1. **Cel**

Określenie zasad związanych z zarządzaniem identyfikatorami oraz hasłami użytkowników systemu informatycznego.

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkie osoby mające uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

1. **Opis postępowania**
   1. Hasło musi zawierać nie mniej niż 12 znaków.
   2. Hasło musi składać się z liter (małych i dużych) oraz cyfr i znaków specjalnych.
   3. Hasło musi być zmieniane nie rzadziej niż raz na 30 dni.
   4. Hasła nie mogą być ujawniane innym osobom.
   5. Hasła do różnych systemów powinny być różne, za wyjątkiem sytuacji, gdy jest możliwe zastosowanie mechanizmu jednokrotnego logowania.
   6. Hasła nie mogą być przechowywane w czytelnej postaci, zarówno jako tekst zapisany w pliku jak i na papierze.
   7. Wyjątkiem jest zdeponowanie haseł użytkowników, jak i administratorów w bezpiecznym miejscu (sejfie, szafie pancernej lub w równoważnym miejscu), w zamkniętej kopercie, opisanej imieniem i nazwiskiem osoby upoważnionej do jej otwarcia.
   8. Hasło powinno zostać niezwłocznie zmienione w przypadku ujawnienia lub podejrzenia ujawnienia osobie nieuprawnionej.
   9. Hasła tymczasowe lub startowe powinny być zmienione po pierwszym logowaniu.
   10. Hasła domyślne tzw. defaultowe powinny być niezwłocznie zmienione.
   11. W przypadku zakończenia świadczenia pracy lub odbiorze upoważnienia do przetwarzania danych, konto użytkownika powinno zostać niezwłocznie zablokowane.
   12. Identyfikator raz użyty nie może być wykorzystywany ponownie.
   13. Hasła wykorzystywane w systemach informatycznych organizacji nie mogą być używane w innych miejscach np. do zabezpieczania zasobów prywatnych użytkownika.
   14. Hasła powinny być trudne do odgadnięcia (zaleca się nie stosować nazw potocznych, imion, nazwisk, dat urodzenia, numerów dokumentów, innych danych osobistych oraz standardowych kombinacji znaków, np. 12345678).
   15. Trzykrotna błędna próba wprowadzenia hasła powinna skutkować zablokowaniem konta użytkownika oraz odpowiednią adnotacją w systemie monitoringu zawierająca co najmniej: identyfikator komputera/urządzenia na którym próbowano dokonać logowania oraz czas wykrycia zdarzenia.
   16. Hasła nie powinny być tworzone według stałego schematu, np.: ALA\_01, ALA\_02 itp.
   17. Hasła powinny być wprowadzane w sposób maskowany.
   18. Powinna zostać tworzona historia haseł w celu zablokowania ich powtarzania.