BURMISTRZ BIERUTOWA
ul. Moniuszki 12, 56-420 Bierutów

ZARZĄDZENIE Nr 33/16
BURMISTRZA BIERUTOWA

z dnia 7 kwietnia 2016 r.

w sprawie Instrukcji Użytkownika Systemu Informatycznego Urzędu Miejskiego w Bierutowie.

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r., poz. 594 ze zm.), art. 36. ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182) oraz §3, §4 i §5 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. z 2004 r. Nr 100 poz. 1024), zarządzam co następuje:

§ 1. Wprowadzam do stosowania „Instrukcję Użytkownika Systemu Informatycznego Urzędu Miejskiego w Bierutowie." w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuję kierowników referatów, osoby zatrudnione na samodzielnych stanowiskach pracy w tut. Urzędzie do sprawowania nadzoru nad ochroną przetwarzanych danych osobowych oraz do współpracy z Administratorem Danych Osobowych (dalej: ADO) w tym zakresie oraz z Administratorem Systemu Informatycznego do przetwarzania danych osobowych (dalej: ASI).

§ 3. Zobowiązuję pracowników Urzędu Miejskiego w Bierutowie przetwarzających dane osobowe, do przestrzegania przepisów o których mowa w § 1.

§ 4. Nadzór nad wykonaniem zarządzenia sprawuję osobiście.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Sporządził: Adam Kutek

Burmistrz Bierutowa
mgr Władysław Bogusław Kobiałka

Załącznik do Zarządzenia nr 33/16
Burmistrza Bierutowa z dnia 7 kwietnia 2016 r.

INSTRUKCJA UŻYTKOWNIKA SYSTEMU INFORMATYCZNEGO URZĘDU MIEJSKIEGO W BIERUTOWIE

1. Bezpieczeństwo haseł.

- Każdy użytkownik systemu informatycznego posiada własne hasło i identyfikator.
- Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.
- Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.
- Przy wyborze hasła obowiązują następujące zasady:

  - minimalna długość hasła – 8 znaków,

  - złożoność hasła - litery duże i małe oraz cyfry i znaki specjalne.
- Zakazuje się stosować haseł:

  - które użytkownik stosował poprzednio,

  - będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),

  - zawierających ogólnie informacje, takie jak np.: imię, nazwisko, numer telefonu, imiona dzieci itp.
- Zmiany hasła nie należy zlecać innym osobom, poza Informatykiem Urzędu Miejskiego.
- W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
- Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
- W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
- Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
- Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.

2. Bezpieczeństwo logowania.

- Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu nazwy użytkownika oraz hasła.
- Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację, należy wykonać opcję wylogowania z systemu.
- Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi, zobowiązana jest wykonać opcję wylogowania z systemu.

3. Bezpieczeństwo pracy z systemem.

- Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych, zagrożone karą dyscyplinarną, włącznie ze zwolnieniem w trybie dyscyplinarnym.
- Zabronione jest podejmowanie działań mogących być zagrożeniem dla systemu, a w tym:

  - łamanie haseł,

  - dokonywanie włamań na konta innych użytkowników,

  - nieprawne uzyskiwanie dostępu do kont administracyjnych,

  - zakłócanie działania usług,

  - omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione),

  - doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty,

  - praca na koncie innego użytkownika.
- Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, a następnie wykonać zamknięcie systemu.

4. Bezpieczeństwo pracy z oprogramowaniem i siecią publiczną Internet.

- Zabronione jest uruchamianie lub instalowanie i uruchamianie oprogramowania niezwiązanego merytorycznie z wykonywaną pracą.
- Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
- Użytkownicy zobowiązani są do niezwłocznego zgłaszania Informatykowi Urzędu, każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów).
- Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów, najnowszą dostępną wersją programu antywirusowego.
- Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
- Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
- W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien:

  - odłączyć stanowisko komputerowe od sieci,

  - zawiadomić Informatyka Urzędu o zaistniałym zdarzeniu,

  - zanotować nazwę wirusa, uruchomić program antywirusowy celem wykonania skanu

  dysku twardego.

5. **Bezpieczeństwo danych na komputerach stacjonarnych i przenośnych.**

- Za bezpieczeństwo komputerów odpowiedzialni są ich użytkownicy.
- Komputery przenośne po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo (szafy zamykane na klucz).
- W przypadku korzystania z komputerów należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
- Podczas transportu komputerów przenośnych wynoszonych poza obszar przetwarzania danych osobowych, należy zapewnić ich bezpieczeństwo, tj. nie należy ich pozostawiać bez nadzoru w samochodzie (lub innym miejscu). Muszą one być przewożone jako bagaż podręczny.
- Należy unikać przechowywania na komputerach przenośnych danych osobowych lub innych ważnych danych.
- W przypadku konieczności zapisania na komputerze przenośnym danych osobowych lub innych ważnych danych, należy stosować wobec tych danych środki ochrony kryptograficznej.

6. **Bezpieczeństwo danych na nośnikach przenośnych.**

- Należy unikać przechowywania ważnych danych na nośnikach zewnętrznych, takich jak np. pendrive-y.
- Zabronione jest używanie pendrive-ów lub innych nośników do przenoszenia danych na prywatne komputery lub inne urządzenia mogące służyć do przechowywania danych.

7. **Postanowienia końcowe:**

- Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych zagrożone karą dyscyplinarną, włącznie ze zwolnieniem w trybie dyscyplinarnym.
- Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.
- Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
- Za bezpieczeństwo komputerów odpowiedzialni są ich użytkownicy.

Burmistrz Bierutowa

mgr Władysław Bogusław Kobiałka