Załącznik do zarządzenia nr 14/2010/2011 – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana w dalszej części „Instrukcją" została opracowana w oparciu o przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych oraz wskazanie osoby odpowiedzialnej za te czynności

Upoważnienie do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych. Upoważnienie nadaje i odwołuje administrator danych. Upoważnienie i jego odwołanie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie, drugi – dla administratora danych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do Instrukcji. Wzór odwołania upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do Instrukcji. Upoważnienia nie sporządza się dla administratora danych. Upoważnienia nadane przed dniem wprowadzenia Instrukcji pozostają w mocy.

Upoważnienia do przetwarzania danych osobowych rejestrowane są w rejestrze osób upoważnionych do przetwarzania danych osobowych. Wzór rejestru stanowi załącznik nr 3 do Instrukcji. Rejestr prowadzi administrator danych.

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

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem. W Gimnazjum nr 2 w Rybniku obowiązują następujące zasady tworzenia hasła:

- hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
- hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
- hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
- hasło nie może być jednakowe z identyfikatorem użytkownika,
- hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.

Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie. Zmiana hasła po jego deklarowanym okresie ważności jest wymuszana przez system informatyczny służący do przetwarzania danych osobowych.

W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora danych.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić administratora danych.

Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi zablokować stację roboczą lub wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, takich jak dyskietki, płyty CD i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuję poprzez wylogowanie się z tego systemu.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik systemu informatycznego służącego do przetwarzania danych osobowych.

Kopie awaryjne może tworzyć jedynie administrator danych. W czasie tworzenia kopii awaryjnej praca w systemie informatycznym służącym do przetwarzania danych osobowych jest zabroniona.

Dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy w systemie informatycznym służącym do przetwarzania danych osobowych.

Kopie zapasowe powinny być kontrolowane przez administratora danych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierających dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych".

Elektroniczne nośniki informacji zawierających dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce bezpieczeństwa danych osobowych", w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.

Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.

Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

Dane osobowe przesyłane poprzez sieć Internet zabezpieczone są poprzez środki kryptograficznej ochrony.

Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, administrator danych odnotowuje je w rejestrze odbiorców danych osobowych. W rejestrze odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Wzór rejestru stanowi załącznik nr 4 do Instrukcji.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

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" przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych.

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

Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator danych. Administrator danych prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji.

Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika Gimnazjum nr 2 w Rybniku.

Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych

Administrator danych ma prawo do **kontroli** stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w **dowolnym terminie.**

Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

Załącznik nr 1 do Instrukcji – wzór upoważnienia do przetwarzania danych osobowych

Rybnik, dnia ..... roku

UPOWAŻNIENIE NR ……. DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych upoważniam Panią/Pana … *(imię i nazwisko)* zatrudnioną/zatrudnionego na stanowisku … *(nazwa zajmowanego stanowiska)* do przetwarzania danych osobowych w ramach wykonywania czynności służbowych.

Administrator danych

……
(pieczątka i podpis)

Załącznik nr 2 do Instrukcji – wzór odwołania upoważnienia do przetwarzania danych osobowych

Rybnik, dnia ..... roku

ODWOŁANIE UPOWAŻNIENIE NR ..... DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych odwołuję z dniem … *(data)* upoważnienie do przetwarzania danych osobowych wystawione dla Pani/Pana … *(imię i nazwisko).*

Administrator danych

……
(pieczątka i podpis)

Załącznik nr 3 do Instrukcji – wzór rejestru osób upoważnionych do przetwarzania danych osobowych

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Numer upoważnienia	Imię i nazwisko	Data nadania upoważnienia	Data odebrania upoważnienia	Identyfikator użytkownika w systemie

Załącznik nr 4 do Instrukcji – wzór rejestru odbiorców danych osobowych

REJESTR ODBIORCÓW DANYCH OSOBOWYCH

Imię i nazwisko lub nazwa odbiorcy	Data udostępnienia	Zakres udostępnienia