Instrukcja Zarządzania Systemem Informatycznym

Rozdział 1
Postanowienia ogólne

§ 1.

Instrukcja Zarządzania Systemem Informatycznym, zwana dalej „Instrukcją", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych

§ 2.

Użyte w Instrukcji określenia oznaczają:

1) Administrator Danych	- Dyrektor Miejsko-Gminnego Ośrodka Kultury w Woźnikach, ul. Górna 5;
2) Użytkownik	- osobę upoważnioną do przetwarzania danych osobowych;
3) Inspektor Ochrony Danych Osobowych (IODO)	- osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych;
4) Administrator Systemu Informatycznego	- osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń, o ile zadanie te zostały wyłączone z zakresu kompetencji IODO;
5) Naruszenie zabezpieczenia	- jakiekolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, niezawodności, integralności lub poufności systemów informatycznych;

Rozdział 2
Przydział haseł i identyfikatorów

§ 3.

Dla każdego użytkownika jest ustalany odrębny identyfikator i hasło dostępu do komputera, na którym pracuje.

§ 4.

Identyfikator użytkownika:
1) jest niepowtarzalny, a po wyrejestrowaniu użytkownika i nie jest przydzielany innej osobie;
2) jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, zgodnie, wraz z imieniem i nazwiskiem użytkownika.

§ 5.

Hasło użytkownika:
1) jest przydzielane indywidualnie dla każdego z użytkowników;
2) nie jest zapisane w systemie komputerowym w postaci jawnej.

§ 6.

1. Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników jest IODO.

§ 7.

Przydziału i zmiany haseł dokonuje się w następujący sposób:

1) hasła powinny mieć co najmniej osiem znaków i muszą zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;

2) hasła nie powinny składać się z kombinacji znaków mogących ułatwić ich odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika);

3) hasło powinno zostać zmienione niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że mogły się z nim zapoznać osoby trzecie.

§ 8.

1. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, który został mu przyznany.

2. Użytkownik jest zobowiązany utrzymywać hasło, którym się posługuje lub posługiwał, w ścisłej tajemnicy, w szczególności dołożyć wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem, nawet po ustaniu jego ważności.

Rozdział 3
Rejestrowanie i wyrejestrowywanie użytkowników

§ 9.

1. Rejestracji i wyrejestrowywania użytkowników dokonuje IODO.

2. IODO prowadzi rejestr użytkowników.

3. Jakakolwiek zmiana informacji ujawnionych w rejestrze podlega natychmiastowemu odnotowaniu i uaktualnieniu.

§ 10.

W systemach informatycznych może zostać zarejestrowany jedynie użytkownik, któremu osoba upoważniona do tego osoba wydała upoważnienie do przetwarzania danych osobowych w ……

§ 11.

1. Po zarejestrowaniu w ……. użytkownik jest informowany przez IODO o ustalonym dla niego identyfikatorze i konieczności posługiwania się hasłami.

§ 12.

Użytkownik jest wyrejestrowywany z …… w każdym przypadku utraty przez niego uprawnień do przetwarzania danych osobowych, co ma miejsce szczególnie w przypadku:

1) ustania zatrudnienia tego użytkownika lub zakończeniu przez tego użytkownika współpracy na podstawie umowy cywilno-prawnej;

2) zmiany zakresu obowiązków użytkownika powodujących utratę uprawnień do przetwarzania danych osobowych.

Rozdział 4
Rozpoczęcie, zawieszenie i zakończenie pracy Użytkownika

§ 13.

Użytkownik rozpoczynając pracę jest zobowiązany zalogować się posługując się swoim identyfikatorem i hasłem.

§ 14.

1. W przypadku, gdy użytkownik planuje przerwać pracę, jest zobowiązany do zabezpieczenia dostępu do komputera za pomocą wygaszacza ekranu z aktywnym hasłem.

2. W przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres, a także kończąc pracę, jest zobowiązany wylogować się oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki zawierające dane osobowe.

§ 15.

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczenia lub zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych, użytkownik jest zobowiązany niezwłocznie poinformować o tym IODO
2. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na oko1iczności, o których mowa w ust. 1.

Rozdział 5
Tworzenie oraz przechowywanie kopii awaryjnych

§ 16.

Za tworzenie i przechowywanie kopii awaryjnych danych osobowych przetwarzanych w sposób zgodny z przepisami prawa oraz poniższymi procedurami jest odpowiedzialny IODO.

§ 17.

1. Kopie awaryjne danych osobowych przetwarzanych są tworzone nie rzadziej niż raz na kwartał i zawierają pełny obraz danych osobowych.
2. Kopie o których mowa w ust. 1 przechowuje się odpowiednio zabezpieczone przed dostępem osób nieuprawnionych w różnych miejscach, w tym w lokalizacjach innych niż zbiór danych osobowych eksploatowany na bieżąco.

§ 18.

1. Kopie awaryjne danych osobowych przetwarzanych po ustaniu ich użyteczności są bezzwłocznie usuwane.
2. Kopie awaryjne danych osobowych przetwarzanych, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.

Rozdział 6
Ochrona przed wrogim oprogramowaniem

§19.

Bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego i kradnącego hasła odbywa się przy zastosowaniu zainstalowanego na każdej stacji roboczej aktualizowanego na bieżąco programu antywirusowego automatycznie monitorującego występowanie wirusów, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego, oprogramowania kradnącego hasła podczas operacji na plikach.

§ 20.

1. Nadzór nad instalowaniem oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje IODO.

§ 21.

1. O każdorazowym wykryciu wirusa lub konia trojańskiego przez oprogramowanie monitorujące użytkownik jest zobowiązany niezwłocznie powiadomić IODO. Po usunięciu wirusa lub innego niebezpiecznego oprogramowania IODO, sprawdza oraz przywraca go do pełnej funkcjonalności i sprawności.

§ 22.

1. W ramach ochrony przed wrogim oprogramowaniem IODO stosuje logiczne lub fizyczne urządzenia firewall.

§ 23.

Dyski lub inne informatyczne nośniki zawierające dane osobowe przetwarzane są przechowywane w sposób uniemożliwiający dostęp do nich osobom innym niż użytkownicy.

§ 24.

1. Żadne nośniki informacji zawierające dane osobowe nie są udostępniane poza obszar, w którym są przetwarzane dane osobowe.
2. Zapis w ust. 1 nie dotyczy sytuacji, gdy IODO udostępnia posiadanych w zbiorze danych osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

Rozdział 7
Przeglądy i konserwacja, sprzętu komputerowego oraz zbioru danych osobowych

§ 25.

1. Przeglądy i konserwacje sprzętu komputerowego wynikające ze zużycia sprzętu oraz warunków zewnętrznych i eksploatacji, z uwzględnieniem ważności sprzętu dla funkcjonowania, są dokonywane przez IODO

§ 26.

1. Dyski lub inne informatyczne nośniki informacji umieszczone w urządzeniach przeznaczonych do napraw, gdzie jest wymagane zaangażowanie zewnętrznych firm serwisowych, usuwa się z tych urządzeń lub pozbawia się przed naprawą zapisu danych osobowych przetwarzanych.
2. W przypadku niemoż1iwości usunięcia nośnika lub pozbawienia go zapisu tych danych osobowych naprawy dokonuje się pod nadzorem IODO

§ 27.

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przetwarzane, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przetwarzane, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych osobowych, pozbawia się wcześniej ich zapisu.

Rozdział 8
Postępowanie w zakresie komunikacji w sieci komputerowej

§ 28.

Dostęp do danych osobowych przetwarzanych jest dozwolony jedynie po właściwym zalogowaniu się i podaniu własnego hasła użytkownika.

Rozdział 9
Wymagania sprzętowo-organizacyjne

§ 29.

1. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
2. Komputery powinny zostać ustawione w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną użytkowników.

§ 30.

Osoby nieuprawnione do dostępu do danych osobowych w …….mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe w ……. wyłącznie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 31.

1. Decyzję o instalacji na stacji roboczej obsługującej przetwarzanie danych osobowych w jakiegokolwiek oprogramowania systemowego lub użytkowego podejmuje IODO

Rozdział 10
Postanowienia końcowe

§ 32.

Do spraw nieuregulowanych w Instrukcji stosuje się przepisy o ochronie danych osobowych.

§ 33.

Instrukcja nie wyłącza stosowania innych instrukcji dotyczących zabezpieczeń.