Złocieniec, 17.12.2018 r.

Zarządzenie nr 12/2018

Dyrektora Złocienieckiego Ośrodka Kultury

z dnia 17 grudnia 2018 roku w sprawie przeprowadzenia weryfikacji sald kont syntetycznych i analitycznych widniejących w księgach rachunkowych Złocienieckiego Ośrodka Kultury na dzień bilansowy 31.12.2018 rok.

Na podstawie art. 17 ustawy z dnia 25 października 1991r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz.U. z 2002r. poz. 406 z późn. zm.) oraz na podstawie ustawy z dnia 29 września 1994r. o rachunkowości (Dz.U. nr 121 poz.591 z późn. zm.) zarządzam co następuje:

§ 1 Zarządzam przeprowadzenie weryfikacji sald kont syntetycznych i analitycznych widniejących w księgach rachunkowych Złocienieckiego Ośrodka Kultury na dzień bilansowy 31.12.2018r.

§ 2 W celu przeprowadzenia weryfikacji sald wyznaczam komisję weryfikacyjną w składzie:

1. Grażyna Skwirowska – główny specjalista ds. administracji
2. Julianna Szulc – księgowa

§ 3 Wyznaczam czas pracy komisji w terminie 02.01.2019r. – 20.03.2019r.

1. Z przeprowadzonej weryfikacji komisja sporządzi protokół, który zostanie dołączony do bilansu.
2. Protokół weryfikacji sald komisja przekaże głównej księgowej.

§ 4 Przeprowadzenie weryfikacji sald powierzam członkom komisji weryfikacyjnej.

§ 5 Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Złocienieckiego Ośrodka Kultury
Jolanta Smulska

ZŁOCIENIECKI OŚRODEK KULTURY
ul.Polczyńska 6, 78-520 Złocieniec/3/
tel. 94 367 14 55
NIP 674-10-04-170, REG.000287094

ZARZĄDZENIE NR 11 / 2018
DYREKTOR ZŁOCIENIECKIEGO OŚRODKA KULTURY

z dnia 26 listopada 2018 r.

w sprawie wprowadzenia dokumentacji opisującej ochronę danych w tym danych osobowych w Złocienieckim Ośrodku Kultury ul. Połczyńska 6 w Złocieńcu

Na podstawie art. 24 ust. 2 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) (Dz.U.UE. z 2016 r., L 119, poz. 1), zarządza się, co następuje:

§1 1. Wprowadzam „Politykę ochrony informacji systemów informatycznych służących do przetwarzania danych, w tym danych osobowych w Złocienieckim Ośrodku Kultury" w brzmieniu określonym w załączniku nr 1 do zarządzenia;

2. Wprowadzam „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych w tym danych osobowych w Złocienieckim Ośrodku Kultury" w brzmieniu określonym w załączniku nr 2 do zarządzenia.

§3. Zarządzenie wchodzi w życie z dniem podjęcia.

Dyrektor
Złocienieckiego Ośrodka Kultury

Jolanta Smulska

ZARZĄDZENIE NR 11 / 2018
DYREKTOR ZŁOCIENIECKIEGO OŚRODKA KULTURY

z dnia 26 listopada 2018 r.

w sprawie wprowadzenia dokumentacji opisującej ochronę danych w tym danych osobowych w Złocienieckim Ośrodku Kultury ul. Połczyńska 6 w Złocieńcu

Na podstawie art. 24 ust. 2 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) (Dz.U.UE. z 2016 r., L 119, poz. 1), zarządza się, co następuje:

§1 1. Wprowadzam „Politykę ochrony informacji systemów informatycznych służących do przetwarzania danych, w tym danych osobowych w Złocienieckim Ośrodku Kultury" w brzmieniu określonym w załączniku nr 1 do zarządzenia;

2. Wprowadzam „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych w tym danych osobowych w Złocienieckim Ośrodku Kultury" w brzmieniu określonym w załączniku nr 2 do zarządzenia.

§3. Zarządzenie wchodzi w życie z dniem podjęcia.

Dyrektor
Złocienieckiego Ośrodka Kultury

Jolanta Smulska

Złocieniec 2018

Złocieniecki Ośrodek Kultury
ul. Połczyńska 6
78-520 Złocieniec

Autor:
Inspektor Ochrony Danych
Ireneusz Sabat

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

służącym do przetwarzania danych, w tym danych osobowych w Złocienieckim Ośrodku Kultury

Opracował:
Inspektor Ochrony Danych

..... DATA

..... INSPEKTOR OCHRONY DANYCH

Zatwierdził:
Dyrektor Złocienieckiego Ośrodka Kultury

26.11.2018 DATA

DYREKTOR
Złocienieckiego Ośrodka Kultury
Jolanta Smulska
..... ADMINISTRATOR

SPIS TREŚCI

ART. 1. CEL INSTRUKCJI

§1. Zgodnie z art. 24 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych RODO, w przypadku zbierania i przetwarzania danych osobowych, Administrator tych danych ma obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie, którego dokonuje, odbywało się zgodnie z tym rozporządzeniem.

Środki te obejmować powinny wdrożenie przez Administratora odpowiednich polityk ochrony danych oraz regulacji wewnętrznych, określających proporcjonalnie w stosunku do podejmowanych czynności przetwarzania danych osobowych i określonego ryzyka, związanego z tym przetwarzaniem, zapewniając zgodność z prawem, rzetelność i przejrzystość w stosunku do osoby, której dane dotyczą.

Celem niniejszego dokumentu jest więc bezpośrednie określenie sposobu zarządzania systemem informatycznym służącym do przetwarzania danych w tym danych osobowych w Złocienieckim Ośrodku Kultury, w celu zabezpieczenia przed zagrożeniami, w szczególności przed utratą poufności, integralności, uszkodzeniem lub trwałym zniszczeniem zgromadzonych danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych w tym danych osobowych powinna być zatwierdzona przez Administratora i przyjęta do stosowania, jako obowiązujący dokument.

Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację, stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.

ART. 2. PODSTAWOWE DEFINICJE

§2. Ilekroć w niniejszym dokumencie jest mowa o:

1. **Administratorze** rozumie się przez to Złocieniecki Ośrodek Kultury w Złocieńcu, w imieniu którego działa Dyrektor, który decyduje o celach i środkach przetwarzania danych w jednostce oraz wdraża odpowiednie środki techniczne i organizacyjne, o których mowa w art. 24 RODO
2. **Administratorze Systemu Informatycznego** – rozumie się przez to osobę zajmującą się zarządzaniem systemem informatycznym i odpowiadającą za jego sprawne i ciągłe działanie. ASI dokonuje niezbędnych czynności technicznych, których zadaniem jest sprawdzanie bieżących zabezpieczeń systemu informatycznego, podnoszenie ich do poziomu adekwatnego do założeń wynikających z przeprowadzanych analiz ryzyka, oraz przeprowadzanie modernizacji i doposażeni sprzętowych umożliwiających ciągłość działania systemu informatycznego.
3. **Danych biometrycznych** rozumie się przez to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
4. **Danych dotyczące zdrowia** rozumie się przez to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.
5. **Danych genetycznych** rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
6. **Danych osobowych** rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można pośrednio lub bezpośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
7. **Haśle** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym Administratora.
   Przy czym za hasło odpowiadające minimalnym wymaganiom uznaje się hasło

o długości minimum 8 znaków zawierające w sobie duże i małe litery, cyfry oraz przynajmniej jeden znak specjalny.

8. **Identyfikatorze użytkownika** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. **Inspektorze Ochrony Danych** rozumie się przez to osobę, powołaną przez Administratora na podstawie art. 37 RODO, realizującą zadania o których mowa w art. 39 RODO.
10. **Administratorze Systemów Informatycznych** rozumie się przez to osobę zajmującą się zarządzaniem systemem informatycznym i odpowiadającą za jego sprawne i ciągłe działanie.
11. **Instrukcji** rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych w tym danych osobowych w Złocienieckim Ośrodku Kultury.
12. **Naruszeniu ochrony danych osobowych** rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
13. **Odbiorcy** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
14. **Organie nadzorczym** rozumie się przez to niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO. Zgodnie z ustawą o ochronie danych jest to Prezes Urzędu Ochrony Danych Osobowych.
15. **Osobie upoważnionej do przetwarzania danych osobowych** rozumie się przez to osobę, która została pisemnie upoważniona do przetwarzania danych osobowych przez Administratora w ściśle określonym zakresie co do danych podlegających przetwarzaniu oraz ram czasowych ważności upoważnienia.
16. **Podmiocie przetwarzającym** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane w imieniu Administratora.
17. **Polityce ochrony informacji** rozumie się przez to Politykę ochrony informacji systemów informatycznych służących do przetwarzania danych, w tym danych osobowych w Złocienieckim Ośrodku Kultury.

18. **Profilowaniu** rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
19. **Przetwarzaniu** rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
20. **Pseudonimizacji** rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji lub narzędzi. Pseudonimizacja danych osobowych ogranicza możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą.
21. **RODO** rozumie się przez to Rozporządzenie 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
22. **Serwisancie** rozumie się przez to firmę lub pracownika firmy zajmującego się aktualizacją lub instalacją oprogramowania (specjalistyczny serwis oprogramowania).
23. **Sieci publicznej** rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt.28 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U.2004.171.1800).
24. **Sieci teleinformatycznej** rozumie się przez to służącą do przetwarzania danych osobowych organizacyjnie i technicznie połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami.
25. **Sieci telekomunikacyjnej** rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt.35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (DZ.U.2004.171.1800).
26. **Stronie trzeciej** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
27. **Systemie informatycznym Administratora** rozumie się przez sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole

współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje przynajmniej jeden komputer centralny wraz ze stacjami roboczymi i system ten tworzy sieć teleinformatyczną.

28. **Teletransmisji** rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

29. **Ustawie o ochronie danych** rozumie się przez to ustawę z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018. Poz. 1000)

30. **Uwierzytelnianiu** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości.

31. **Użytkowniku** rozumie się przez to osobę upoważnioną do dostępu i przetwarzania danych osobowych, której nadano Identyfikator użytkownika i przyznano hasło.

    W szczególności Inspektor ochrony danych z upoważnienia Administratora czuwa nad przestrzeganiem realizacji zapisów RODO, przepisów ustawy o ochronie danych i innych przepisów z zakresu ochrony danych, współpracuje z organem nadzorczym i stanowi punkt konsultacyjno – doradczy w sprawach związanych z ochroną danych.

32. **Zabezpieczeniu danych w systemie informatycznym** rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

33. **Zabezpieczeniu systemu informatycznego** rozumie się przez to wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

34. **Zbiorze danych** rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

35. **Zgodzie osoby, której dane dotyczą** rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

ART. 3. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH W TYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

§3. 1. Każdy nowo zatrudniony pracownik Złocienieckiego Ośrodka Kultury a w szczególności użytkownik systemu informatycznego, którego zakres obowiązków służbowych obejmuje bądź może obejmować przetwarzanie danych osobowych, przed przystąpieniem do czynności służbowych zobowiązany jest do odbycia szkolenia w zakresie ochrony powierzonych mu danych a w szczególności do zapoznania się z treścią i stosowania:

1) 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)
2) ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000),
3) Polityki ochrony informacji Systemów informatycznych służących do przetwarzania danych, w tym danych osobowych w Złocienieckim Ośrodku Kultury,
4) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w tym danych osobowych w Złocienieckim Ośrodku Kultury.

§4. W Złocienieckim ośrodku Kultury wyróżnia się następujące systemy informatyczne służące do przetwarzania danych osobowych:

1. Systemy scentralizowane obejmujące przetwarzanie danych osobowych w centralnych bazach, których administratorem jest inny podmiot niż Złocieniecki Ośrodek Kultury:
   1) System Bankowości Elektronicznej.
2. Lokalne systemy bazodanowe użytkowane w Złocienieckim Ośrodku Kultury:
   1) System finansowo – księgowy Zakładu Elektronicznej Techniki Obliczeniowej w Koszalinie,
   2) System Płatnik.
3. System rozproszonych danych w postaci plików danych osobowych w formie arkuszy kalkulacyjnych, plików tekstowych zgromadzonych lokalnie na dyskach komputerów.

§5. Procedura nadawania uprawnień do systemu informatycznego.

1. Dostęp do Systemu Bankowości Elektronicznej nadawany jest dla osoby reprezentującej Złocieniecki Ośrodek Kultury przez oddział banku lub inną jego placówkę, na podstawie pisemnego upoważnienia.

2. Dostęp do systemów informatycznych użytkowanych w Złocienieckim Ośrodku Kultury, o których mowa §4 ust. 2, możliwy jest na podstawie pisemnego wniosku pracownika, kierowany do Administratora.

Wniosek powinien zawierać:

1) Nazwę systemu informatycznego,
2) zakres nowych lub modyfikację istniejących uprawnień do przetwarzania danych osobowych lub nazwy modułów programowych będących składowymi systemu informatycznego
3) okres dostępu do danych (w przypadku zaistnienia konieczności czasowego dostępu do danych).

Wzór wniosku stanowi Załącznik Nr 1 do Instrukcji.

§6. 1. Na podstawie wniosku o nadanie uprawnień w systemie, o którym mowa w §5 ust. 2, Inspektor ochrony danych przeprowadza szkolenie z zakresu ochrony danych osobowych a po jego zakończeniu wystawia pisemne zaświadczenie o odbyciu kursu z zakresu ochrony danych osobowych oraz wystawia upoważnienie do przetwarzania danych osobowych w Złocienieckim Ośrodku Kultury i dokonuje aktualizacji rejestru osób upoważnionych do przetwarzania danych.

Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik Nr 2 do Instrukcji.

2. Na podstawie wniosku o którym mowa w §5 ust. 2 firma świadcząca usługi w zakresie wsparcia informatycznego lub upoważniony przez Administratora pracownik, dokonuje zmiany ustawień systemu informatycznego, tworząc bądź modyfikując ustawienia dla wskazanego użytkownika oraz nadając stosowne uprawnienia.

§7. 1. W przypadku dłuższej nieobecności pracownika, spowodowanej np. długotrwałą chorobą, której okres przekracza 30 dni kalendarzowych, bądź ustaniem zatrudnienia, bezpośredni przełożony pracownika przedkłada Administratorowi informację o tym fakcie, wnioskując o czasowe zawieszenie lub całkowite usunięcie uprawnień pracownika połączone z usunięciem jego konta w systemie informatycznym.

2. Upoważniony przez Administratora pracownik lub firma świadcząca usługi informatyczne wykonuje niezbędne czynności w systemie informatycznym, uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia zostały czasowo zawieszone lub wygasły z powodu ustania zatrudnienia.

§8. 1. W przypadku przetwarzania danych poza systemem informatycznym, Administrator na podstawie ustalonego zakresu obowiązków, kieruje pracownika do Inspektora Ochrony Danych celem przeszkolenia go z zakresu ochrony danych osobowych, na podstawie którego wystawia upoważnienie do przetwarzania powierzonych mu danych określające zakres oraz okres na który zostaje wystawione.

2. W przypadku zmiany zakresu obowiązków analogicznie stosuje się zapisy §8 ust. 1.

§9. Rejestrowanie uprawnień w systemie informatycznym.

1. Inspektor Ochrony Danych prowadzi bieżący rejestr osób posiadających upoważnienia do przetwarzania danych osobowych.

Wzór rejestru osób upoważnionych do przetwarzania danych osobowych w Złocienieckim Ośrodku Kultury stanowi Załącznik Nr 3 do Instrukcji.

Rejestr prowadzony jest w formie elektronicznej lub papierowej.

2. Wykorzystywane systemy informatyczne służące do przetwarzania danych osobowych wyposażone są w moduły administracyjne, umożliwiające nadzór nad użytkownikami, rejestrowanie ich uprawnień w systemie oraz identyfikację personalną poszczególnych użytkowników systemu.

§10. Za proces przetwarzania danych osobowych, realizację zapisów instrukcji oraz zakres uprawnień do danych gromadzonych i przetwarzanych na stanowiskach odpowiadają osoby merytorycznie odpowiedzialne.

§11. 1. Szkolenia z zakresu danych osobowych, prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych oraz nadawanie uprawnień przeprowadza Inspektor Ochrony Danych w uzgodnieniu i w imieniu Administratora..

2. W przypadku dłuższej nieobecności Inspektora Ochrony Danych jego obowiązki w zakresie procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień wykonuje Administrator lub wskazane przez niego osoba.

§12. 1. Czynności techniczne związane z modyfikacją systemu informatycznego umożliwiające zakładanie, zmianę oraz usuwanie użytkowników systemu oraz przypisanych im uprawnień, wykonuje Administrator Systemu Informatycznego lub upoważniony przez Administratora pracownik.

2. W sytuacjach losowych dopuszcza się, że obowiązki związane z technicznymi czynnościami w systemie informatycznym wykonuje na podstawie umowy zlecenia wyspecjalizowana firma zewnętrzna.

ART. 4. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

§13. Metody i środki uwierzytelnienia użytkownika w systemie.

1. W sieci wewnętrznej Złocienieckiego Ośrodka Kultury stosuje się następujące typy dostępu, uwierzytelniania i autoryzacji:

1) Dostęp do sieci wewnętrznej możliwy jest poprzez skonfigurowane routery i switche sieciowe umożliwiające podłączenie przewodowe skrętką UTP kat. 5 lub dostęp bezprzewodowy WiFi w standardzie IEEE 802.11n, IEEE 802.11g, IEEE 802.11b.
2) Dostęp do sieci bezprzewodowej zabezpieczony jest hasłem z typem uwierzytelnienia WPA2-PSK.
3) Adres IP komputera pracującego w sieci wewnętrznej, pobierany jest dynamicznie DHCP z wydzielonej puli adresów sieciowych w oparciu o weryfikację mac adresu karty sieciowej urządzenia, któremu adres sieciowy jest nadawany.

4) Każdy użytkownik posiada imienny login i indywidualne hasło do komputera pracującego w sieci wewnętrznej. Ponadto każda jednostka komputerowa posiada konto administracyjne zabezpieczone hasłem administracyjnym, umożliwiające zmianę konfiguracji jednostki oraz zmianę uprawnień użytkowników.

5) Każdy wdrożony i użytkowany program służący do przetwarzania danych osobowych, posiada wbudowane konto bądź moduł administracyjny, umożliwiający zmianę ustawień użytkowników, konfiguracje ich uprawnień, nadawania określonych zakresem obowiązków ról.

2. Zasady uwierzytelnienia dostępu do stacji roboczych pracujących w sieci wewnętrznej:

1) Każdy komputer pracujący w sieci wewnętrznej ma skonfigurowane konto użytkownika, identyfikujące go jednoznacznie jako użytkownika systemu informatycznego.

2) Identyfikator konta użytkownika stacji roboczej nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego lub w przypadku jego dłuższej nieobecności w pracy, nie powinien być udostępniany bądź przydzielany innej osobie.

3) Konto użytkownika zabezpieczone jest hasłem znanym tylko użytkownikowi.

4) Każdy komputer wyposażony jest w konto administracyjne o nazwie „admin" do którego dostęp posiada Administrator lub osoba przez niego wyznaczona, lub w przypadku zaistnienia takiej potrzeby – firma świadcząca usługi z zakresu IT na rzecz Administratora.

5) Konto administracyjne posiada hasło administracyjne.

3. Zasady uwierzytelniania dostępu do systemów i aplikacji służących do przetwarzania danych osobowych:

1) Dostęp do programów służących do przetwarzania danych osobowych możliwy jest poprzez podanie loginu i hasła dostępu.

2) Login składa się z oznaczenia cyfrowego, literowego bądź literowo-cyfrowego w zależności od możliwości konfiguracji i funkcjonalności stosowanego programu dziedzinowego.

§14. Zasady konstrukcji i przydziału haseł użytkownikom.

1. Użytkownik systemu informatycznego z chwilą utworzenia jego konta w systemie, otrzymuje dedykowany login oraz hasło startowe, które z chwilą pierwszego logowania do systemu, powinien zmienić.

2. Wymagania dotyczące hasła użytkownika:

1) Hasło powinno składać się z minimum ośmiu znaków (przynajmniej jedna duża litera, jedna mała litera, cyfra oraz znak specjalny),

2) Hasło powinno być ciągiem luźno powiązanych znaków nie zawierających w sobie imion, nazw itd.,

3) System wymusza zmianę hasła użytkownika nie rzadziej niż co 30 dni, a w przypadku braku reakcji systemu po upływie ww. okresu użytkownik zobowiązany jest do ręcznej zmiany hasła,

4) Kolejne hasło powinno różnić się od poprzedniego przynajmniej dwoma znakami,

5) System informatyczny zapamiętuje trzy ostatnie hasła użytkownika.

3. Zestawienie kont administracyjnych funkcjonujących w Złocienieckim Ośrodku Kultury stanowi załącznik Nr 4 do instrukcji. Za prowadzenie i aktualizację zestawienia odpowiada Administrator Systemu Informatycznego.

§15. Zasady bezpiecznego użytkowania systemu informatycznego.

1) Login użytkownika systemu podlega wpisowi do rejestru osób posiadających upoważnienie do przetwarzania danych osobowych w Złocienieckim Ośrodku Kultury i po jego wyrejestrowaniu nie może być przydzielony innej osobie;

2) Podczas przetwarzania danych osobowych w systemie posługiwanie się identyfikatorem i hasłem innej osoby jest zabronione;

3) Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu przypisanego mu loginu;

4) Hasło dostępu zapisywane jest na ekranie monitora w formie niejawnej i znane jest tylko użytkownikowi. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł a przechowywanie haseł w formie zapisu ich w widocznych i ogólnie dostępnych miejscach jest niedopuszczalne.

5) W wypadku ujawnienia hasła użytkownika systemu i podejrzenia możliwości wykorzystania go przez osoby nieuprawnione, należy niezwłocznie dokonać jego zmiany na nowe a fakt podejrzenia naruszenia danych osobowych zgłosić Inspektorowi Ochrony Danych a w przypadku jego nieobecności Administratorowi lub osobie przez niego wskazanej.

§16. Zabezpieczenie danych osobowych przetwarzanych w tradycyjnych rejestrach i ewidencjach.

Za zabezpieczenie danych osobowych przechowywanych w tradycyjnych rejestrach i ewidencjach papierowych odpowiadają pracownicy merytoryczni, którym nadano upoważnienia do przetwarzania i powierzono przetwarzanie danych w formie tradycyjnej, a zbiory:

1) Powinny być przetwarzane w wyznaczonych do tego pomieszczeniach lub miejscach na terenie Złocienieckiego Ośrodka Kultury;

2) Przetwarzania zbiorów papierowych powinno następować w taki sposób aby uniemożliwić wgląd i dostęp do tych zbiorów osobom do tego nieupoważnionym;

3) Zakończenie pracy ze zbiorem w formie papierowej powinno skutkować odpowiednim jego zabezpieczeniem, w zamkniętej na klucz szafie do której klucze posiadają jedynie pracownicy upoważnieni do przetwarzania danych osobowych;

4) Bezwzględnie zakazane jest samowolne wynoszenie całych zbiorów bądź ich części poza teren przetwarzania w tym poza lokalizację Złocienieckiego Ośrodka Kultury, bez wiedzy i zgody Administratora, przy czym pracownik powinien umieć wykazać, że zgoda taka została mu wydana.

ART. 5. PRAKTYCZNE PROCEDURY OCHRONY DANYCH PRZY WYKORZYSTYWANIU SYSTEMU INFORMATYCZNEGO

§17. 1. Stosuje się następujące praktyczne procedury zwiększające poziom ochrony danych przy wykorzystywaniu systemu informatycznego na stanowisku pracy:

1) w celu zalogowania do systemu informatycznego, użytkownik podaje swój identyfikator oraz hasło,
2) system jest skonfigurowany w taki sposób, aby po okresie 15 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu identyfikatora i hasła,
3) po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera.
4) w pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie upoważnionego pracownika albo Administratora, Administratora Systemu Informatycznego lub Inspektora Ochrony Danych;
5) monitory komputerów powinny być tak ustawione w pomieszczeniu aby uniemożliwiały bezpośredni odczyt danych na nim wyświetlanych osobom nieupoważnionym;
6) monitory komputerów, które ze względu na specyfikę pomieszczenia, gdzie odbywa się przetwarzanie danych osobowych, nie mogą być odpowiednio zabezpieczone, powinny być wyposażone w specjalne nakładki ograniczające kąt widzenia danych wyświetlanych na monitorze dla osób nieupoważnionych;
7) wszelkie wydruki zawierające dane osobowe powinny być zabezpieczone przed swobodnym dostępem osób nieupoważnionych;
8) dokumenty znajdujące się na biurkach powinny być tak składowane w trakcie pracy, aby zapobiec odczytowi danych na nich zawartych przez osoby nieupoważnione;
9) szafy w których przechowywane są dokumenty powinny być zamknięte a po zakończeniu czynności służbowych zamykane na klucz;
10) wszystkie stacje robocze mogą być poddane bieżącemu monitoringowi, przez Administratora Systemu Informatycznego, który w przypadku zaistnienia takiej potrzeby, przekazuje pisemną informację z przeprowadzonej analizy

Inspektorowi Ochrony Danych, pod kątem wykorzystania powierzonego sprzętu i oprogramowania jak również pod kątem nadzoru bezpieczeństwa sieci wewnętrznej;

11) zabrania się gromadzenia na stacjach roboczych oraz w przestrzeni sieci wewnętrznej, materiałów nie związanych z zakresem wykonywanych obowiązków, w tym zdjęć, plików muzycznych i filmowych oraz innych materiałów i oprogramowania chronionych prawem autorskim;

12) po zakończeniu pracy a przed opuszczeniem obszaru przetwarzania danych osobowych należy:

a. skutecznie zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,

b. schować do zamykanych na klucz szaf karty kryptograficzne używane do identyfikacji użytkownika,

c. schować do zamykanych na klucz szaf akta zawierające dane osobowe,

d. umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,

e. zamknąć okna znajdujące się w pomieszczeniu,

f. zabezpieczyć drzwi wejściowe poprzez zamknięcie ich na klucz i umieszczenie klucza w szafce na klucze.

ART. 6. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

§18. W Złocienieckim Ośrodku Kultury rozróżnić można dwa typy danych, ze względu na ich funkcjonalną strukturę, których wykonywane są kopie zapasowe w postaci zewnętrznych nośników danych bądź danych gromadzonych na nośnikach informacji na wydzielonych strukturach dysków:

1. Bazy danych programów, zgromadzonych w uporządkowanych bazach programów dziedzinowych zgromadzonych centralnie na serwerze głównym, z którym łączą się komputery lokalne użytkowników, pracujących w sieci wewnętrznej Złocienieckiego Ośrodka Kultury.

   Systemy: Finansowo-księgowy, Kadry, Płace, Płatnik, Systemu rezerwacji biletów, Systemu bibliotecznego.

2. Kopie danych zgromadzonych na lokalnych stacjach roboczych pracujących w wewnętrznej sieci Złocienieckiego Ośrodka Kultury, zgromadzone w formie rejestrów i ewidencji lub pojedynczych plików multimedialnych, plików programów biurowych, zawierających w swej treści dane osobowe.

§19 1. Kopie systemów informatycznych, o których mowa w §18 ust. 1 sporządza się w cyklu tygodniowym w formie spakowanej bazy danych programu.

Za sporządzenie kopii odpowiada Administrator Systemu Informatycznego, który nadzoruje ich wykonywanie na wskazanej partycji dysku, w dedykowanym folderze z opisem czasu ich sporządzenia.

2.W celu zminimalizowania ryzyka utraty danych zgromadzonych w bazach systemów informatycznych, sporządza się kopię kwartalną programów o których mowa w §18 ust. 1 na nośniku zewnętrznym. Nośnik przetrzymywany jest w zamykanej szafie w Księgowości.

Kopie kwartalne sporządza Administrator Systemu Informatycznego.

3. Raz w roku sporządza się kopię programu oraz kopię bazy danych programów o których mowa w §18 ust. 1 na zaszyfrowanym nośniku zewnętrznym, którą przechowuje się w zamykanej szafie w księgowości.

Za kopie roczne odpowiada Administrator Systemu Informatycznego.

§20 Kopie danych, o których mowa w §18 ust. 2 wykonywane są w zależności od potrzeb przez użytkowników systemu informatycznego i w sposób przez nich określony na wydzielonych partycjach dysku bądź na zaszyfrowanych nośnikach zewnętrznych w postaci dysków przenośnych lub nośników pendrive. Nośniki te przetrzymywane są w zamykanych szafkach.

§21 Miejsce przechowywania kopii danych:

1. Kopie o których mowa w §19 ust. 1 przechowywane są w lokalnych folderach komputera będącego bazą użytkowanego systemu.
2. Kopie o których mowa w §19 ust. 2 przechowywane są w zamykanej szafie w formie opisanych nośników danych w Księgowości.
3. Kopie o których mowa w § 19 ust. 3 przechowywane są w zamykanej szafie w formie opisanych nośników danych w Księgowości.
4. Kopie o których mowa w §20 przechowywane są w zamykanych szafkach użytkowników systemu.

§22 Wzór ewidencji kopii kwartalnych i rocznych, stanowi Załącznik Nr 5 do instrukcji.

§23. Pozostałe zasady i procedury przechowywania i niszczenia nośników danych, na których przechowywane były archiwizowane dane osobowe.

1. Wszystkie nośniki danych na których dokonane są kopie bezpieczeństwa, należy przynajmniej raz w roku sprawdzić pod kątem ich dalszej przydatności.

2. Stwierdzenie utraty przez kopie awaryjne waloru przydatności, upoważnia do ich zniszczenia.

3. Zniszczenie wszelkich nieprzydatnych nośników danych odbywa się w sposób trwały poprzez wszelkie dostępne techniczne możliwości uniemożliwiające jakikolwiek późniejszy odczyt danych z tych nośników w formie całościowej lub częściowej.

4. Poświadczeniem zniszczenia nośnika jest protokół zniszczenia wykonywany przez osobę wskazaną przez Administratora. Wzór protokołu zniszczenia nośników danych stanowi Załącznik Nr 6 do instrukcji.

ART. 7. SPOSÓB I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

§24. 1. Zabronione jest bez zgody Administratora, wynoszenie poza siedzibę Złocienieckiego Ośrodka Kultury danych osobowych w postaci elektronicznej – zapisywanych na zewnętrznych nośnikach danych, przenośnych pamięciach masowych, dyskach magnetooptycznych czy dyskach twardych.

2. Administrator danych wyraża zgodę określając zakres danych, które podlegają przeniesieniu z miejsca przetwarzania poza ich pierwotną lokalizację, wskazaną do ich gromadzenia i przetwarzania, oraz sposób zabezpieczenia danych przed dostępem dla osób nieupoważnionych.

§25. Miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe na stanowisku pracy:

1. Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są w szufladach bądź szafach wyposażonych w zamki zamykane na klucz, do których dostęp posiadają pracownicy upoważnieni do przetwarzania tych danych osobowych.

2. Kopie kwartalne wszystkich danych, o których mowa w §19 ust. 2, przechowywane są w zamykanej szafie w Księgowości, a dostęp do nich posiada Administrator Systemu Informatycznego, Główny Księgowy oraz Administrator, a w sytuacjach wyjątkowych - osoba przez nich wyznaczona.

3. Kopie roczne, o których mowa w §19 ust. 3, przechowywane są w zamykanej szafie w Księgowości, a dostęp do nich posiada Administrator Systemu Informatycznego, Główny Księgowy oraz Administrator, a w sytuacjach wyjątkowych - osoba przez nich wyznaczona.

§26. Okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.

1. Dane przechowywane na elektronicznych nośnikach informacji, zawierające dane osobowe, przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania, po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

2. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest i eksploatowany wewnątrz Złocienieckiego Ośrodka Kultury w obszarze przetwarzania danych osobowych.

ART. 8. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ SZKODLIWEGO OPROGRAMOWANIA

§27. System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie zabezpieczeń sprzętowych oraz programowych rozwiązań, w zależności od bieżących możliwości oraz względem zaistniałych okoliczności, niezbędnych celem ochrony całego systemu bądź wyodrębnionych danych, których poufność lub integralność mogła by być narażona.

1. Sprzętowe formy zabezpieczenia przed uzyskaniem nieuprawnionego dostępu do systemu:

Za sprzętową formę zabezpieczenia sieci wewnętrznej odpowiadają urządzenia sieciowe, których konfiguracja umożliwia bieżący nadzór nad ruchem w sieci wewnętrznej oraz umożliwia autoryzację urządzeń pracujących wewnątrz systemu.

2. Oprogramowanie zabezpieczające system informatyczny przed nieuprawnionym dostępem.

Każda stacja robocza pracująca w sieci wewnętrznej Złocienieckiego Ośrodka Kultury posiada zainstalowany i aktywny program antywirusowy, ze skonfigurowaną codzienną aktualizacją baz danych wirusów oraz z możliwością obsługi centralnej konsoli administracyjnej umożliwiającej bieżący nadzór nad zagrożeniami. Centralny moduł administracyjny programu antywirusowego monitoruje aktualność systemów operacyjnych, występujących na poszczególnych stacjach roboczych zagrożeń oraz aktualizacji baz danych wirusów.

Za wdrożenie i korzystanie z oprogramowania antywirusowego oraz za funkcjonowanie i nadzór nad modułem administracyjnym odpowiada Administrator Systemu Informatycznego, lub w przypadku jego nieobecności, osoba wskazana przez Administratora.

3. Zasady i procedury związane z utrzymaniem podwyższonego poziomu bezpieczeństwa systemu i zabezpieczeniem go przed nieuprawnionym dostępem:

1) Użytkownikom systemu informatycznego nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła.
2) Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik systemu informatycznego.
3) Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
4) Zabrania się pobierania, odczytywania lub rozpakowywania załączników poczty elektronicznej, zwłaszcza pochodzących z niewiadomych źródeł, bez

wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

5) Zabrania się z korzystania i pobierania plików (np. filmów, gier, muzyki itp.) ze wszelkich źródeł typu p2p, tor renty itp.

   Pobieranie i magazynowanie takich plików może powodować konsekwencje łamania praw autorskich oraz generować nadmierny ruch w sieci wewnętrznej, spowalniając jednocześnie przepustowość łącza.

ART. 9. SPOSÓB REALIZACJI UDOSTĘPNIANIA DANYCH OSOBOWYCH ORAZ JEGO EWIDENCJONOWANIA

§28. 1. Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (z wyłączeniem osób: których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, organów państwowych lub organów jednostek, którym dane są udostępniane w związku z prowadzonym postępowaniem lub na podstawie ustawy w związku z którą realizują czynności służbowe), odbywa się poprzez zapisanie tej informacji w stosownej ewidencji.

2. Wzór ewidencji udostępniania danych osobowych stanowi Załącznik nr 8 do Instrukcji.

3. Dopuszcza się prowadzenie elektronicznej ewidencji udostępniania danych osobowych zgodnie z obowiązującym załącznikiem do niniejszej instrukcji.

§29. Za prowadzenie ewidencji odpowiada Administrator lub osoba przez niego wskazana do realizacji niniejszej czynności.

§30. Wzór wniosku o udostępnienie danych osobowych zgromadzonych w bazach i rejestrach oraz ewidencjach zgromadzonych w Złocienieckim Ośrodku Kultury stanowi Załącznik Nr 7 do Instrukcji.

ART. 10. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

§31. Stosowane są następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1. Raz na pół roku Administrator Systemu Informatycznego wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji.

2. W przypadku stwierdzenia nieprawidłowości w działaniu elementów systemu, podejmowane są niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania o czym w formie raportu powiadomiony zostaje Inspektor Ochrony Danych.

3. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności Administratora Systemu Informatycznego, osoby przez niego upoważnionej lub Inspektora Ochrony Danych Osobowych.

4. Jeżeli naprawa lub przywrócenie systemu informatycznego wiązać się będzie z dostępem podmiotu zewnętrznego do zgromadzonych w systemie danych, niezbędne jest podpisanie stosownej umowy powierzenia danych, o której mowa w Załączniku Nr 10 Polityki ochrony informacji.

5. Przeglądu pliku zawierającego raport dotyczący działalność poszczególnych aplikacji bądź systemów serwerowych (log systemowy) dokonuje Administrator Systemu Informatycznego w ramach przeprowadzanych audytów i monitoringu systemu lub w przypadku zaistnienia nieprawidłowości w działaniu systemu.

6. Z przeprowadzonych czynności naprawy lub przywrócenia systemu informatycznego, Administrator Systemu Informatycznego lub osoba przez niego wskazana, przeprowadza służbową notatkę, którą przekazuje Inspektorowi Ochrony Danych.

7. Raz w roku do dnia 31 grudnia Administrator Systemu Informatycznego sporządza ogólny raport z działania systemu oraz z przeprowadzonych w trakcie roku modernizacji i napraw mających wpływ na funkcjonowanie systemu i zmianę bezpieczeństwa przetwarzanych danych w tym danych osobowych. Raport przekazywany jest w formie pisemnej i elektronicznej Inspektorowi Ochrony Danych.

ART. 11. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

§32. Użytkownik zobowiązany jest zawiadomić Administratora lub Administratora Systemu Informatycznego o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła),
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
4) wykryciu wirusa komputerowego, którego program antywirusowy nie jest w stanie wyleczyć,

5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Złocienieckiego Ośrodka Kultury,
6) znacznym lub całkowitym spowolnieniu w działaniu systemu informatycznego,
7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
8) zmianie położenia sprzętu komputerowego,
9) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

§33. Do czasu przybycia na miejsce Administratora lub Administratora Systemu Informatycznego, należy:

1) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu również ustalenie jego przyczyny lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
5) przygotować opis incydentu,
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Systemu Informatycznego.

§34. Administrator lub Administrator Systemu Informatycznego przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować Inspektora Danych Osobowych:

1) o każdym naruszeniu systemu informatycznego mogącym mieć wpływ na dostęp do danych osobowych przez osoby nieupoważnione,
2) o każdym naruszeniu danych osobowych mogącym mieć wpływ na wyciek danych poza jednostkę,
3) o każdym naruszeniu systemu informatycznego mogącym mieć wpływ na integralność lub utratę danych w tym na częściowe lub całkowite uszkodzenia zbiorów zawierających dane osobowe,
4) o każdym naruszeniu danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

§35. Inspektor Ochrony Danych po otrzymaniu zawiadomienia o naruszeniu bądź podejrzeniu naruszenia bezpieczeństwa systemu, powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
2) podjąć działania chroniące system przed ponownym naruszeniem,

3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego urzędu, a następnie niezwłocznie przekazać jego kopie Administratorowi,

§36. 1. Administrator po otrzymaniu pełnej informacji o naruszeniu bezpieczeństwa systemu informatycznego a w tym o naruszeniu danych osobowych, zgodnie z Art. 33 RODO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z Art. 55 RODO, chyba że w ocenie Administratora jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

§37. Zgłoszenie, o którym mowa w §36, musi zawierać co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§38. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych, zawiadamia osobę, której dane dotyczą, o takim naruszeniu, zawierając również informację o których mowa w §35 pkt 2, 3 i 4.

§39. Zawiadomienie o którym mowa w §36 nie jest wymagane w następujących przypadkach:

1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§40. Wzór raportu z naruszenia bezpieczeństwa systemu informatycznego w Złocienieckim Ośrodku Kultury stanowi Załącznik Nr 10 do Instrukcji.

§41. Inspektor Ochrony Danych w uzgodnieniu z Administratorem może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej naruszeniem bezpieczeństwa systemu informatycznego od pozostałej jego części w celu separacji zagrożenia od pozostałej części systemu informatycznego i ograniczenia rozprzestrzeniania się zagrożenia.

§42. W przypadku wystąpienia konieczności odtworzenia danych z kopii zapasowych przez Administratora Systemu Informatycznego, konieczne jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem naruszenia. Dotyczy to zwłaszcza przypadków infekcji wirusowej.

§43. Administrator po zapoznaniu się z raportem, o którym mowa w §40, podejmuje decyzję o dalszym trybie postępowania, o konieczności powiadomienia o którym mowa w §36 oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

§44. Administrator Systemu Informatycznego zobowiązany jest informować Inspektora Ochrony Danych, a ten z kolei zobowiązany jest do informowania Administratora o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

§45. Raz w roku do końca pierwszego kwartału, Inspektor Ochrony Danych przedstawia Administratorowi, pisemną kompleksową analizę zarządzania systemem informatycznym.

ART. 12. ZASADY POSTEPOWANIA Z KOMPUTERAMI PRZENOŚNYMI

§46. 1. Osoba użytkująca komputer przenośny zawierający dane osobowe, po uzyskaniu zgody Administratora, na przeniesienie danych osobowych poza obszar ich przetwarzania, zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.

2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:

1) Jeżeli to tylko możliwe, stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym;
2) Szyfrować poszczególne katalogi zawierające dane osobowe lub całe nośniki danych na których dane osobowe są zapisane;
3) Zabezpieczyć dostęp do komputera przynajmniej na poziomie systemu operacyjnego w formie identyfikatora użytkownika i hasła składającego się z minimum 8 znaków (duża, mała litera, cyfra i znak specjalny);

4) Nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych na nim zgromadzonych;
5) Nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej;
6) Zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych;
7) W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią wewnętrzną Złocienieckiego Ośrodka Kultury, należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz zaktualizowany system antywirusowy;
8) Wykonywać kopie danych zgromadzonych na przenośnym komputerze;
9) W przypadku zgubienia lub kradzieży przenośnego komputera, pracownik zobowiązany jest do natychmiastowego powiadomienia Administratora oraz Inspektora Ochrony Danych lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych, o których mowa w Art. 11 Instrukcji;

3. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego użytkownik;

ART. 13. POSTANOWIENIA KOŃCOWE

§47. W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują:

1) Rozporządzenie 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;
2) Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018r. poz. 1000);
   - Ustawa z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2017r. poz. 570);
   - instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów oraz umów serwisowych;

§48. 1. Niezastosowanie się do procedur określonych w niniejszej Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

2. Niezależnie, osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 102 i art. 107 ustawy o ochronie danych oraz art. 266 Kodeksu karnego.

SPIS ZAŁĄCZNIKÓW

Załącznik Nr 01
do Instrukcji zarządzania systemem informatycznym

WNIOSEK O NADANIE / ZMIANĘ / ZAWIESZENIE * UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

NAZWA ZBIORU DANYCH OSOBOWYCH / SYSTEMU INFORMATYCZNEGO		
.....		
NADANIE UPRAWNIEŃ ☐	ZMIANA UPRAWNIEŃ ☐	ZAWIESZENIE UPRAWNIEŃ ☐
IMIĘ I NAZWISKO UŻYTKOWNIKA:	STANOWISKO:	
.....	.....	
OPIS I ZAKRES UPRAWNIEŃ UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM:		
.....		
PRZYCZYNA ORAZ OKRES ZAWIESZENIA POSIADANYCH UPRAWNIEŃ W SYSTEMIE:		
.....		
DATA SPORZĄDZENIA WNIOSKU:	PODPIS PRZEŁOŻONEGO UŻYTKOWNIKA SYSTEMU:	
.....	.....	
DATA NADANIA UPRAWNIEŃ W SYSTEMIE:	PODPIS I AKCEPTACJA INSPEKTORA OCHRONY DANYCH	
.....	.....	

Załącznik Nr 02
do Instrukcji zarządzania systemem informatycznym

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

NR ..... / 20 .....

1. Upoważniam Panią/Pana .....
IMIĘ I NAZWISKO

zatrudnioną/-ego na stanowisku .....

w Złocienieckim Ośrodku Kultury w Złocieńcu, do dostępu do zbiorów danych osobowych lub czynności przetwarzania danych osobowych, zgodnie z zakresem obowiązków na zajmowanym stanowisku pracy (*należy określić zbiory danych osobowych lub określić czynności przetwarzania zgodnie z Polityką Bezpieczeństwa Informacji):*

– .....

– .....

– .....

– .....

– .....

– .....

2. Okres trwania upoważnienia: .....

Zatwierdził: .....
ADMINISTRATOR

3. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik Nr 03
do Instrukcji zarządzania systemem informatycznym

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W ZŁOCIENIECKIM OŚRODKU KULTURY

LP.	NAZWA ZBIORU DANYCH OSOBOWYCH	IMIĘ I NAZWISKO OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH	STANOWISKO	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	UWAGI

Załącznik Nr 04
do Instrukcji zarządzania systemem informatycznym

ZESTAWIENIE KONT ADMINISTRACYJNYCH W ZŁOCIENIECKIM OŚRODKU KULTURY

LP.	NAZWA SYSTEMU / PROGRAMU / ZBIORU DANYCH OSOBOWYCH / URZĄDZENIA / INNEGO DOSTĘPU Z UPRAWNIENIAMI ADMINISTRATORA	MIEJSCE UŻYTKOWANIA BĄDŹ LOKALIZACJA	LOGIN	HASŁO	UWAGI

Załącznik Nr 05
do Instrukcji zarządzania systemem informatycznym

EWIDENCJA KOPII ROCZNYCH / KWARTALNYCH*
ZGROMADZONYCH DANYCH OSOBOWYCH W ZŁOCIENIECKIM OŚRODKU KULTURY

LP.	NAZWA SYSTEMU / PROGRAMU / BAZY DANYCH OSOBOWYCH	DATA SPORZĄDZENIA KOPII	MIEJSCE PRZECHOWYWANIA	PODPIS

Załącznik Nr 06
do Instrukcji zarządzania systemem informatycznym

PROTOKÓŁ NR .....
ZNISZCZENIA NOŚNIKÓW DANYCH

ZŁOCIENIEC, dnia ..... r.

Komisja w składzie:

1. Przewodniczący: .....
2. Członkowie: .....

.....

Dokonała trwałego zniszczenia następujących nośników komputerowych:

LP	NAZWA / OPIS	NR EWIDENCYJNY / NR SERYJNY	SPOSÓB ZNISZCZENIA	UWAGI
1	2	3	4	5

Dokonane w/w czynności potwierdzone zostają podpisami:

.....

.....

.....

ZATWIERDZAM: .....

ADMINISTRATOR

Załącznik Nr 08
do Instrukcji zarządzania systemem informatycznym

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH PRZETWARZANYCH W ZŁOCIENIECKIM OŚRODKU KULTURY

1. Wniosek do .....
(DOKŁADNE OZNACZENIE ADMINISTRATORA)

2. Wnioskodawca .....

.....
(NAZWA FIRMY I JEJ SIEDZIBA ALBO NAZWISKO, IMIĘ I ADRES ZAMIESZKANIA WNIOSKODAWCY, EW. NIP ORAZ NR REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych innej osoby niż Wnioskodawca:

.....

.....

.....

..... * _ ew ☐ cd. w załączniku nr .....

4. Wskazanie przeznaczenia dla udostępnionych danych:

.....

..... * _ ew ☐ cd. w załączniku nr .....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane: .....

.....

..... * _ ew ☐ cd. w załączniku nr .....

6. Zakres żądanych informacji ze zbioru: .....

.....

..... * _ ew ☐ cd. w załączniku nr .....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych: .....

.....

..... * _ ew ☐ cd. w załączniku nr .....

---------- * Jeżeli TAK, to zakreśla kwadrat literą „x":

.....
DATA

.....
PODPIS I EW. PIECZĘĆ WNIOSKODAWCY

Załącznik Nr 09
do Instrukcji zarządzania systemem informatycznym

EWIDENCJA UDOSTĘPNIONYCH DANYCH OSOBOWYCH

NAZWA ZBIORU / EWIDENCJI / BAZY DANYCH / SYSTEMU INFORMATYCZNEGO ZAWIERAJĄCEGO DANE OSOBOWE:			.....		
LP.	**NAZWA PODMIOTU WYSTĘPUJĄCEGO O UDOSTĘPNIENIE DANYCH OSOBOWYCH**	**CEL UDOSTĘPNIENIA**	**RODZAJ UDOSTĘPNIONYCH DANYCH OSOBOWYCH**	**DATA UDOSTĘPNIENIA**	**IMIĘ I NAZWISKO PRACOWNIKA UDOSTĘPNIAJĄCEGO DANE**

Załącznik Nr 10
do Instrukcji zarządzania systemem informatycznym

ZGŁOSZENIE
NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W ZŁOCIENIECKIM OŚRODKU KULTURY

1. Data ..... godzina .....
DD.MM.RRRR GG:MM

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
IMIĘ I NAZWISKO

.....
STANOWISKO SŁUŻBOWE

3. Opis zaistniałej sytuacji mogącej mieć wpływ na bezpieczeństwo danych osobowych bądź bezpieczeństwo systemu informatycznego:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....
PODPIS OSOBY ZGŁASZAJĄCEJ

4. Przyjęcie zgłoszenia:

☐ ☐ ☐

.....
PODPIS INSPEKTORA OCHR. DANYCH / ADMINISTRATORA DANYCH OSOBOWYCH

Załącznik Nr 11
do Instrukcji zarządzania systemem informatycznym

RAPORT ZE ZGŁOSZENIA
NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W ZŁOCIENIECKIM OŚRODKU KULTURY

1. Data ..... godzina .....
DD.MM.RRRR GG:MM

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
IMIĘ I NAZWISKO

.....

3. Lokalizacja zdarzenia: .....
NR POKOJU / POMIESZCZENIE / STANOWISKO PRACY / SYSTEM INFORMATYCZNY

.....

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące: .....

.....

.....

.....

5. Podjęte działania: .....

.....

.....

.....

.....

6. Przyczyny wystąpienia zdarzenia: .....

.....

.....

.....

7. Postępowanie wyjaśniające: . .....

.....

.....

.....

[ ] : [ ] [ ]

.....
PODPIS INSPEKTORA OCHRONY DANYCH