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. W celu zapewnienia wyłącznie prawidłowego i uzasadnionego dostępu do systemu informatycznego oraz dla zapobiegania nieuprawnionemu dostępowi do systemu informatycznego, nadawanie uprawnień do systemów teleinformatycznych odbywa się z uwzględnieniem poniższych zasad:
      1. Pracownikowi mogą być nadane wyłącznie uprawnienia, które są konieczne do realizacji zleconych mu zadań (stosuje się zasadę minimalnych uprawnień, tzn. domyślnie stosuje się brak jakichkolwiek uprawnień).
      2. Uprawnienia do systemu nadawane są przez Administratora Systemów Informatycznych.
      3. Pracownikom nadawane są unikalne identyfikatory.
      4. Nazwy kont pracowników muszą zapewniać jednoznaczną identyfikację.
      5. Konta umożliwiające działania administracyjne (np. root, Administrator) muszą zapewniać pełną rozliczalność i identyfikalność działań. W tym celu konta z uprawnieniami administracyjnymi winny być przypisane do konkretnych osób.
      6. Hasła administracyjne ustala Administrator Systemów Informatycznych.
      7. Administratora Systemów Informatycznych jest zobowiązany do prowadzenia metryk haseł administratora i przechowywania ich w zamkniętych kopertach, odrębnych dla każdego systemu/aplikacji, w sejfie lub w szafie pancernej, do których dostęp ma także Administrator Danych.
      8. Wszyscy użytkownicy systemu zobowiązani są do stosowania polityki haseł zgodnie z wytycznymi zawartymi w procedurze Polityka haseł.
      9. Wszelkie zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub cofnięcie upoważnienia do przetwarzania danych osobowych są przesłanką do niezwłocznego zablokowania konta użytkownika systemu informatycznego.
      10. Administrator Systemów Informatycznych ma obowiązek okresowej kontroli i weryfikacji zasadności posiadanych przez użytkowników uprawnień (przynajmniej raz na 3 miesiące). W przypadku braku zasadności, dostęp do systemu powinien zostać niezwłocznie cofnięty.
      11. Nie dopuszcza się tworzenia kont grupowych.