Załącznik Nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Kultury w Drawsku Pomorskim

REGULAMIN UŻYTKOWNIKA SYSTEMÓW TELEINFORMATYCZNYCH OŚRODKA KULTURY W DRAWSKU POMORSKIM

§1.Zasady korzystania ze sprzętu komputerowego i systemów informatycznych:

1) użytkownik zobowiązany jest do bezterminowego zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę;

2) tworzenie kont w systemach, nadawanie, modyfikacja oraz usunięcie uprawnień, instalacja lub deinstalacja oprogramowania, grupowa instalacja lub deinstalacja, wydanie lub przekonfigurowanie sprzętu odbywa się na pisemny wniosek osoby zainteresowanej. Wnioski realizowane są przez Administratora Systemu Informatycznego;

3) sprzęt komputerowy oraz zainstalowane na nim oprogramowanie, jakie zostało oddane użytkownikowi w okresie jego pracy jest wykorzystywany tylko do celów służbowych;

4) użytkownik dba o powierzony mu sprzęt oraz chroni go przed szkodliwym wpływem warunków zewnętrznych;

5) użytkownik zabezpiecza w miarę posiadanych możliwości sprzęt przed kradzieżą;

6) hasła użytkowników do systemów podlegają następującym zasadom:

   a) hasło składa się z minimum 8 znaków, przy czym zawiera wielki i małe litery, oraz cyfry lub znaki specjalne,
   b) hasło musi być zmieniane minimum co 30 dni,
   c) kolejne hasła muszą być różne,
   d) hasła należy przechowywać w sposób gwarantujący ich poufność,
   e) zabrania się udostępniania haseł innym osobom;

7) zabrania się tworzenia haseł na podstawie:

   a) cech i numerów osobistych (np. dat urodzenia, imion itp.),
   b) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
   c) identyfikatora użytkownika,
   d) innych haseł łatwych do odgadnięcia.

8) użytkownicy nie mogą udostępniać innym osobom indywidualnych identyfikatorów (nazwa użytkownika, token, karta inteligentna i inne dane umożliwiające uwierzytelnienie);

9) użytkownik zobowiązany jest przestrzegać zasady „czystego biurka” i „czystego ekranu”. Stosowanie tych zasad sprowadza się do:
   a) schowania wszystkich dokumentów, nośników danych, związanych z informacjami chronionymi w miejsce niedostępne dla innych osób po zakończeniu pracy,
   b) odchodząc od stacji roboczej, użytkownik blokuje komputer uniemożliwiając zalogowanie się do systemu osobie nieuprawnionej,
   c) kończąc pracę użytkownik zamyka wszystkie aplikacje, wylogowuje się z systemu i wyłącza komputer;

10) zabrania się użytkownikom uruchamiać (w tym aplikacji przenośnych ang. portable) i instalować na sprzęcie służbowym jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonuje Administrator Systemu Informatycznego, na podstawie pisemnych wniosków;

11) zabrania się użytkownikom:

   a) omijania mechanizmów kontroli (np. używania serwerów proxy),
   b) testowania wdrożonych zabezpieczeń,
   c) skanowania urządzeń sieciowych, serwerów oraz stacji roboczych pod kątem badania świadczonych usług,
   d) wyłączania programów uruchamianych automatycznie przy starcie systemu,
   e) odinstalowania programów,
   f) przyłączania i użytkowania prywatnego sprzętu, w tym używania prywatnych nośników danych,
   g) podejmowania jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją;

12) ważne pliki należy przechowywać w wyznaczonych folderach na serwerach, które gwarantują bezpieczeństwo danych;

13) za bezpieczeństwo danych przechowywanych lokalnie na komputerze odpowiada użytkownik;

14) zabrania się przechowywania na sprzęcie służbowym gier oraz plików multimedialnych np. filmów, obrazów, dźwięków nie związanych z zadaniami służbowymi;

15) na sprzęcie komputerowym instaluje się oprogramowanie do ilościowej jak i jakościowej kontroli użytkowników, które stosuje się w celu okresowej kontroli wykorzystania sprzętu służbowego przez użytkowników;

16) w przypadku używania zewnętrznych nośników danych na stacji roboczej użytkownik wcześniej wykonuje skanowanie programem antywirusowym wszystkich danych na nośniku;

17) w przypadku gdy użytkownik wykryje zainfekowane dane niezależnie od źródła (np. strona internetowa, załącznik poczty elektronicznej, dane na nośniku)

bezzwłocznie powiadamia o tym fakcie Administratora Systemu Informatycznego;

18) zabrania się użytkownikom samodzielnego przenoszenia i podłączania sprzętu teleinformatycznego między stanowiskami pracy. Czynności te wykonuje Administrator Systemu Informatycznego;

19) kończąc świadczenie pracy dla Pracodawcy, użytkownik ma obowiązek przekazać wszystkie dane (dokumenty papierowe, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu.

§2.Zasady korzystania z poczty elektronicznej:

1) nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje Administrator Systemu Informatycznego. Użytkownik zobowiązany jest do sprawdzania własnej skrzynki poczty elektronicznej;

2) poczta elektroniczna jest wykorzystywana tylko do celów służbowych;

3) zabrania się rozsyłania m.in.:
   a) ogłoszeń komercyjnych,
   b) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej),
   c) treści wulgarnych,
   d) materiałów erotycznych,
   e) treści niezgodnych z obowiązującymi przepisami prawa,
   f) treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie;

4) korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy;

5) pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli skrzynek pocztowych użytkowników. O wynikach kontroli powinien być poinformowany użytkownik;

6) nie należy otwierać linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia;

7) w przypadku dostępu do poczty elektronicznej z sieci Internet należy przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować ostrzeżeń;

8) nie zaleca się logowania do systemów poczty elektronicznej z komputerów dostępnych publicznie (np. kafejki internetowe);

9) skrzynki pocztowe posiadają ograniczoną wielkość. Użytkownik zobowiązany jest do okresowej archiwizacji wiadomości.

§3. Zasady korzystanie z Internetu

1) użytkownicy korzystają z dostępu do Internetu tylko w celach służbowych;

2) praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych;

3) pracodawca może wprowadzić kategoryzację stron internetowych oraz zablokować dostęp do wybranych kategorii;

4) odblokowanie witryny internetowej może nastąpić na pisemny wniosek kierownika komórki organizacyjnej;

5) Zabrania się:

    a) wykorzystywania sieci Internet w sposób, który mógłby narazić Pracodawcę na utratę dobrego imienia,
    b) pobierania oprogramowania (w tym w wersjach darmowych), nie związanego z wykonywanymi obowiązkami służbowymi,
    c) podłączania sieci Internet do fizycznie odseparowanych sieci,
    d) udostępniania łącza internetowego dostarczonego przez pracodawcę innym osobom bez zgody kierownika komórki organizacyjnej oraz Administratora Systemu Informatycznego,
    e) instalowania urządzeń udostępniających Internet na sprzęcie Pracodawcy bez zgody kierownika komórki organizacyjnej oraz Administratora Systemu Informatycznego.