danych o charakterze osobowym,
3) Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4) Inspektor Ochrony Danych Osobowych – osoba monitorująca przestrzeganie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych,
5) Bezpieczeństwo systemu informatycznego – wdrożenie przez administratora danych osobowych lub inną osobę przez niego wyznaczoną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed dostępem, modyfikacją, ujawnieniem, pozyskiwaniem lub zniszczeniem,

6) Nośniki danych osobowych – dyski twarde komputerów, płyty CD lub DVD, dyski zewnętrzne, pamięć flash, itp.,
7) Pracownicy – osoby zatrudnione w Ośrodku na umowę o pracę..
2. Dane osobowe w Ośrodku Kultury przetwarzane są w budynkach znajdujących się przy ul. T. Noniewicza 71 oraz Papieża Jana Pawła II 5 w Suwałkach.
3. Polityka zawiera:
1) wykaz zbiorów danych osobowych przetwarzanych w Ośrodku wraz z opisami struktury zbiorów i sposobów ich przetwarzania (załącznik nr 1 do Polityki bezpieczeństwa Informacji)
2) wykaz pomieszczeń, w których przetwarzane są dane osobowe w sposób tradycyjny i z użyciem stacjonarnego sprzętu komputerowego (załącznik nr 2 do Polityki bezpieczeństwa informacji)
3) rejestr czynności przetwarzania danych osobowych (załącznik nr 3 do Polityki bezpieczeństwa informacji

Rozdział 3

Opis zagrożeń naruszających ochronę danych osobowych.

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:
a) Zagrożenia losowe:
- zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu prądu) – ich wystąpienie może prowadzić do utraty danych lub ich zniszczenia lub uszkodzenia,
- wewnętrzne (np., awarie sprzętowe) – w wyniku ich wystąpienia może dojść do zniszczenia danych.
2) Zagrożenie zamierzone (świadome i celowe naruszenie poufności danych).

Rozdział 4

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności przetwarzanych danych osobowych .

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
a) wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatnią upoważnioną do przetwarzania danych osobę - także w godzinach pracy,
b) w Ośrodku funkcjonuje system alarmowy, który zostaje włączony przez pracownika, który opuszcza Ośrodek jako ostatni (budynek T. Noniewicza 71), w budynku przy ul. Papieża Jana Pawła II 5 nadzór fizyczny przez całą dobę.
2. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
a) ochrona przed utratą zgromadzonych danych poprzez cykliczne (co pół roku) wykonywanie kopii zapasowych, z których w przypadku awarii, odtwarzane są dane i system operacyjny
b) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie gaśnic
3. Organizacyjną ochronę danych osobowych i ich przetwarzania realizuje się poprzez:
a) zapoznanie każdego pracownika z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem do pracy przy ich przetwarzaniu
b) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych osobowych oraz form zabezpieczenia pomieszczeń i budynku, sprzętu
c) upoważnienie osób do przetwarzania danych osobowych (załącznik nr 4 do Polityki bezpieczeństwa informacji)

d) upoważnienie osób do przebywania w pomieszczeniach przetwarzania danych osobowych (załącznik nr 5 do Polityki bezpieczeństwa informacji)
d) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 6 do Polityki bezpieczeństwa informacji).
e)prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w określonym przedziale czasowym (załącznik nr 6.1 do Polityki bezpieczeństwa informacji
f)prowadzenie ewidencji osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych (załącznik nr 7 do Polityki bezpieczeństwa informacji)
g) prowadzenie ewidencji osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych w określonym przedziale czasowym (załącznik nr 7.1 do Polityki bezpieczeństwa informacji).

Rozdział 5

Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy Rozporządzenia 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) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
2. Niniejsza „Polityka bezpieczeństwa" służąca do przetwarzania danych osobowych w Suwalskim Ośrodku Kultury wchodzi w życie z dniem podpisania.

Załącznik nr 2 do Zarządzenia Dyrektora Suwalskiego Ośrodka Kultury
nr ..8..... z dnia 24.05.2018

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Rozdział I

Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Suwalskim Ośrodku Kultury zwanym dalej „Ośrodkiem".
2. Instrukcja została opracowana zgodnie z Rozporządzeniem 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) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
3. Dyrektor Ośrodka wykonuje obowiązki administratora danych osobowych i administratora systemów informatycznych, a funkcję Inspektora Ochrony Danych Osobowych sprawuje wyznaczony pracownik w odniesieniu do prowadzonych w Ośrodku zbiorów danych.
4. W systemach informatycznych służących do przetwarzania danych osobowych w Ośrodku stosuje się środki bezpieczeństwa na poziomie wysokim.

Rozdział II

Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym.

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez Inspektora Ochrony Danych Osobowych z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Ośrodku wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie

osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych.
3. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na przekazaniu dostępu do hasła oraz ustalenia zakresu dostępnych danych.
4. Inspektor ochrony Danych Osobowych jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Rozdział III

Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Użytkownik uzyskuje dostęp do danych osobowych wyłącznie po podaniu hasła zaraz po włączeniu komputera.
2. Hasło składa się co najmniej z 8 znaków.
3. Hasło powinno zawierać małe i wielkie litery oraz cyfry i znaki specjalnej.
4. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy.
5. Hasło należy zmieniać co najmniej raz na miesiąc.
6. Użytkownik nie może udostępniać osobom nieuprawnionym hasła dostępu oraz osobom nieuprawnionym do swojego stanowiska pracy.
7. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło.
8. Hasła do firmowej poczty elektronicznej nie mogą być zapisane na stałe w programie pocztowym komputera.
9. Zabrania się instalowania oprogramowania nieznanego pochodzenia bez zgody administratora.

Rozdział IV

Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego lub programu pocztowego.
2. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane. Kończąc pracę użytkownik obowiązany jest wyłączyć sprzęt komputerowy. Monitor z danymi wrażliwymi nie może stać przy oknie do którego możliwy jest dostęp dla osób postronnych.

Rozdział V

Korzystanie z bankowości internetowej.

1. Do dokonywania operacji związanych z obsługą bankowości internetowej, dostępu do konta Ośrodka i wykonywania jakichkolwiek operacji, upoważnieni są wyłącznie główny księgowy i osoby upoważnione przez Dyrekcję.

2. Zabrania się przechowywania haseł dostępu do konta na biurku, w dokumentacji ,razem z osobistym kluczem do konta (token), zapisywania w notatkach, w pamięci komputera na dyskach. Hasła i login należy zapamiętać.
3. Osobisty klucz do konta (token) każda z osób, główny księgowy i inne osoby upoważnione, przechowują w sposób należycie zabezpieczony, zapewniający nieużycie przez osoby trzecie. Po wylogowaniu się z banku, w czasie godzin pracy, token zamykany jest na klucz w kontenerach przy biurkach, a na zakończenie dnia pracy, w szafie pancernej.
4. Główny księgowy wprowadza wszelkie dane, które następnie zatwierdza Dyrektor.
5. Zabrania się korzystania z bankowości internetowej na komputerze, na którym stwierdzono źle działającą ochronę, oprogramowanie lub inne problemy.
6. W czasie wykonywania operacji bankowych, zabrania się odchodzenia od komputera, przyjmowania rozmów telefonicznych i załatwiania innych spraw.

Rozdział VI

Tworzenie kopii zapasowych zbiorów danych.

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie raz na pół roku kopii zapasowych.
2. Kopie zapasowe przechowywane są na dysku zewnętrznym w szafie pancernej.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
4. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
5. Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii.

Rozdział VII

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego i danych wrażliwych.

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator danych osobowych.
2. System antywirusowy zainstalowany jest w każdym komputerze.
3. Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym lub programie pocztowym.
4. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora bezpieczeństwa informacji.

Rozdział VIII

Udostępnianie danych osobowych i sposób odnotowywania informacji

o udostępnianiu danych.

1. Dane osobowe przetwarzane w Ośrodku mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy Rozporządzenia 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) oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek chyba, że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Ośrodkowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Dokładna kopia danych osobowych przesłanych do Zakładu Ubezpieczeń Społecznych przechowywana jest w bazie danych programu ..... w postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia dokumentu, datą wysłania zestawu,
5. Dokładna kopia danych osobowych przesłanych do banku przechowywana jest w bazie danych systemu bankowości elektronicznej do wejścia, której konieczne jest wprowadzenie loginu i hasła.

Rozdział IX

Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych.

1. Wszelkie prace związane z naprawami sprzętu komputerowego wykonywane są przez firmę zatrudnioną na podstawie umowy z klauzulą powierzenia przetwarzania danych osobowych i zachowaniem tajemnicy.
2. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora danych osobowych.