Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania Danych Osobowych

Cieszyński Ośrodek Kultury „Dom Narodowy"

Rynek 12

43-400 Cieszyn

Zatwierdzenie dokumentu: 11.05.2017 r.

sporządził:	Janusz Dębowski	ABI/DPO/IOD/Audytor Janusz Dębowski .....
zatwierdził:	Administrator Danych	DYREKTOR COK "DOM NARODOWY" ..... mgr Monika Sikora Monkiewicz

Spis treści

1. Informacje ogólne

1.1. Dokument spełnia wymogi ustawy z dnia 29.08.1997 o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), 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).

1.2. Instrukcja zarządzania systemami informatycznymi opisuje sposoby nadawania upoważnień i uprawnień pracownikom oraz innym osobom wykonującym zadania na rzecz Cieszyńskiego Ośrodka Kultury „Dom Narodowy" określa sposób pracy w systemie informatycznym i aplikacjach. Określa procedury oraz czynności mające wpływ na zapewnienie bezpieczeństwa organizacyjnego i fizycznego przetwarzanych danych osobowych. Instrukcja obowiązuje wszystkich pracowników oraz pozostałe osoby zaangażowane w przetwarzania danych osobowych.

1.3. Terminologia obowiązująca w niniejszym dokumencie została częściowo zdefiniowana w dokumencie Polityki Bezpieczeństwa Danych Osobowych. Pozostałe terminy zdefiniowane są poniżej.

1.4. Definicje

1.4.1. Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024)

1.4.2. System operacyjny – oprogramowanie zarządzające komputerem, tworzące środowisko do uruchamiania programów komputerowych i kontroli zadań użytkownika, np. Microsoft Windows, Apple OS X, Ubuntu.

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

1.4.4. Informatyk (ASI) – osoba wskazana przez Administratora Danych do obsługi systemu informatycznego,

1.4.5. 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. Uprawnienia do systemów informatycznych (§ 5 ust.1 rozporządzenia).

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

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

2.3. Administrator Danych może zarejestrować w systemie uprawnienia użytkownika osobiście lub zlecić to zadanie ASI. Administrator Danych nadaje użytkownikom uprawnienia do systemów informatycznych adekwatne do potrzeb przetwarzania danych. Uprawnienia mogą być zmieniane w zależności od potrzeb Administratora Danych.

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

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

2.6. Zakres dostępu do systemów informatycznych może być dokumentowany w indywidualnych kartach uprawnień.

3. Uwierzytelnianie w systemach informatycznych (§ 5 ust.2 rozporządzenia).

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

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

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

3.4. Każdy użytkownik dysponuje indywidualnym identyfikatorem oraz hasłem. Użytkownik nie może ujawniać swojego hasła. W przypadku jego ujawnienia użytkownik musi niezwłocznie zmienić hasło. O przyczynach zmiany powiadamia Administratora Danych.

3.5. 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.

3.6. Hasło musi spełniać następujące wymagania:

3.6.1. nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
3.6.2. musi zawierać co najmniej 8 znaków, w tym małe i wielkie litery oraz cyfry lub znaki specjalne,
3.6.3. nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
3.6.4. nie może być jednakowe z identyfikatorem użytkownika,
3.6.5. musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika,
3.6.6. w trakcie wpisywania, nie może być wyświetlane na ekranie,
3.6.7. musi być zmieniane nie rzadziej niż co 30 dni.

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

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

4. Praca z systemem informatycznym (§ 5 ust.3 rozporządzenia).

4.1. Kontrola stanowiska pracy - czynności wykonywane przed przystąpieniem przetwarzania danych osobowych:

4.1.1. użytkownik powinien sprawdzić czy nie ma oznak fizycznego naruszenia zabezpieczeń.

4.1.2. w przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora Danych.

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

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

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

4.5. 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"

4.6. 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.

4.7. 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.

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

5. Postępowanie z nośnikami danych oraz kopie bezpieczeństwa. (§ 5 ust. 4 oraz ust. 5 rozporządzenia)

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

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

5.3. 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.

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

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

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

5.7. 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.

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

5.9. Zaleca się, aby w miarę możliwości, dane na nośnikach elektronicznych były zabezpieczone hasłem.

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

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

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

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

6. Zabezpieczanie systemu informatycznego oraz systemu operacyjnego (§ 5 ust.6 rozporządzenia).

6.1. Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym ustala się na poziomie wysokim w rozumieniu § 6 ust.1 rozporządzenia

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

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

6.4. Ochrona przed złośliwym oprogramowaniem

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

- wirusy, robaki, konie trojańskie, key loggery, 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.

6.4.2. Minimalizacja prawdopodobieństwa zainfekowania systemu informatycznego szkodliwym oprogramowaniem.

a) Instalacja oprogramowania bez zgody Administratora Danych (lub informatyka) jest zabroniona.
b) Zabrania się użytkownikom dokonywania jakichkolwiek zmian w konfiguracji zainstalowanego oprogramowania, w szczególności dotyczy to oprogramowania zabezpieczającego takiego: programy antywirusowe, systemy firewall.
c) Zabrania się użytkowania nośników danych (dyskietki, płyty CD itp.) bez wcześniejszego sprawdzenia ich oprogramowaniem antywirusowym.
d) Prowadzi się jak najczęstszą aktualizację elementów systemu informatycznego o wymagane poprawki bezpieczeństwa.
e) Prowadzi się jak najczęstszą aktualizację systemów antywirusowych oraz reguł systemów wykrywania włamań (IDS - Intrusion Detection System).

6.4.3. Sprzęt i czynności, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania oprogramowania o którym mówi rozporządzenie:

a) Separacja wewnętrznej sieci komputerowej za pomocą zapory, tzw. „firewall".
b) Wyłączenie nieużywanych usług systemu informatycznego.
f) Ograniczenie uprawnień użytkowników do niezbędnego minimum.
g) Stosowanie podziału na podsieci (wydzielanie vlanów).
h) Stosowanie szyfrowanych kanałów dostępu do sieci z zewnątrz (VPN).

6.4.4. Ochrona antywirusowa

a) 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.

b) Dostęp do konfiguracji oprogramowania konfiguracyjnego musi być dostępny jedynie dla Administratora Danych lub Informatyka

i) Każdy element wprowadzany / zapisywany w komputerze, w tym załączniki do korespondencji elektronicznej „e-mail", musi zostać sprawdzony za pomocą programu antywirusowego.

6.5. Korzystanie z poczty elektronicznej

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

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

6.5.3. Użytkownicy SI powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

6.5.4. 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.

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

6.5.6. Zabrania się:

- 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.

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

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

6.6. Korzystanie z sieci Internet

6.6.1. Korzystanie z sieci dozwolone jest wyłącznie dla celów służbowych,

6.6.2. Zabronione jest:

- przesyłanie lub udostępnianie w sieci Internet jakichkolwiek informacji lub danych przy pomocy narzędzi typu: e-mail, ftp, 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,
- stosowanie niezatwierdzonych komunikatorów internetowych,
- korzystanie z prywatnej poczty e-mail, w tym do celów służbowych,
- wykorzystywanie w Internecie przydzielonych do celów służbowych loginów i haseł,
- wchodzenie na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo.

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

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

6.7. Przesyłanie danych osobowych

6.7.1. Przesyłanie danych osobowych lub innych informacji chronionych za pośrednictwem służbowej poczty elektronicznej 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 inną drogą niż poczta elektroniczna.
- Każdorazowe udostępnienie danych drogą elektroniczną musi zostać odnotowane w rejestrze udostępnień.

6.8. 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.

7. Przeglądy i konserwacja i naprawa systemu informatycznego oraz sprzętu komputerowego

7.1. Miejsce wykonywania przeglądów i konserwacji.

7.1.1. 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".

7.1.2. 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.

7.1.3. 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.

7.2. Częstotliwość wykonywania przeglądów i konserwacji.

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

7.3. 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.

7.4. 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.

8. Ewidencja wpisów, udostępnianie informacji (§ 5 ust.7 oraz § 7 ust.1 rozporządzenia).

8.1. Administrator Danych 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.

Administrator Danych 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.

8.2. Rejestracja informacji o odbiorcach danych osobowych.

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

a) imię i nazwisko lub nazwa odbiorcy,

b) data udostępnienia oraz zakres udostępnienia.

Wzór rejestru udostępnień danych osobowych jest załącznikiem do Polityki Bezpieczeństwa Danych Osobowych.