INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

MYŚLENICKI OŚRODEK KULTURY I SPORTU

ul. Piłsudskiego 20,
32-400 Myślenice

NIP: 6811353451, REGON: 000284888

Zatwierdzenie dokumentu:	01.02.2019	
sporządził (a): Krzysztof Dybeł	inż. Krzysztof Dybeł	INSPEKTOR OCHRONY DANYCH OSOBOWYCH
zatwierdził: Administrator Danych	p.o. Dyrektora Myślenickiego Ośrodka Kultury i Sportu mgr Piotr Szewczyk	

SPIS TREŚCI

1. TERMINY I DEFINICJE

Terminologia obowiązująca w niniejszym dokumencie została zdefiniowana w Polityce Bezpieczeństwa Danych Osobowych (BA01-Polityka bezpieczeństwa DO). Pozostałe terminy zostały zdefiniowane poniżej.

System operacyjny – oprogramowanie zarządzające komputerem, tworzące środowisko do uruchamiania programów komputerowych, kontroli zadań użytkownika i świadczenia usług, np. Microsoft Windows, Apple OS_X, Linux;

System informatyczny (SI) – program komputerowy przetwarzający dane osobowe, osadzony w systemie operacyjnym, oprogramowaniu zarządzającym komputerem;

Informatyk (ASI) – osoba wskazana przez Administratora Danych do obsługi systemu informatycznego;

Sprzęt komputerowy – zestaw urządzeń elektronicznych, służących do przetwarzania danych osobowych; do ww. urządzeń zalicza się komputery stacjonarnych, komputery przenośne, serwery, drukarki, elementy otoczenia sieciowego (routery, switche, etc.).

2. CELE INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

„Instrukcja zarządzania systemami informatycznymi" służy realizacji wymogów prawnych odnoszących się do przestrzegania praw i wolności osób których dane osobowe są przetwarzane w Myślenickim Ośrodku Kultury i Sportu.

„Instrukcja zarządzania systemami informatycznymi" ma umocowanie w ROZPORZĄDZENIU 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.

„Instrukcja zarządzania systemami informatycznymi" jest jednym z fundamentów dla procesów i zasad przetwarzania danych osobowych w Myślenickim Ośrodku Kultury i Sportu.

Strategicznymi celami „Instrukcji zarządzania systemami informatycznymi" jest:

- zapewnienie przetwarzania danych osobowych zgodnie z wymogami prawa w zakresie ochrony danych osobowych,
- zagwarantowanie poszanowania praw i wolności osób fizycznych, których dane są przetwarzane w Myślenickim Ośrodku Kultury i Sportu,
- prowadzenie dokumentacji przetwarzania danych osobowych,
- określenie warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Powyższe cele będą realizowane poprzez wskazanie zasad:

- nadawania uprawnień do systemów informatycznych
- uwierzytelniania w systemach informatycznych
- pracy z systemem informatycznym oraz systemem operacyjnym
- postępowanie z nośnikami danych
- wykonywania kopii bezpieczeństwa.
- zasad wykonywania przeglądów i konserwacji i realizacji napraw systemu informatycznego oraz sprzętu komputerowego

- dokonywania zapisów potwierdzających wykonanie czynności związanych z administracją i konserwacją infrastruktury informatycznej,
- udostępniania informacji przetwarzania danych osobowych określonych we właściwych przepisach.

3. ZAKRES INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

„Instrukcja zarządzania systemami informatycznymi" opisuje sposoby nadawania upoważnień i uprawnień pracownikom oraz innym osobom wykonującym zadania na rzecz Myślenickiego Ośrodka Kultury i Sportu.
Określa sposób pracy w systemie informatycznym i aplikacjach. Określa procedury oraz czynności mające wpływ na zapewnienie bezpieczeństwa organizacyjnego i fizycznego przetwarzanych danych osobowych.

„Instrukcja zarządzania systemami informatycznymi" obowiązuje wszystkich pracowników oraz współpracowników Myślenickiego Ośrodka Kultury i Sportu wykorzystujących do pracy systemy informatyczne przetwarzające dane osobowe, oraz obejmuje wszystkie obszary działania systemów informatycznych gdzie występują dane osobowe.

Naruszenie zasad ochrony danych osobowych wynikających z przepisów prawa oraz przepisów wewnętrznych, w tym „Instrukcji zarządzania systemami informatycznymi" stanowi pogwałcenie obowiązków pracowniczych, które może być sankcjonowane zgodnie z przepisami prawa, m.in. Kodeksem Pracy, Kodeksem Karnym, Kodeks Cywilnym.

4. UPRAWNIENIA DO SYSTEMÓW INFORMATYCZNYCH

4.1.1. Dostęp do systemów informatycznych mogą mieć jedynie osoby będące upoważnione przez Administratora Danych do przetwarzania danych osobowych. Zakres przetwarzania ujęty jest w upoważnieniu.

4.1.2. Administrator Danych nadaje uprawnienia do systemów informatycznych przetwarzających dane osobowe. Zakres uprawnień musi być adekwatny do upoważnienia do przetwarzania danych osobowych.

4.1.3. Uprawnienia są przekazywane użytkownikowi w sposób przyjęty w porządku organizacyjnym.

4.1.4. Uprawnienia użytkowników, którzy przestają przetwarzać dane są niezwłocznie blokowane. Zablokowane konta użytkowników pozostawia się w systemach w celach archiwalnych.

4.1.5. Użytkownikom, którzy zaprzestali pracy w systemie tymczasowo, zawiesza się dostęp do systemu informatycznego. Odblokowanie konta odbywa się za zgodą Administratora Danych.

5. UWIERZYTELNIANIE W SYSTEMACH INFORMATYCZNYCH

5.1.1. W czasie tworzenia konta w systemie informatycznym użytkownikowi przydzielany jest unikalny identyfikator użytkownika, tzw. „login".

5.1.2. Środkiem uwierzytelnienia dostępu do systemu informatycznego jest właściwy identyfikator użytkownika autoryzowany hasłem dostępu.

5.1.3. Pierwsze hasło do systemu informatycznego jest przekazywane użytkownikowi razem z identyfikatorem. Obowiązkiem użytkownika jest zmiana hasła przy pierwszym logowaniu do systemu informatycznego.

5.1.4. Każdy użytkownik dysponuje indywidualnym identyfikatorem oraz hasłem. Użytkownik nie może ujawniać swojego hasła. W przypadku jego ujawnienia użytkownik musi niezwłocznie zmienić hasło.

5.1.5. Użytkownik może pracować na indywidualnej stacji roboczej. Zasady udostępniania konta w systemie operacyjnym stacji są analogiczne do zasad postępowania w przypadku systemu informatycznego przetwarzającego dane osobowe. W wyjątkowych sytuacjach wynikających z przyczyn organizacyjnych możliwe jest odstępstwo od tej reguły.

5.1.6. Hasło musi spełniać następujące wymagania:

a) nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,

b) musi zawierać co najmniej 8 znaków, w tym małe i wielkie litery oraz cyfry lub znaki specjalne,

c) nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,

d) nie może być jednakowe z identyfikatorem użytkownika,

e) musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika w obrębie ostatnich 10 haseł,

f) w trakcie wpisywania, nie może być wyświetlane na ekranie,

g) musi być zmieniane nie rzadziej niż co 30 dni.

5.1.7. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.

5.1.8. Jeżeli to możliwe, system przetwarzający dane osobowe powinien zostać wyposażony w system zarządzania jakością haseł (wymuszanie zmiany oraz pilnowanie jakości hasła).

5.1.9. Administrator Systemów Informatycznych (ASI) prowadzi rejestr przydzielonych identyfikatorów w systemach informatycznych z przypisaniem ich do konkretnych osób.

6. PRACA Z SYSTEMEM INFORMATYCZNYM ORAZ SYSTEMEM OPERACYJNYM

6.1.1. Kontrola stanowiska pracy – czynności wykonywane przed przystąpieniem do przetwarzania danych osobowych powinny w szczególności obejmować:

a) użytkownik powinien sprawdzić czy nie ma oznak fizycznego naruszenia zabezpieczeń,

b) w przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora Danych.

6.1.2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło w opcji logowania. System informatyczny przetwarzający dane osobowe może wykorzystywać mechanizmy zintegrowanej autoryzacji, np. poprzez przez usługę ACTIVE DIRECTORY.

6.1.3. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło w opcji logowania.

6.1.4. Wprowadzenie identyfikatora i hasła należy przeprowadzić w sposób minimalizujący ryzyko podejrzenia przez osoby niepowołane.

6.1.5. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

6.1.6. Użytkownik opuszczając stanowisko pracy musi wylogować się z systemu informatycznego. Może to zrobić bezpośrednio w systemie informatycznym lub przez zablokowanie systemu operacyjnego, jeśli posiada w nim indywidualne konto. System operacyjny blokuje się poprzez jednoczesne wciśnięcie klawiszy „Windows + L”

6.1.7. Bezczynności użytkownika przez okres dłuższy niż 15 minut musi powodować automatyczne wylogowanie z systemu informatycznego lub systemu operacyjnego. Wznowienie pracy po wymaga ponownego logowania do systemu.

6.1.8. Zmiana użytkownika systemu informatycznego musi być poprzedzona wylogowaniem się poprzedniego użytkownika. Niedopuszczalne jest aby dwóch lub więcej użytkowników wykorzystywała wspólnie jedno konto w systemie informatycznym.

6.1.9. Przetwarzanie danych osobowych bezpośrednio w systemie operacyjnym komputera (przez edytor tekstu, np.: open office, ms office) może odbywać się w oparciu o indywidualne konto użytkownika oraz zastosowanie mechanizmów autoryzacji, takich samych, jak dla systemów informatycznych.

6.1.10. Zakończenie pracy w systemie informatycznym dokonuje się poprzez wylogowanie użytkownika ze wszystkich aplikacji oraz systemu operacyjnego komputera.

7. POSTĘPOWANIE Z NOŚNIKAMI DANYCH ORAZ KOPIE BEZPIECZEŃSTWA

7.1.1. Obowiązek wykonania kopii zapasowej danych zawartych w systemach informatycznych spoczywa na Administratorze Danych. Administrator może przekazać ten obowiązek Administratorowi Systemu Informatycznego.

7.1.2. Wykaz nośników danych oraz plan wykonywania kopii zapasowych znajduje się w załączniku nr 1 do niniejszej instrukcji.

7.1.3. Wykonujący kopię zapasową musi mieć pewność, że kopia zapasowa wykonana jest prawidłowo (np. poprzez odczyt komunikatu systemu informatycznego). Przydatność kopii zapasowych powinna być weryfikowana w zaplanowanych odstępach czasu.

7.1.4. Nośniki zawierające kopie zapasowe muszą zostać odpowiednio oznaczone, wskazując nazwę kopii oraz datę jej wykonania.

7.1.5. Przed zbyciem lub przekazaniem nośników informatycznych zawierających dane osobowe lub ich kopie zapasowe należy skutecznie usunąć te dane.

7.1.6. W przypadku braku możliwości skutecznego usunięcia danych osobowych nośnik należy uszkodzić w sposób uniemożliwiający odczyt.

7.1.7. Nośniki informacji zawierające dane osobowe przechowywane są w pomieszczeniach wskazanych jako obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych", w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

7.1.8. Nośniki informacji zawierające dane osobowe nie mogą być wynoszone poza obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych" bez zgody Administratora (danych osobowych).

7.1.9. Zaleca się, aby w miarę możliwości, dane na nośnikach elektronicznych były zabezpieczone hasłem. Metody zabezpieczenia wynikają z analizy ryzyka i odpowiada za nie Administrator Systemu Informatycznego.

7.1.10. Zabrania się pozostawiania nośnika zawierającego dane osobowe bez nadzoru, w miejscach dostępnych dla osób postronnych lub nie posiadających upoważnienia do przetwarzania danych osobowych.

7.1.11. Zaleca się, by nośniki zawierające kopie zapasowe były przechowywane w innej lokalizacji niż robocza (główna) baza danych.

7.1.12. Nie należy przechowywać kopii zapasowych po upływie ich przydatności określonej przepisami prawa oraz zobowiązaniami Administratora Danych.

7.1.13. Zbędne nośniki zawierających dane osobowe muszą zostać skasowane lub zniszczone w sposób uniemożliwiający ich odczytanie. Sposób niszczenia nośników musi wskazać Administrator Danych.

8. ZABEZPIECZANIE SYSTEMU INFORMATYCZNEGO ORAZ SYSTEMU OPERACYJNEGO

8.1. POSTANOWIENIA OGÓLNE

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym ustala się w oparciu o analizę ryzyka w sposób adekwatny do zagrożeń jakie mogą wystąpić w związku z przetwarzaniem danych osobowych. W ramach analizy ryzyka należy uwzględnić rodzaj przetwarzanych danych osobowych ich ilość oraz skutki jakie mogły by się wiązać z naruszeniem tych danych.

Użytkownik zobowiązany jest korzystać ze sprzętu komputerowego w sposób zgodny z jego przeznaczeniem i chronić go przed zniszczeniem, uszkodzeniem, dostępem osób nieupoważnionych.

Otwieranie (demontaż) sprzętu komputerowego, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie samodzielnie jakichkolwiek urządzeń bez zgody Administratora Danych jest zabronione.

8.2. OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

8.2.1. Przez oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego rozumie się:

- wirusy, robaki, konie trojańskie, keyloggery, cryptolockery itp. – oprogramowanie, rozprzestrzeniające się w sieci informatycznej i instalujące się samoczynnie w systemach informatycznych,
- exploity – powszechnie dostępne programy, wykorzystujące znane błędy w systemach informatycznych, umożliwiające nieuprawnione korzystanie z systemu informatycznego,
- skanery sieci, portów, programy do podsłuchu i analizy ruchu sieciowego, skanery luk bezpieczeństwa itp. –oprogramowanie do rozpoznania potencjalnych celów i przygotowania właściwego ataku, wykorzystującego wykryte luki w zabezpieczeniach systemu informatycznego.

8.2.2. Minimalizacja prawdopodobieństwa zainfekowania systemu informatycznego szkodliwym oprogramowaniem.

- Samodzielna - bez zgody Administratora Danych instalacja oprogramowania jest zabroniona.
- Zabrania się użytkownikom dokonywania jakichkolwiek zmian w konfiguracji zainstalowanego oprogramowania, w szczególności dotyczy to oprogramowania zabezpieczającego takiego: programy antywirusowe, systemy firewall.
- Zabrania się użytkowania nie zautoryzowanych przez ASI nośników danych (płyty CD/DVD, karty pamięci, przenośne twarde dyski itp.).
- Zabrania się użytkowania nośników danych (płyty CD/DVD, karty pamięci, przenośne twarde dyski itp.) bez wcześniejszego sprawdzenia ich oprogramowaniem antywirusowym.
- Prowadzi się jak najczęstszą aktualizację elementów systemu informatycznego o wymagane poprawki bezpieczeństwa.
- Prowadzi się jak najczęstszą aktualizację systemów antywirusowych oraz reguł systemów wykrywania włamań (IDS - Intrusion Detection System).

8.2.3. Sprzęt i czynności, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania oprogramowania:

- Separacja wewnętrznej sieci komputerowej za pomocą zapory, tzw. „firewall".
- Wyłączenie nieużywanych usług systemu informatycznego.
- Ograniczenie uprawnień użytkowników do niezbędnego minimum.
- Stosowanie podziału na podsieci (wydzielanie vlanów).

- Stosowanie szyfrowanych kanałów dostępu do sieci z zewnątrz (VPN, RDP, SSH).

8.2.4. Ochrona antywirusowa

- Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed wpływem szkodliwego oprogramowania jest niedopuszczalne.
- Dostęp do konfiguracji oprogramowania konfiguracyjnego musi być dostępny jedynie dla Administratora Systemu Informatycznego.
- Każdy element wprowadzany / zapisywany w komputerze, w tym załączniki do korespondencji elektronicznej „e-mail", musi zostać sprawdzony za pomocą programu antywirusowego.

8.3. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

8.3.1. Przesyłanie informacji za pomocą służbowej poczty elektronicznej może odbywać się tylko przez osoby do tego upoważnione.

8.3.2. W przypadku przesyłania informacji chronionych bądź wszelkich danych osobowych należy wykorzystywać mechanizmy szyfrujące (np. pakowanie i hasłowanie wysyłanych plików, podpis elektroniczny).

8.3.3. Użytkownicy SI powinni zwracać szczególną uwagę na poprawność adresu odbiorcy/nadawcy dokumentu.

8.3.4. W korespondencji nadesłanej przez nieznanego nadawcę nie wolno otwierać załączników (plików) oraz zawartych w treści tzw. linków do stron internetowych. Nie wolno otwierać podejrzanych załączników nadanych przez znanego nadawcę. W razie wątpliwości o podejrzanej korespondencji powiadomić Administratora Danych lub Informatyka.

8.3.5. Użytkownicy SI powinni kasować niepotrzebne wiadomości pocztowe w zaplanowanych odstępach czasu.

8.3.6. Zabrania się:

- korzystania w Myślenickim Ośrodku Kultury i Sportu z prywatnej poczty elektronicznej(w tym także do celów służbowych),
- rozsyłania niezamówionych ofert, ogłoszeń komercyjnych,
- rozsyłania tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej, zbierają adresy e-mail),
- rozsyłania treści wulgarnych, materiałów erotycznych oraz pornograficznych,
- rozsyłania treści niezgodnych z obowiązującymi przepisami prawa,
- rozsyłania treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie.

8.3.7. Korespondencja przekazywana przez system pocztowy jest własnością Administratora Danych.

8.3.8. Administrator Danych ma prawo kontrolować korespondencję przekazywaną za pośrednictwem systemy poczty elektronicznej. Kontrola prowadzona przez Administratora Danych powinna odbywać się przy obecności użytkownika.

8.4. KORZYSTANIE Z SIECI INTERNET

8.4.1. Sieć Internet w Myślenickim Ośrodku Kultury i Sportu służy do realizacji zadań służbowych,

8.4.2. Zabronione jest:

- przesyłanie lub udostępnianie w sieci Internet jakichkolwiek informacji lub danych chronionych z naruszeniem zasad opisanych dokumentacji ochrony danych osobowych przy pomocy narzędzi typu: e-mail, ftp, chmura publiczna, WWW lub do połączeń bezpośrednich P2P (np.: torrent, direct connect),
- łamanie praw autorskich lub licencyjnych poprzez pobieranie lub rozpowszechnianie treści prawnie chronionych, w tym plików audiowizualnych (np.: mp3, wma, avi, DivX), publikacji (e-book), oprogramowania,
- korzystanie z portali społecznościowych oraz usług typu chat, blog (za wyjątkiem sytuacji wynikających z polecenia Administratora w tym zakresie),
- stosowanie niezatwierdzonych komunikatorów internetowych,
- wykorzystywanie w Internecie przydzielonych do celów służbowych loginów i haseł,
- wchodzenie na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.

8.4.3. Użytkownik może zostać pociągnięty do odpowiedzialności porządkowej za szkody spowodowane przez oprogramowane ściągnięte z Internetu i przez niego zainstalowane.

8.4.4. Zapamiętywanie haseł oraz autouzupełnianie formularzy przez przeglądarki internetowe musi być wyłączone.

8.5. PRZESYŁANIE DANYCH OSOBOWYCH

8.5.1. Przesyłanie danych osobowych lub innych informacji chronionych za pośrednictwem służbowej poczty elektronicznej lub innych kanałów informatycznych jest dozwolone za zgodą Administratora Danych z zachowaniem zasad bezpieczeństwa:

- należy zweryfikować prawidłowość adresu odbiorcy danych,
- należy zminimalizować ilość przesyłanych danych do niezbędnego minimum,
- przesyłane dane muszą zostać zaszyfrowane z zachowaniem wymogu jakości hasła, które powinno zawierać co najmniej 8 znaków, w tym małe i duże litery, cyfry lub znaki specjalne,
- hasło musi zostać przekazane odbiorcy innym kanałem niż informacja (dane osobowe),
- udostępnienie danych osobowych przez pocztę elektroniczną musi być możliwe do udokumentowania na potrzeby informacyjne względem osób, których dane dotyczą.

8.6. ZABEZPIECZENIE PRZED WAHANIAMI LUB ZANIKIEM ZASILANIA

Komputery, na których pracuje system informatyczny powinny zostać zabezpieczone przed wahaniami lub zanikiem zasilania. Komputery, na których pracują bazy danych (serwery) muszą być zabezpieczone obowiązkowo. Zabezpieczenie może odbywać się przez system zasilania awaryjnego (UPS). Administrator Danych powinien wyznaczyć oraz przeszkolić osobę, która będzie odpowiedzialna za bezpieczne wyłączenie serwera w sytuacji zaniku zasilania.

9. PRZEGLĄDY, KONSERWACJA I NAPRAWA SYSTEMU INFORMATYCZNEGO ORAZ SPRZĘTU KOMPUTEROWEGO

9.1. MIEJSCE WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI.

9.1.1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych".

9.1.2. Jeżeli przeglądy i konserwacje są realizowane przez pracowników firm zewnętrznych, a w trakcie prac mają oni dostęp do danych osobowych to musi być zawarta umowa powierzenia danych osobowych pomiędzy Administratorem Danych a firmą zewnętrzną. W przypadkach gdzie ryzyko ujawnienia danych osobowych wiązało by się z poważnymi sankcjami zaleca się dodatkowo zawrzeć „Umowę o zachowaniu poufności NDA".

9.1.3. W przypadku przekazywania sprzętu komputerowego do naprawy z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służącym do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych. Za prawidłowość przeprowadzonych działań odpowiada Administrator Danych.

9.2. CZĘSTOTLIWOŚĆ WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI.

Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

9.3. NADZÓR NAD PRZEGLĄDAMI I KONSERWACJĄ - DOKUMENTOWANIE DZIAŁAŃ.

Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji, napraw sprzętu komputerowego oraz systemu informatycznego służącego do przetwarzania danych osobowych pełni Administrator Danych. Administrator Danych prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji.

9.4. RESTRYKCJE.

Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych bez zgody Administratora Danych.

10. EWIDENCJA WPISÓW, UDOSTĘPNIANIE INFORMACJI

10.1. FUNKCJONALNOŚĆ OPROGRAMOWANIA PRZETWARZAJĄCEGO DANE OSOBOWE

10.1.1. Administrator (danych osobowych) zobowiązany jest używać oprogramowania umożliwiającego rejestrację następujących parametrów:

- data pierwszego wprowadzenia danych osobowych do zbioru,
- identyfikator osoby wprowadzającej te dane,
- źródło tych danych (w przypadku pozyskanie nie od osoby której te dane dotyczą),
- informacje o udostępnieniu danych osobowych,
- sprzeciw dotyczący przetwarzania danych osobowych.

10.1.2. Administrator (danych osobowych) jest odpowiedzialny za stosowanie w organizacji systemów informatycznych (oprogramowania przetwarzającego dane osobowe), realizującego wymogi określone w powyższych punktach. Informację o możliwościach systemów w tym zakresie należy pozyskać od dostawców użytkowanego oprogramowania. W przypadku braku zgodności oprogramowania należy rozważyć jego wymianę.

10.2. REJESTRACJA INFORMACJI O ODBIORCACH DANYCH OSOBOWYCH

10.2.1. Niezależnie od cech systemów informatycznych Administrator Danych prowadzi rejestr udostępnień danych osobowych. Prowadzony rejestr zawiera w szczególności:

- imię i nazwisko lub nazwa odbiorcy,
- data udostępnienia oraz zakres udostępnienia.

10.2.2. Wzór rejestru udostępnień danych osobowych jest załącznikiem do „Polityki bezpieczeństwa danych osobowych".

11. ZARZĄDZANIE DOKUMENTEM

Dokument wchodzi w życie z dniem podpisania przez Administratora.

Właścicielem tego dokumentu jest Administrator Danych lub upoważniona przez niego osoba.

Dokumentacja niniejszej polityki zawiera:

Załącznik nr 1. Wzorcowy plan wykonywania kopii zapasowych.
Załącznik nr 2. Wzór zakresów obowiązków ASI.

Załączniki stanowią integralną część dokumentu – wymagają nadzoru, jednak dokonywane w nich zmiany (zawartość, sposób prezentacji) nie wymagają aktualizacji polityki bezpieczeństwa.

Aktualna wersja oraz data wydania jest wymaganym elementem identyfikacji załącznika.

12. HISTORIA DOKUMENTU.

Data / wydanie	Opis zmiany
20.09.2018 r. / v1	Utworzenie dokumentu.

Załącznik nr 1 do
Instrukcji Zarządzania Systemem Informatycznym
Wzór wykazu elektronicznych nośników danych oraz plan wykonywania kopii zapasowych

Wykaz elektronicznych nośników danych oraz plan wykonywania kopii zapasowych				
Nazwa baz danych, które podlegają wykonaniu kopii zapasowej	**Główny nośnik danych**	**Sposób sporządzania kopii**	**Miejsce przechowywania kopii zapasowej**	**Okres przechowywania kopii**

zaakceptował : .....
(podpis Administratora)

Załącznik nr 2 do
Instrukcji Zarządzania Systemem Informatycznym
Wzór zakresu obowiązków administratora systemów informatycznych - ASI

Myślenice, data: ..... r.

W oparciu o umowę na świadczenie usług informatycznych zawartą dnia 20.09.2018 r. pomiędzy :
Myślenickim Ośrodkiem Kultury i Sportu, ul. Piłsudskiego 20, 32-400 Myślenice,
a .....
zostaje powołana/ny do pełnienia funkcji i obowiązków administratora systemów informatycznych – ASI.
W związku z czym zobowiązuje się do realizacji następujących zadań w stosunku do Myślenickiego Ośrodka Kultury i Sportu.

lp.	Zakres obowiązków	Czas realizacji
1.	Administrowanie systemem informatycznym MOKIS	Bezpieczeństwo Danych osobowych w MOKIS
2.	Aktualizacja zabezpieczeń DO	Bezpieczeństwo Danych osobowych w MOKIS
3.	Wykonywanie kopii zapasowych	Bezpieczeństwo Danych osobowych w MOKIS
4.	Naprawy oraz zabezpieczenie powierzeń danych na nośnikach elektron.	Bezpieczeństwo Danych osobowych w MOKIS
5.	Informowanie ADO o zagrożeniach	Bezpieczeństwo Danych osobowych w MOKIS
6.	Współpraca z IOD – Krzysztofem Dybłem	Bezpieczeństwo Danych osobowych w MOKIS
7.		
8.		
9.		
10.		
11.		
12.		
13.		

....

Administrator Systemów Informatycznych Administrator Danych