**ZASADY BEZPIECZNEGO UŻYTKOWANIA**

**INTERNETOWEGO SYSTEMU ATMS Kids/ePrzedszkole**

1. Każdy użytkownik systemu otrzymuje i posługuje się indywidualnym, imiennym

kontem.

1. Informacje o koncie (identyfikator, hasło) przekazywane są użytkownikom w formie

zapewniającej poufność. Jeżeli użytkownik podejrzewa naruszenie poufności zobowiązany jest niezwłocznie zgłosić ten fakt przedstawicielowi Zamawiającego w Umowie odrębnej, odpowiedzialnemu za realizację Umowy odrębnej.

1. Wraz z informacją o koncie użytkownik w czasie szkolenia zostaje pouczony w

zakresie odpowiedzialności za posługiwanie się kontem oraz otrzymuje opis zasad bezpiecznego użytkowania systemu.

1. Zaleca się, by każdy użytkownik złożył oświadczenie potwierdzające znajomość zasad

bezpieczeństwa i przepisów o ochronie danych osobowych oraz zobowiązanie do ich przestrzegania. Szczegółowe zasady w tym zakresie regulują wewnętrzne procedury Powierzającego.

1. Użytkownik podczas pierwszej sesji pracy z systemem, niezwłocznie po uzyskaniu

dostępu do indywidualnego konta powinien dokonać zmiany hasła.

6. Użytkownik powinien zmieniać swoje hasło nie rzadziej niż co 30 dni.

7. Hasło powinno składać się z co najmniej jednej wielkiej litery, co najmniej jednej

 małej litery oraz co najmniej jednej cyfry lub znaku specjalnego. Minimalna

 dopuszczalna długość hasła to 8 znaków.

8. Hasło należy zapamiętać, nie należy go zapisywać. Jeśli istnieje konieczność zapisania

 hasła, należy przechowywać je w bezpiecznym miejscu.

9. Obowiązuje bezwzględny zakaz ujawniania haseł osobom trzecim.

10. W przypadku podejrzenia wejścia w posiadanie hasła przez osoby trzecie należy

 niezwłocznie: a. podjąć próbę zmiany hasła, b. zgłosić fakt przedstawicielowi

 Zamawiającego w Umowie odrębnej, odpowiedzialnemu za realizację Umowy

 odrębnej.

11. W przypadku zapomnienia bądź utraty hasła należy zgłosić się do administratora

 jednostki nadrzędnej w stosunku do jednostki, do której przypisany jest użytkownik.

12. Administrator dokonuje zmiany hasła jedynie na wniosek właściciela konta, po potwierdzeniu jego tożsamości.

13. Użytkownik wprowadzając hasło powinien mieć pewność, że nie zostanie ono podejrzane przez osoby trzecie.

14. Kończąc lub przerywając pracę z systemem należy się bezwzględnie wylogować. Dotyczy to w szczególności sytuacji, w której użytkownik oddala się od komputera, na którym pracował.

15. Komputery, za pomocą których użytkownicy korzystają z systemu powinny być chronione za pomocą rozwiązań zapewniających zachowanie poufności i integralności danych.

16. Użytkownicy zobowiązani są do przestrzegania powszechnie obowiązujących przepisów z zakresu ochrony danych osobowych.